TÜBİTAK BİLGEM

BİLGEM TEKNOLOJİ

Eylül 2020 / Sayı:10

TÜBİTAK BİLGEM Kurumsal Dergisi. Dört ayda bir yayınlanır. Parayla satılamaz.

TÜBİTAK BİLGEM

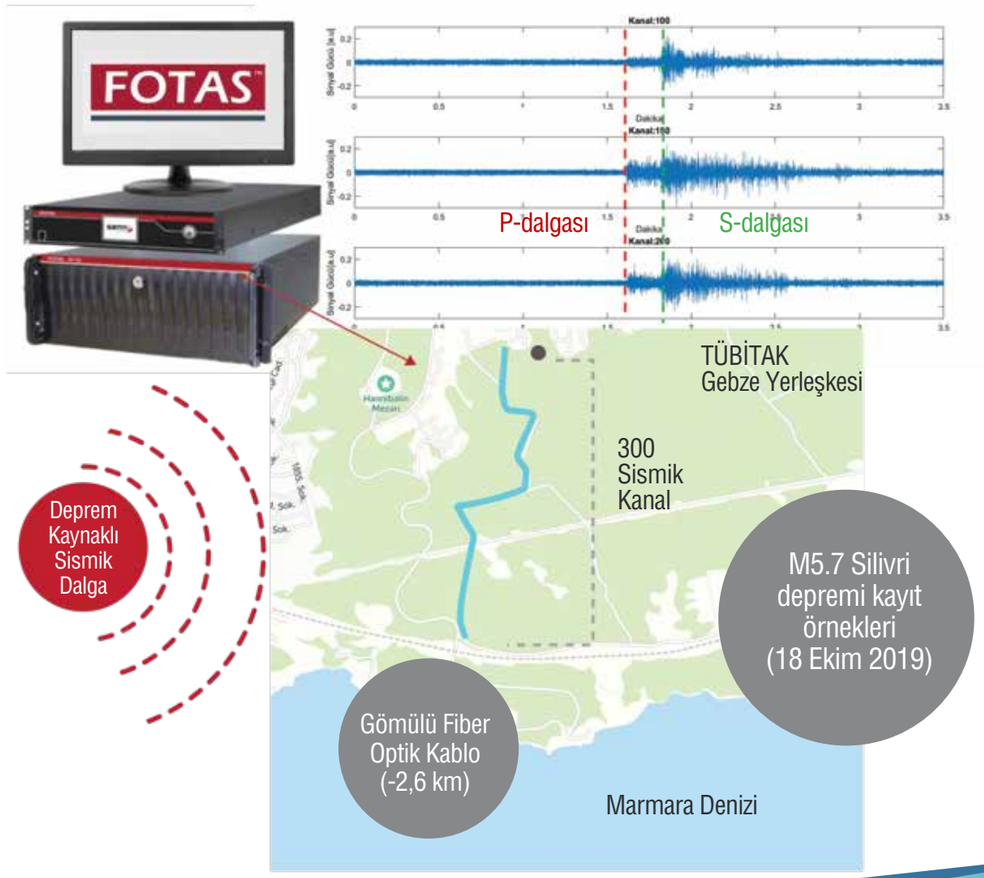
Bu bir proje tanıtımıdır.

Fiber Optik Tabanlı Akustik Sensör (FOTAS) Projesi

BİLGEM, fiber kablo teknolojisi ile sismik hareketleri ölçüyor. Prototip çalışmalarında sona gelinen Fiber Optik Tabanlı Akustik Sensör (FOTAS) Projesiyle geliştirilen teknolojinin endüstriye kazandırılması için özel sektörle görüşmelere başlandı.

Fiber optik kabloların akustik algılayıcı olarak kullanımı ile kablo güzergahı boyunca akustik titreşime neden olan her türlü insan kaynaklı (yürüme, kazma, delme, patlatma, vb.) ve doğal (kaya düşmesi, heyelan, deprem, vb.) olayları algılamak mümkün.

Fiber Optik Tabanlı Akustik Sensör (FOTAS) sistemi ile ülkemizde gerçekleşen depremler kayıt altına alınmaya başlandı. FOTAS ile Marmara Bölgesi'ndeki depremler kolay bir şekilde algılanırken, uzak bölgelerdeki depremler de şiddetine göre tespit edilebiliyor.



Başkandan

Merhaba

Sayısal (dijital) elektronik devrelerin geliştirilmeye başlanması, buna bağlı olarak bilgisayarların, internetin ortaya çıkması ve haberleşme sistemlerinin hızlı gelişimi ile veri işleme, depolama ve iletişim her açıdan çok kolaylaştı ve tüm bu sistemler hızla yaşamımızın bir parçası haline geldi. Bu hızlı gelişim, elbette içerisinde pek çok tehdit de barındırıyor. Bu gelişmeler ve kolaylıklarla beraber günümüzde bilgi güvenliği de bireyler, kurumlar ve devletler için en önemli ihtiyaçlardan biri haline gelmiştir.

Temel olarak bilgi güvenliği; bilginin izinsiz veya yetkisiz bir biçimde erişimi, kullanımı, değiştirilmesi, ifşa edilmesi, ortadan kaldırılması, el değiştirmesi ve hasar verilmesini önlemek olarak tanımlanabilir. Buna bağlı olarak bilgi güvenliğinin "gizlilik", "bütünlük" ve "erişilebilirlik" olmak üzere üç temel unsurdan meydana geldiğini söyleyebiliriz. Öğelerden herhangi biri zarar görürse, bilgi güvenliği zaafı oluşacaktır.

Günümüzde ticari ve askeri savaşlar, bilgi casusluğu ve siber saldırılar üzerinden yürütülmeye başlanmıştır. Sadece kritik verilerin güvenliği yetmemekte aynı zamanda kritik altyapıların güvenliğinin de sağlanması gerekmektedir. Her ülke, kendi kritik bilgilerinin/kurumlarının güvenliğini kendisi sağlamak durumundadır. Bu ihtiyaç, en az sınırları korumak kadar önemli bir hal almıştır. Bilgi güvenliği alanında, ülke ihtiyaçlarını kritik donanım/yazılım bileşenlerinden başlayarak kullandığımız sistemlere kadar kendimiz geliştirmediğimiz sürece, bilgi güvenliğini tam olarak sağlamamız mümkün olmayacaktır.

Bilgi Güvenliği ve BİLGEM

TÜBİTAK BİLGEM olarak kırk yılı aşkın bir süredir, seçkin ve konularında uzman araştırmacı kadrolarımız ve donanımlı araştırma laboratuvarlarımızla, ülkemizin kritik kurumlarının bilgi güvenliğini sağlamak için çalışıyoruz. Bu amaçla cihazlar, sistemler geliştiriyor, gerektiğinde test, danışmanlık ve eğitim hizmetleri veriyoruz. Sadece günümüz ihtiyaçlarına odaklanmıyoruz; bilgi güvenliği alanında ülkemiz açısından risk teşkil edebilecek tüm gelişmeleri takip ediyor, önceden tedbir alınmasını sağlıyoruz. Örneğin henüz geliştirme aşamasında olan kuantum bilgisayarların bilgi güvenliği alanında oluşturabileceği tehditleri şimdiden değerlendiriyor ve bu kapsamda alınması gereken tedbirleri belirleyerek hayata geçiriyoruz. Son dönemlerde tasarladığımız cihazlarımızda kuantum hesaplamaya dayanımlı algoritmalar ve protokoller kullanıyoruz. Sahada halen çalışan cihazlarımızda da buna ilişkin güncellemeler yapıyoruz.

Türkiye'nin bilgi güvenliği birikimine önemli katkılarda bulunan BİLGEM, bilgi güvenliği konusunda teknolojik dışa bağımlılığı yok etmek amacıyla, tasarımdan tümdevreye cihazların kritik öneme sahip tüm bileşenlerini sağlamaya çalışmaktadır. Cihazlarımızda bulunan kriptografik algoritma, protokol, donanım ve yazılım tasarımları tamamen milli olarak gerçekleştirilmektedir. Uydu, hava, kara, deniz gibi platformlar için cihaz tasarımları bulunan BİLGEM'in bilgi güvenliği kapsamında tasarlamış olduğu cihazlar, ülkemizin kritik kurumlarının yanı sıra NATO tarafından da kullanılmaktadır.

Dergimizin bu sayısında "Bilgi Güvenliği" konusunda kapsamlı bir dosya oluşturmaya çalıştık. Umuyorum ki az bilinen, ancak günümüzde gittikçe daha fazla önem kazanan bu konuda bir farkındalık oluşturabiliriz.

Dergimizin hazırlanmasında emeği geçen tüm çalışma arkadaşlarıma teşekkür ederim. Bir sonraki sayımızda buluşmak üzere, sağlıcakla kalın.

Prof. Dr. Hacı Ali Mantar

İÇİNDEKİLER

İletişim Adresi
BİLGEM Teknoloji Dergisi
P.K. 74, 41470 Gebze KOCAELİ

Telefon
(0262) 648 1000

Web
www.bilgem.tubitak.gov.tr

e-posta
bilgemteknoloji@tubitak.gov.tr

Baskı
San Ofset
Tel: (0212) 289 24 24

Baskı Tarihi
Ağustos 2020
ISSN 2717-9273

Bertuğ Kayhan - Uzman Yrd / BİLGEM İGBY

ARMERKOM Bünyesinde MÜREN Laboratuvarı Açıldı

TÜBİTAK BİLGEM tarafından, Deniz Kuvvetleri Komutanlığı Araştırma Merkezi Komutanlığı (ARMERKOM) bünyesinde "Müren Laboratuvarı" açıldı. Açılış programında proje paydaşları METEKSAN, YALTES, HAVELSAN, KBS ve STM temsilcileri de hazır bulundu.

Açılış konuşmalarından sonra katılımcılar, 'Milli Üretim Entegre Denizaltı Savaş Yönetim Sistemi Preveze Sınıfı Uygulaması'na ait 'Karaya Konuşlu Test Sistemi'nin de yer aldığı ve tüm denizaltılar için sistemlerin gemiye entegrasyonu öncesinde test edileceği Müren Laboratuvarı'nı gezdi ve icra edilen bir angajman senaryosunu izledi.

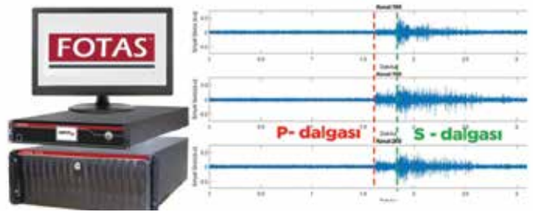
TÜBİTAK ve ARMERKOM'un denizaltı savaş yönetim sistemlerine yönelik 20 yılı aşkın tecrübesinin yansıtıldığı MÜREN Laboratuvarı, Dz.K.K.lığı ile BİLGEM arasındaki MÜREN Savaş Yönetim Sistemi (SYS) geliştirme programının ikinci büyük adımı olan MÜREN-PREVEZE Projesi kapsamında hayata geçirildi.

2017 yılında başlayan MÜREN-PREVEZE Projesi kapsamında 4 adet Preveze Sınıfı denizaltımızın tüm savaş yönetim sistemi yerli ve milli olarak geliştirilen MÜREN-SYS ile modernize edilecek. Bu kapsamda MÜREN-SYS'li ilk geminin 2021 yılı Haziran ayında filomuza katılması hedefleniyor.

Fiberoptik Kablo Teknolojisi ile Depremleri Ölçebiliyoruz

BİLGEM, yer altına gömülü fiber kablo teknolojisi ile sismik hareketleri ölçüyor. Prototip çalışmalarında sona gelinen Fiber Optik Tabanlı Akustik Sensör (FOTAS) Projesiyle geliştirilen teknolojinin endüstriye kazandırılması için özel sektörle görüşmelere başlandı.

Fiber Optik Tabanlı Akustik Sensör (FOTAS) sistemi ile ülkemizde gerçekleşen depremler kayıt altına alınmaya başlandı. FOTAS ile Marmara Bölgesi'ndeki depremler kolay bir şekilde algılanırken, uzak bölgelerdeki depremler de şiddetine göre tespit edilebiliyor.



FOTAS Nasıl Çalışıyor?

Fiber optik kablodan iletilen ışık enerjisi, FOTAS hattının güzergâhı boyunca oluşan her türlü fiziksel aktiviteden hassas bir şekilde etkileniyor. Bu etki, uygun bir optik ve elektronik donanım ve sinyal işleme yöntemleriyle analiz ediliyor ve tüm kabloyu binlerce akustik mikrofon gibi kullanmak mümkün hale geliyor. Bu nedenle fiber optik kabloların sınır ve kritik tesislerin güvenliği gibi alanlarda kullanımı da hızla yaygınlaşıyor. Güvenlik odaklı kullanımın yanında, fiber optik haberleşme altyapısının, sismik hareketleri incelemede kullanımına yönelik araştırmalar pek çok ülkede devam ediyor.

Kilometrelerce uzunluktaki mevcut fiber optik kablo altyapısının binlerce sismik algılayıcı olarak kullanımı için araştırmalar devam ederken BİLGEM, birkaç km'lik fiber optik kablo ile yüzlerce kilometre uzaktaki depremlerin tespit edilebildiğini doğruladı.

Deprem Üzerine Çalışan Kurumlar FOTAS'ı Değerlendirmeye Başladı

BİLGEM, Kandilli Rasathanesi Deprem Araştırma Enstitüsü ve İstanbul Teknik Üniversitesi'nden bilim insanları, bu teknolojinin deprem araştırmalarındaki kullanımını değerlendirmeye başladı. Mevcut haberleşme altyapısının imkânları ile sismik hareketlerin tespit ve ölçümlerinin çok daha hassas bir şekilde yapılır hale gelmesiyle, özellikle Marmara Bölgesi'nde beklenen büyük depreme yönelik hazırlık çalışmaları, daha geniş kapsamlı olarak sürdürülebilecek.

'Exascale Bilgisayarlar' Üzerine Çalışıyoruz

Bu yılın başında başlayan AB destekli The MareNostrum Experimental Exascale Platform (MEEP) Projesinde, TÜBİTAK BİLGEM ve Zagreb Ünivesitesi ortak olarak yer alıyor.

MEEP projesi, AB programı EuroHPC'nin exascale (süper bilgisayarlardan en az 30 kat daha güçlü) süper bilgisayarlarına bütünleşmiş ve bu konuda rekabetçi Avrupa teknolojisini üretme hedefinde olan bir projedir. Proje, Avrupa tarafından geliştirilen exascale sistemlerinin parçalarını oluşturabilecek teknolojilerin geliştirilmesi, entegrasyonu, test edilmesi ve ortak tasarımı için süper hesaplama altyapısı geliştirmeyi amaçlamaktadır. Hem yüksek performanslı hem de gömülü hesaplama gibi birçok Avrupa sisteminin temelini oluşturabilecek açık kaynak yazılım ve donanım ekosistemini oluşturmak, temel proje hedeflerindendir.

MEEP
MareNostrum Experimental Exascale Platform
TÜBİTAK BİLGEM
BSC Barcelona Supercomputing Center

BİLGEM olarak projeye dijital tasarım ve bilgisayar mimarisi teknolojileri konularında katkı yapacağız. Projeyle, bilgisayar mimarisinin yeni nesil versiyonlarının geliştirilmesine imkân sağlanması planlanıyor.

Projeyle ilgili detaylı bilgi için: https://meep-project.eu

Yeni Tip Sualtı Telefonu Geliştirdik

Kırktan fazla deniz platformu için sualtı telefonu geliştiren ve endüstriye bu sistemlerin teknoloji transferini yapan BİLGEM, havadan bağımsız tahrik sistemine sahip yeni denizaltılarımız için 'Yeni Tip Sualtı Telefonu geliştirdi. Tasarım ve üretim süreçleri BİLGEM bünyesinde tamamlanan 'Yeni Tip Sualtı Telefonu', milli ve yerli bir çözüm olarak savunma sanayimizin envanterine girdi. Yeni tip denizaltılarımız için batarya izleme sistemi geliştirmesi de Temmuz ayında tamamlanmıştı.

BİLGEM, bütünleşik savaş yönetim sistemlerinden çok çeşitli altyapılara kadar geniş bir yelpazede geliştirdiği cihaz ve sistemlerle, yakın zamanda milli denizaltımızı Türk Silahlı Kuvvetleri'nin hizmetine sunacak olan ana aktör kurumlar arasında yer almaktadır.

LÖSEV'den Minik Ziyaretçilerimiz Vardı

Teknolojiyle ilgili çocuklar, LÖSEV organizasyonuyla BİLGEM Siber Güvenlik Enstitüsü (SGE)'nün Ankara'daki binasını ziyaret etti.

SGE ofislerini gezen minik kardeşlerimize Enstitümüzün faaliyetlerini anlattık. SGE Konferans Salonunda ağırladığımız misafirlerimize BİLGEM ve SGE'yi tanıtan, temel bilgi güvenliği prensiplerini içeren bir sunum gerçekleştirdik. Sunum sonrasında kendilerine TÜBİTAK Yayınları'ndan çeşitli kitaplar hediye ettik. Gözlerindeki ışığın hiç solmaması temennilerimizle sevgili miniklerimizi uğurladık.

Bilgi Güvenliği

BİLGEM UEKAE Müdürü Erdal Bayram:

Ülkemizde Bir Bilgi Güvenliği Otoritesine İhtiyaç Var!

Erdal Bayram

1963 Bayburt doğumlu olup, 1986 yılında İTÜ Elektronik ve Haberleşme Bölümü'nden mezun olmuştur. 1986-1994 yılları arasında ALCATEL TELETAŞ Ar-Ge Bölümü'nde Ar-Ge Mühendisi / Kıdemli Mühendis unvanları ile çalışmış, MODEM ve Sayısal Telefon Santralı geliştirilmesi projelerinde görev almıştır.

1994 yılından bu yana TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nde çalışmaktadır. Uzman Araştırmacı olarak işe başladığı UEKAE'de Başuzman Araştırmacı, Proje Yöneticisi, Birim Yöneticisi, Bölüm Yöneticisi ve Enstitü Müdür Yardımcısı görevlerinde bulunmuştur.

Erdal Bayram, Eylül 2017 tarihinden itibaren UEKAE Müdürü olarak BİLGEM bünyesinde çalışmaya devam etmektedir. Evli ve iki çocuk babasıdır.

Bilgi güvenliği gereksinimi; kişiler, ticari kuruluşlar ve kritik devlet kurumları için farklı düzeylerdedir.

Fotoğraflar: Müge Arıtürk Mızrak-Memur / BİLGEM İGBY

Yayın Kurulu olarak Kriptoloji ve Bilgi Güvenliği konularıyla ilgili UEKAE Enstitü Müdürümüz Sayın Erdal Bayram ile bir röportaj gerçekleştirdik. Erdal Hocamızın dile getirdikleri, kurum ve ülke olarak bu alanda büyük mesafeler kat ettiğimizi gösteriyor…

Bilgi güvenliği kavramının tarihçesi hakkında bilgi verebilir misiniz?

Sahip olunan bilgilerin saklanması ve istenmeyen kişilerden korunması, insanlık tarihinde hep önemli olmuştur. Buna ilişkin bildiğimiz ilk örnekler, M.Ö. 2000'li yıllara kadar uzanmaktadır. Bu dönemde bilgi, semboller şeklinde ifade edilerek oluşturulmaktaydı ve hiç kullanılmamış semboller yardımıyla gizlilik sağlanmaya çalışılıyordu. Örneğin, M.Ö. 1500 yıllarından kalma Mezopotamya'da bulunan bir çivi yazısı tablette, az kullanılan hecelerle, çömlek yapım yöntemi şifrelenip yazılı olarak saklanmaya çalışılmıştır.

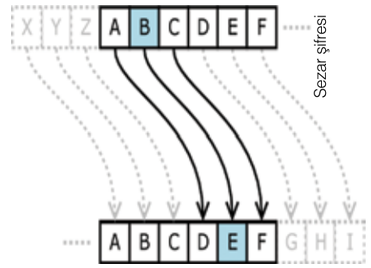
Yazının kullanılmasıyla birlikte, gizlenmesi istenen yazılı metinler, çeşitli yöntemlerle anlaşılmaz hale getirilmeye başlandı. Bunlardan belki de en bilineni Jül Sezar'ın generalleri ile haberleşmede kullandığı Sezar Şifresi'dir. Geçen zaman içerisinde bilginin saklanması ve iletilmesi için pek çok yöntem geliştirildi ve kullanıldı. Buradaki en önemli husus, aslında kullanılan yöntemin gizliliğiydi. Osmanlılar döneminde de ülkemizde benzeri bazı kripto tekniklerinin kullanıldığı bilinmektedir.

Bilgi güvenliği kavramının en fazla önem kazanmaya başladığı ve geliştiği dönem Birinci ve İkinci Dünya Savaşı dönemleridir. Özellikle telsiz sistemlerinin haberleşmede yoğun olarak kullanımı, güvenli haberleşme ihtiyacını artırmıştır. Bu dönem, kriptolojinin öneminin ciddi olarak anlaşıldığı ve kriptolama tekniklerinin ciddi anlamda geliştiği dönemdir. Askeri sistemlerin yanında bankacılık gibi kritik alanlarda da modern kripto teknikleri bu dönemde kullanılmaya başlanmıştır.

Bilgisayarların kullanılmaya başlanması, internetin ve haberleşme araçlarının gelişimi ile birlikte günümüzde bilgi güvenliği artık bireyler, kurumlar ve devletler için en önemli ihtiyaçlardan biri haline gelmiştir. Ticari ve askeri savaşlar çoğunlukla bilgi casusluğu ve siber saldırılar üzerinden yürütülmeye başlanmıştır. Bu dönemle birlikte kriptoloji de önemli bir bilim dalı haline gelmiştir.

Bilgi güvenliğinde milli ve yerli yazılım / donanım kullanımının önemi ve kritik olduğu kısımlar hakkında bilgi verebilir misiniz?

Nasıl ki ülkemizin iç ve sınır güvenliğini yabancı ülkelerin asker ve polisine emanet etmiyorsak, ülkemizin bilgi güvenliğini de yabancı ülkelerden aldığımız cihaz ve sistemlerle sağlamayı düşünemeyiz. Çeşitli ülkelerle müttefik olsanız bile sonuçta doğal olarak herkesin önceliği kendi ülkesi olmakta, ülkesinin çıkarı neyi gerektiriyorsa o yönde hareket etmektedir. Zaman zaman medyaya da yansıyan olaylar göstermiştir ki NATO kapsamında birlikte hareket ettiğimiz ülkeler dahi, ülkemize sattıkları çeşitli cihaz ve sistemlerde oluşturdukları açıklıklar vasıtasıyla ülkemizin kritik kurumlarını yıllarca dinlemişlerdir. Ayrıca komponent düzeyinde satılan bir takım ürünlerde de zaman zaman kritik bazı açıklıklar tespit edilebilmektedir. Bu tip açıklıklar genellikle yazılım veya donanım hatası, yani "bug" olarak nitelendirilip geçiştirilebilmektedir.



Yine çok sık kullanıma sahip, hatta standartlaşmış, günlük hayatımıza dahi girmiş kriptografik bir takım ürünlerde, bir süre sonra kritik bir takım açıklıklar olduğu tespit edilebilmektedir. Doğrusu, bunları "bug" deyip geçiştirmek saflık olacaktır. Kısacası bilgi güvenliği kapsamındaki ülke ihtiyaçlarını, kritik donanım/yazılım bileşenlerinden kullandığınız sistemlere kadar kendiniz geliştirmediğiniz sürece, bilgi güvenliğinizi tam olarak sağlamanız mümkün olmayacaktır.

Çömlek yapımının şifreli olarak anlatıldığı çivi yazısı tablet

BİLGEM ve Kriptoloji

BİLGEM bilgi güvenliği alanında neler yapmaktadır? Kurumu bu açıdan ulusal ve uluslararası ölçekte değerlendirebilir misiniz?

NATO üyesi olduktan sonra, ülkemizde kritik kurumların bilgi güvenliği ürünleri, genelde NATO üyesi ülkelerden tedarik edilmeye başlandı. Savunma ihtiyaçlarımız için gerekli silah ve mühimmatlarımız da öyle. Ancak 1974 Kıbrıs Barış

> **Nasıl ki ülkemizin iç ve sınır güvenliğini yabancı ülkelerin asker ve polisine emanet etmiyorsak, ülkemizin bilgi güvenliğini de yabancı ülkelerden aldığımız cihaz ve sistemlerle sağlamayı düşünemeyiz.**

Harekât'yla birlikte uygulanan ambargo, bu anlamda bir dönüm noktası oldu. Aslında ambargolar, kısa vadede ülkemiz için zararlı gibi görünseler de uzun vadede bir uyanışa ve çözüm arayışlarına sebep olmuşlardır. Uygulanan bu ambargo da ülkemiz açısından savunma sanayimizin bir nevi doğuşu olmuştur. Bugün savunma sanayimiz gün geçtikçe gelişmektedir ve ihracat yapar hale gelmiştir.

Söz konusu ambargo, bilgi güvenliği açısından da ülkemiz için bir dönüm noktası olmuştur. BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nün temeli olan 1968 yılında kurulmuş TÜBİTAK Elektronik Araştırma Ünitesi (EAÜ)'ne, 1976 yılında ülkemizin ilk çevrim içi (on-line) kriptosunu geliştirme görevi verildi. İlk prototipleri 1978 yılında hazırlanan MİLON-I Kripto Cihazı, 1984 yılında 77 adet ilk grup teslimatı ile TSK envanterine girmiş oldu. Bu tarihten sonra 1995 yılına kadar MİLON-II ve MİLON-III Kripto Cihazları da geliştirilerek kullanıma sunuldu.

1994 yılında haberleşme alanında özel sektör Ar-Ge tecrübesine sahip bir grup araştırmacının EAÜ'de çalışmaya başlaması, EAÜ'nün 1995 yılında Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü adını alması ile kriptoloji ve bilgi güvenliği konusundaki çalışmalar hız kazandı. Bilgi güvenliğinin sac ayaklarından kripto analiz, COMSEC, TEMPEST ve EMI/EMC bölümlerinin kurulup faaliyetlere başlaması ile kripto cihazı geliştirme çalışmalarında büyük bir ivme yakalandı.

Bugün ülkemizin kritik kurumlarının tüm kripto cihaz/sistem ihtiyaçları, kağıt üstündeki tasarımdan, cihazın ilgili kurumlara teslimine kadar tüm faaliyetler BİLGEM bünyesinde gerçekleştirilebilmektedir. Hatta BİLGEM UEKAE bünyesinde bulunan Yarıiletken Teknolojileri Araştırma Laboratuvarı (YİTAL)'nda, kripto cihazlarımıza ilişkin kritik tümdevreler (çip) tasarlanıp üretilmekte ve cihazlarımızda kullanılmaktadır.

Geldiğimiz noktada uydularımızdan denizaltılarımıza kadar her platformda ve her tür haberleşme ortamında çalışan, Enstitümüz tarafından geliştirilmiş kripto cihazlarımız ülke güvenliğine hizmet etmektedir.

Bir zamanlar kripto kullanıcısı olduğumuz NATO'da da kripto üretici ülke konumuna gelmiş durumdayız. Her tür NATO gizlilik düzeyinde kullanılabilirlik onayı bulunan pek çok cihaz ve kripto algoritmamız mevcuttur. Bir takım cihazlarımız NATO tarafından da kullanılmaktadır. Bunun yanında daha önce sadece izleyici olarak katıldığımız NATO toplantılarında artık ülkemiz çıkarlarını gözetecek şekilde yön verici olarak rol alıyoruz.

NATO ve Rusya Federasyonu savaş gemileri arasında ilk kriptolu haberleşme, UEKAE tasarımı haberleşme ve kripto cihazları kullanılarak gerçekleştirilmiştir. Bu durum 2006 yılında NATO tarafından Kurumumuza gönderilen bir teşekkür mektubunda "tarihi olay" olarak nitelendirilmiştir.

Bilgi Güvenliği Testleri

BİLGEM, bilgi güvenliği kapsamında yazılım ve donanımlara ne tür testler uyguluyor? Bu testlerin içerikleri hakkında kısaca bilgi verebilir misiniz?

Bilgi güvenliği gereksinimi; kişiler, ticari kuruluşlar ve kritik devlet kurumları için farklı düzeylerdedir. Kişilerin bilgileri ile ilgilenenler, genellikle "hacker" diye adlandırılan bilgisayar korsanlarıdır. Bunların amacı elde ettikleri bilgilerle menfaat sağlamaktır. Bu grupların ellerindeki teknik olanaklar ve hareket alanları sınırlıdır.

Ticari kuruluşların bilgileri ile ilgilenenler genellikle ticari rakipleridir. Bunların sahip olduğu bu konuya ayırabilecekleri bütçe ve teknik yetkinlikler, sıradan bir bilgisayar korsanına oranla çok daha fazladır.

Devletlerin kritik kurumlarının GİZLİ, ÇOK GİZLİ gibi gizlilik içeren bilgileri ile ilgilenenlerse, genellikle yine diğer devletlerdir ve bu maksatla ayırabilecekleri bütçe ve teknik kapasitenin neredeyse sınırı yoktur. Bu maksatla uzaya uydu gönderebilir, denizaltılar, gemiler, uçaklar, insansız hava araçları kullanabilir, büyük dinleme tesisleri inşa edebilir, on binlerce farklı uzmanlık alanında insan çalıştırabilir ve sizin elinizdeki bilgilere erişebilmek ya da elde ettiği verileri kırmak, anlamlandırmak için büyük veri işlem kapasiteleri kullanabilirler.

Dolayısıyla bilgi güvenliği için kullandığınız cihaz/sistemler ile ne tür bir bilgiyi koruyacaksanız, cihaz tasarımında da o düzeye uygun tedbirler almalı ve cihazları bu düzeye uygun güvenlik testlerinden geçirerek sertifikalandırmalısınız. Bireylerin ihtiyaçları için geliştirilmiş ya da ticari güvenlik düzeyindeki bir cihazı, devletin GİZLİ bilgilerini korumak/iletmek için kullanırsanız çok ciddi bir hata yapmış olursunuz.

Ülkemizdeki duruma gelmeden önce NATO'dan örnek vermek gerekirse, NATO devreleri üzerinde kullanacağınız GİZLİ gizlilik ve üstü dereceli bilgi güvenliği ekipmanları/kripto cihazları, SECAN (Security and Evaluation Agency) tarafından test edilir ve NATO Askeri Komite tarafından ilgili gizlilik düzeyine göre onaylanır. Söz konusu onayı almamış hiçbir cihaz NATO devrelerinde kullanılamaz. Ülkemiz ve NATO'da kripto üreticisi ülke statüsünde bulunan diğer ülkelerin milli maksatla kullandıkları cihazları için de buna benzer milli bir test ve sertifikalandırma süreçleri vardır. Ülkemizde kritik kurumlarımızın kullanacakları cihazların testleri, BİLGEM Test ve Değerlendirme Başkan Yardımcılığı altında bulunan birimlerce yapılır. Onay makamı ise cihaz kullanıcısı makamlar olur.

Milli maksatla kullanılacak bir kripto cihazının tasarımında kullanılan hemen her türlü bileşen ve en nihayetinde cihaz, bir bütün olarak çok sıkı güvenlik testlerinden geçirilir. Burada uygulanan testlerin sıkılığı, cihazların koruyacağı bilgilerin güvenlik düzeylerine göre farklılık gösterir. Ülkemizde genellikle HİZMETE ÖZEL, ÖZEL, GİZLİ, ÇOK GİZLİ gibi güvenlik düzeyleri kullanılır. Cihaz tasarım ve testlerinde en sıkı kurallar GİZLİ düzeyinde uygulanır. ÇOK GİZLİ gizlilik düzeyi birkaç kripto işlemi kullanılarak sağlanır.

Cihazda kullanılan güvenlik bileşenleri, rasgele sayı üreteçleri, kripto algoritmaları, kriptografik protokoller, anahtar yönetimi (dağıtım, yükleme, saklama) protokolleri ayrıntılı olarak teste tabi tutulur. Cihaz bazında da EMI/EMC (Electromagnetic Interference/Electromagnetic Compatibility), TEMPEST, COMSEC (Communications Security) testleri yapılır.

Cihaz bazında uygulanan testler hakkında kısaca bilgi verecek olursak, günümüzde hemen her elektronik cihazın bir takım EMI/EMC standardına uyması beklenir. Böylelikle hem cihazın yaydığı elektromanyetik dalgaların diğer cihazları ve insanları etkileyecek düzeyin altında olmasına, hem de çeşitli ortamlarda oluşan elektromanyetik dalgaların cihazın çalışmasını etkilememesine çalışılır. Bu tip testler hemen her elektronik cihaz için yapılır ancak kripto cihazlarında güvenlik gereklerinden dolayı bu standartlar, normalden çok daha sıkı koşullar içerir. Dolayısıyla cihaz tasarımında da bu durumu göz önünde bulundurmak gerekir.

MİLON-I: Ülkemizin ilk çevrimiçi (on-line) kripto cihazı

IPKC-GX: 10 Gb/sn hızında çalışan IP Kripto Cihazı

MİLSEC-4: Emniyetli ses ve görüntülü konuşma için kullanılan VoIP (Voice over IP) Kripto Cihazı

GÖKTÜRK-1: İstihbarat Uydusu Kriptosu

Kuantum Rasgele Sayı Üreteci (RNG-Random Number Generator)

Enigma: İkinci Dünya Savaşı'na her yönüyle damga vurmuş olan Alman Kriptosu

Özellikle askeri ve kritik kurumların kullandıkları kripto cihazlarında olması gereken bir diğer önemli özellik ise çeşitli TEMPEST koşullarını sağlamasıdır. TEMPEST kısaca, cihazdan istem dışı ışıma ya da iletkenler (güç hattı, haberleşme bağlantıları v.b.) yoluyla bilgi kaçağını tanımlamaktadır. Cihazın içinde işlenen, henüz şifrelenmemiş GİZLİ bilgi ve şifrelemede kullanılan kripto anahtarları gibi kritik bilgilerin korunması gerekir. Bu bilgilerin istem dışı olarak cihaz dışına çıkmayacağı güvence altına alınmalıdır. Buna cihazın sağlaması gereken TEMPEST standartları ile test edilerek ulaşılır.

COMSEC testlerinde ise, bilgi güvenliği ürünü, tasarım ve gerçekleme yönteminin, milli COMSEC kriterlerine uygunluğu test edilir. COMSEC testi sonucunda, belli bir gizlilik seviyesindeki bilgi güvenliği ürününün sahada karşılaşabileceği "kurcalama, çalınma, hata yaratma, yan kanal analizi ve protokol saldırıları" gibi tehditlere karşı, hangi güvenlik seviyesinde koruma sağlayabildiğinin değerlendirmesi yapılmış olur.

İkili Dijital Sistem ve Kuantum Bilgisayarlar

Dijital dönüşüm sürecinden geçtiğimiz bu dönemde, bilgi güvenliği daha da önemli hale geldi. Bu dönüşümün, avantajlar yanında bilgi güvenliği açısından getirdiği tehditler nelerdir? Alanda yapılan çalışmalar hangi yöne doğru ilerlemektedir, trendler nelerdir?

Dijital (sayısal) sistemlerin temeli 0 ve 1 rakamları ile ifade edilen ikili sayı sistemidir. Bu sayı sistemi yüzyıllardır biliniyordu. 1947 yılında transistorun bulunması, ardından tümdevrelerin (chip) geliştirilmesi ve ikili sistemin elektronik devrelerde kullanımının kolaylığı ile sayısal elektronik devreler geliştirilmeye başlandı. Bu gelişim, tarihte hiç görülmediği kadar hızlı oldu. Bilgisayarların gelişimi, internet, mobil-otonom sistemler derken bugün her şeyi internete bağlayıp birbirleriyle ve kullanıcılarıyla iletişime geçmesini, nesnelerin internetini (IoT – Internet of Things) konuşuyoruz.

Tüm bu gelişmeler insanlığın bir nesli boyunca gerçekleşti ve bu gelişim, hayatımızın her aşamasına yansıdı. Veri işleme, depolama ve iletişim her açıdan çok kolaylaştı. Artık insan müdahalesi olmadan çalışan fabrikalardan, otonom araçlardan, kendi kendine karar verebilen ve eğitebilen akıllı sistemlerden bahseder olduk. Bu baş döndürücü gelişmeler, hayatımızı çok kolaylaştırdı ve yaşamımızın birer parçası haline geldi.

Elbette bu hızlı gelişim, içinde pek çok tehdit de barındırıyor. Bilgi güvenliği açısından bu tehditlere bakarsak; bu tip sistemleri tasarlarken, bilgi güvenliğinin nasıl sağlanacağını da değerlendirip sistem tasarımını bir bütün olarak oluşturmamız gerekiyor. Geliştirilmiş bir sistemin daha sonra yapılacak eklemelerle bilgi güvenliğini sağlamaya çalışmak, çok da verimli ve etkili olmayabiliyor. Modern sistemlerde artık bu durum göz önünde bulundurulmaya çalışılıyor. Otonom sistemlerin ve internete bağlı makinaların ele geçirilmesine veya çeşitli ataklarla çalışmasının durdurulmasına, mobil iletişim sistemleri üzerinden yaptığımız görüşmelerin dinlenmesine engel olmak için çeşitli tedbirler alınıyor ve bunlar standartlara dâhil ediliyor.

Ancak tüm bu sistemler için bilgi güvenliği kapsamında alınan tedbirler, kişisel ve belki bir yere kadar ticari bilgilerin güvenliğini sağlayabilecek düzeydedir. Aslında bu durum bile tartışmalıdır zira bir takım hacker gruplarının bile bu tip sistemlerdeki güvenlik tedbirlerini kolaylıkla aşabildiğini görüyor ve biliyoruz. Dolayısıyla dijital dönüşümün getirdiği tüm bu nimetlerden faydalanırken özellikle kritik kamu kurumlarımızın bilgi güvenliğini sağlamak için milli olarak geliştirilmiş bilgi güvenliği sistemleri kullanmamız gerekmektedir. Söz konusu tedbirlerin bir bütün olarak tasarlanması hem uygulama ve maliyet hem de kullanım kolaylığı açısından çok daha uygun olmaktadır.

İkili sistemin (dijital) elektronik devrelerde ve yaşamımızda yaptığı değişimin benzerini şimdi kuantum sistemlerinin gelişiminde görmek üzereyiz. Klasik bir bilgisayar, ikili sistemle çalışıp aynı anda 1 ya da 0 (bit) kullanıp tek bir işlem yapabilirken, kuantum bilgisayarlar kübit (qubit) kullanır; kübitler 1, 0 olabilirken aynı anda hem 1 hem de 0 olabilir. Bu, kuantum bilgisayarları ile aynı anda birden fazla işlem yapabilmemize ve işlem gücümüzün muazzam bir şekilde artmasına imkân sağlamaktadır. Kuantum bilgisayarlar gelişim aşamasında ve henüz hayatımıza girmeye başlamadı. Bu olduğunda, dijital sistemler gibi bir dönüm noktası oluşturacaktır.

Kuantum bilgisayarlar bu haliyle müthiş bir gelişim sunsa da tedbirli olmaz isek bilgi güvenliği anlamında ciddi tehditler de barındırmaktadır. Bilgi güvenliğini sağlamak için kullanılan bir takım asimetrik algoritmalar ve bu algoritmaları kullanan kriptografik protokoller kırılabilir hale gelebilir. Günümüz teknolojisi ile kırılamayan ve dolayısı ile güvenli olarak kabul ettiğimiz iletişim kanalları kaydedilip ileride kuantum bilgisayarlarla çözülmek üzere saklanabilir. Bu nedenle özellikle ülke güvenliği için kullandığımız bilgi güvenliği sistemlerinin şimdiden kuantum hesaplamaya dayanımlı hale getirilmesi gerekmektedir.

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü olarak uzunca bir süredir kuantum hesaplamaya dayanımlı kripto algoritma ve bu algoritmaları kullanan kripto protokolleri geliştirme konusunda altyapı ve bilgi birikimi oluşturmaya çalışıyoruz. Son dönemlerde tasarladığımız cihazlarımızda kuantum hesaplamaya dayanımlı algoritmalar ve protokoller kullanıyoruz. Sahada halen çalışan cihazlarımızda da buna ilişkin güncellemeler yapıyor, kuantum bilgisayarlar ülke güvenliğimiz için tehdit oluşturmaya başlamadan önce tedbirlerimizi alıyoruz.

Ulusal Bilgi Güvenliği Otoritesi

Bilgi güvenliği çözümlerinde ülkemizdeki mevcut durum ve gelişimi gerekli alanlarla ilgili görüşleriniz nelerdir?

Kritik kurumlarımızın bilgi güvenliğini sağlamak için kullanacağımız bilgi güvenliği sistemlerinin üst düzeyde güvenlik özelliklerine sahip olması gerekmektedir. Bu tür cihaz/sistemlerin geliştirilmesi için elektronik tasarım, yazılım, mekanik tasarım, rasgele sayı üreteçleri, TEMPEST, EMI/EMC, COMSEC, kripto algoritma/protokol tasarım gibi alanlarda uzmanların bir arada uyum içerisinde çalışması gerekmektedir.

Tasarlanan cihazların işletim koşullarını test etmek için de çevresel ve işlevsel test altyapılarının sağlanması gereklidir. Ayrıca geliştirilmiş olan sistemlerin güvenlik testlerinin de tam olarak yapılabilmesi için kripto analiz, rasgele sayı üreteçleri analizi, TEMPEST, EMI/EMC, COMSEC test laboratuvarlarına ihtiyaç vardır. Ancak tüm bu uzmanlık alanlarını oluşturduğumuzda ulusal ve uluslararası (NATO) standartlarına uygun bilgi güvenliği cihaz/sistemleri geliştirmek mümkün olmaktadır.

Kurumumuz uzun yıllar boyunca elde ettiği tasarım deneyimi ve seçkin altyapısı ile ülkemizin kritik kurumları ve NATO için kripto cihazları tasarlamakta, güvenlik testlerinden ve onaylardan geçirerek kullanıma sunmaktadır. Ülkemizin ihtiyacı olan her türlü bilgi güvenliği sisteminin, kâğıt üstü tasarımdan cihaz haline dönüşmesi evresine kadar geçen tüm aşamalar için gerekli yetkinliğimiz mevcuttur.

Ülkemizdeki bilgi güvenliği farkındalığına gelirsek, bu kapsamda kimi kurumlarımız çok hassas ve bilinçli bir şekilde konuya önem vermekte ve kurum içi tedbirlerini buna göre almaktadır. Bu kurumların talep ettikleri çözümler sayesinde, ülkemizde milli bilgi güvenliği ürünleri çeşitlenebilmektedir. Ancak bu farkındalık, tüm kurumlarımız için aynı düzeyde değildir. Bazı kurumlarımız, bu kapsamda alınması gerekli tedbirlere çok fazla önem vermeden faaliyetlerini sürdürmeyi tercih edebilmekte, ya da ticari kullanım maksadıyla geliştirilmiş kimi yerli ya da yabancı bilgi güvenliği ürünlerini kullanarak güvenlik tedbiri almaya çalışmaktadır. Bu yaklaşım, ülkemizde bütüncül bir bilgi güvenliği anlayışı oluşturulmasına katkı sunmamaktadır.

> **"Ülkemizde kritik kurumlarımızın kullanacakları cihazların testleri, BİLGEM Test ve Değerlendirme Başkan Yardımcılığı birimleri tarafından yapılmaktadır."**

Doğrusu burada temel sorun olarak, ülkemizde bilgi güvenliği kapsamında uygulanacak kuralları belirleyip uygulamayı takip edecek tek bir otorite olmamasını görüyorum. Konuya önem veren kurumlarımız kendi içlerinde uygulanacak kuralları belirleyip kurum içerisinde titizlikle uygulanmasını sağlamakta, ancak farklı kurumlarda farklı uygulamalar olması sebebiyle bütüncül bir yaklaşım oluşamamaktadır. Ülkemizde, belli başlı ülkelerde de örnekleri bulunan, bir bilgi güvenliği otoritesinin oluşturulmasının faydalı olacağını değerlendiriyorum.

Ofis Dışında Verimli ve Güvenli Çalışma

TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE) tarafından, Dijital Olgunluk Değerlendirme Modeli kapsamında "İşletim ve Bakım: Uzaktan Çalışma Rehberi" hazırlandı.

Fatih Koç – Araştırmacı, Emre Gül – Uzman Araştırmacı, Yasin Karapınar – Uzman Araştırmacı / BİLGEM YTE

Dizüstü bilgisayarlar, akıllı telefonlar veya video konferans yazılımları gibi giderek yaygınlaşan iletişim araçları sayesinde, çalışanlar neredeyse her yerde ve zamanda işlerini sürdürebilme imkânı bulmaktadır. Teknolojinin gelişmesiyle beraber, pek çok kurumsal faaliyet yalnızca ofis alanlarında değil, ofis dışındaki alanlarda da rahatlıkla yürütülebilmektedir. İster evde veya ulaşım aracında olsun, ister müşterinin yanında, uzaktan çalışma modeli, mesai saati, çalışma alanı ve görev dağılımına kadar iş hayatımızda yer alan birçok tanımı değiştirmektedir.

Teknik altyapıları, insan kaynakları, politika ve prosedürleri ile iş yapış şekilleri bakımından uzaktan çalışma modeline uyumluluk gösteren organizasyonlar, bu modeli uygulamada daha güvenli ve başarılı bir yerde konumlanmaktalar. Ayrıca müşteriler, tedarikçiler ve iş ortakları gibi diğer paydaşların da uzaktan çalışma modeline gösterdikleri uyum, modelin güvenliğini ve başarısını etkilemektedir. Paydaşların bu modeli uygularken yaşadıkları sorunlar veya iş yapış şekillerinden kaynaklanan bir takım doğal kısıtlar, uzaktan çalışma modeline geçiş sürecini olumsuz etkileyebilir. Bazı sektörlerin yapısı gereği bu modeli uygulaması mümkün olmayabilir.

Uzaktan çalışma modeli ile birlikte iletişim altyapısına olan ihtiyaç artmaktadır, buna paralel olarak bilgi güvenliği riskleri de artış göstermektedir. Birçok kurum ve kuruluş uzaktan çalışma için istekli olsa bile, çok azı uygun bilgi güvenliği politikalarına ve altyapısına sahiptir. Kimlik avı dolandırıcılığı, Dağıtılmış Hizmet Reddi (Distributed Denial Of Service, DDOS) atakları, hassas bilginin ifşasına neden olan saldırılar ya da farklı yöntemlerle mevcut sistem açıklarından faydalanan saldırganlar; işlerini uzaktan sürdüren çalışanları herhangi bir açık ağ üzerinden hedef alabilmektedir.

İşlerin uzaktan yürütülmesi esnasında tüm bu saldırı ve risklere karşı önlem alınabilmesi ve bilgi teknolojileri altyapısının ve barındırılan verilerin bilgi güvenliği gereksinimlerinin karşılanabilmesi için kuruma ait iş modeli, süreç ve politikaların uzaktan çalışma modeline uygun olarak hazır hale getirilmesi gerekmektedir.

Uzaktan çalışma esnasında kullanılan bilgi teknolojisi (BT) sistemleri, çalışma ortamları, altyapıları, yazılımlara özgü gereksinimler ve yasal sorumluluklar gibi BİLGEM YTE tarafından hazırlanan Uzaktan Çalışma Rehberi'nin öne çıkan içerikleri aşağıda listelenmektedir.

Uzaktan çalışmanın usul ve esasları: Uzaktan çalışmada kurum dışına çıkarılan taşınabilir bilgi teknolojisi sistemleri ile ilgili düzenlemelerin, mutlaka yapılması gerekmektedir. Bu kapsamda, hangi bilgi varlıklarının kimler tarafından kurum dışına çıkarılabileceği, kurum dışına çıkarılan bu bilgi varlıkla-

> BİLGEM YTE tarafından hazırlanan Uzaktan Çalışma Rehberinde, uzaktan çalışma ile ilgili gereksinimler, alınması gereken tedbirler, yapılması gereken kontroller ve güvenli uygulama örnekleri yer alıyor.

rıyla ilgili temel güvenlik gereksinimlerinin ne olacağı belirlenmelidir. Kurum dışına çıkarılan bilgi varlıklarının kim tarafından ne zaman çıkarıldığı kayıt altına alınmalıdır.

Uzaktan çalışan personelin bilinçlendirilmesi: Uzaktan çalışma yapacak bütün çalışanlar, taşınabilir BT cihazlarının doğru kullanımı hakkında düzenli olarak bilgilendirilmelidir. Bu kapsamda çalışanlara, uyması gerekli güvenlik önlemleri ile ilgili eğitimler verilmelidir. Kurallar açık ve anlaşılır bir şekilde belgelenmeli ve uzaktan çalışma yürütecek tüm çalışanlarla paylaşılmalıdır.

Güvenlik ve erişim kontrolü: Ofis dışında çalışan personel, uzaktan çalışma alanında oluşabilecek hırsızlık veya erişim koruması ile ilgili önlemler hakkında bilgilendirilmelidir. Çalışma alanı boşaltıldıktan sonra çalışma alanın kapıları kilitlenmeli böylece yetkisiz kişilerin oda içerisinde yer alan belgelere ve BT bileşenlerine fiziksel erişimi önlenmelidir.Çalışanın bu uygulamaya uyumluluğu belirli aralıklarla kontrol edilmelidir.

Uzaktan çalışma ortamının güvenlik politikası: Uzaktan çalışma modelini uygulayan organizasyonlar, modelin ilgili tüm güvenlik gereksinimlerini kapsayan bir politika hazırlamalı ve bu modelde çalışan personele, gereksinimleri uygulama zorunluluğu getirmelidirler. Bu politika, kurumun güvenlik gereksinimleri ile ilgili tüm uzman bölümler ile koordineli hazırlanmalı ve düzenli olarak güncellenmelidir. Kurum çalışanları, mevcut güvenlik politikalarına ek olarak uzaktan çalışmayla ilgili güvenlik politikasından haberdar edilmeli ve bu kapsamda çalışanlara eğitimler verilmelidir.

Taşınabilir bilgi varlıklarının şifrelenmesi: Hassas bilgilere, yetkisiz üçüncü taraflarca erişimin engellenmesi veya görsel hırsızlığın önlenmesi için prosedür, talimat ve kılavuzlar oluşturulmalıdır. Hassas bilgiler içeren BT sistemleri veya veri taşıyıcıları mümkünse tamamen şifrelenmelidir. Şifreleme anahtarları şifrelenmiş aygıttan ayrı bir ortamda tutulmalıdır.

Kurum ağına güvenli uzaktan erişim: Uzaktan çalışan kullanıcıların kişisel cihazları ile kurum ağına bağlanması gerektiği durumlarda, şifrelenmiş güvenli bağlantı oluşturulmadan önce, bağlantı için kullanılacak cihazda anlık güvenlik denetimleri yapabilen Sanal Özel Ağ (Virtual Private Network, VPN) uygulamaları tercih edilmelidir. VPN uygulamaları, kullanıcının kimlik doğrulamasını ve yetkilendirmesini yaptığı gibi kullanılan cihazın (güncel virüsten koruma yazılımının yüklü olup olmadığı, işletim sisteminin güncel olup olmadığı gibi) asgari güvenlik gereksinimlerini sağlayıp sağlamadığını da kontrol edebilmelidir.

Veri yedekleme: Çalışanlar, yerel olarak depolanan verilerin yedeklerini almakla yükümlü tutulmalıdır. Buna ek olarak, daha yüksek erişilebilirliğin sağlanabilmesi için çalışanlar, kullandıkları cihazlarda tutulan kurumsal verileri ve yedekleri belirli aralıklarla kurum sunucularına yüklemelidir.

Bilgi varlığının kaybolması veya çalınması: Ofis dışında çalışanlar, BT cihazları veya veri taşıyıcılarını kaybettiklerinde, ivedilikle kurumlarını bilgilendirmelidir. Kurumun ilgili prosedüründe bu süreç açık ve net bir şekilde düzenlenmeli ve irtibat noktası belirlenmelidir.

Harici BT sistemleri ve ağlarıyla çalışma: Kurum ve kuruluşlar, ortak kullanım alanlarında bulunan ve üçüncü taraflarca yönetilen harici BT sistem ve altyapılarının kullanımıyla ilgili düzenlemeleri yapmalıdır.

> Koronavirüse karşı iş kaybının oluşmamasına yönelik çözüm olarak uygulamaya konulan uzaktan çalışmanın, salgın sonrasında bazı meslekler için kalıcı hale gelebileceği öngörülüyor.

Bu tür sistem ve alt yapıların güvenlik koruma seviyesi, kurumun sahip olduğu güvenlik seviyesinden farklı olabileceğinden, kullanıcılar bu sistem ve altyapıların kullanımı ile ilgili düzenlemelere uymalı ve bu hizmetlerden sadece gerekli düzeyde faydalanmalıdır.

Hassas bilgilerin imha edilmesi: Uzaktan çalışma esnasında kullanılan hassas veriler güvenli bir şekilde silinmeli, imha edilmeli veya en azından anonim hale getirilmelidir. Ömrünü bitiren veya arızalanmış veri taşıma ortamları ve belgeler atılmadan önce, hassas bilgiler içerip içermedikleri kontrol edilmelidir. Mümkünse, hassas bilgiler içeren veya içerdiği düşünülen materyallerin imhası kurum içerisinde gerçekleştirilmelidir.

Uzaktan çalışmayla ilgili yasal düzenlemeler: Uzaktan çalışmaya ilişkin iş hukukunda ve iş güvenliğinde yer alan hükümler gözetilerek kurumun ilgili prosedürleri güncellenmelidir. Ayrıca, çalışanla yapılan veya diğer bağlayıcı sözleşmelerde yer alan ve ileride fikir ayrılığına neden olabilecek tüm hususlar açık bir şekilde düzenlenmelidir.

Bulut bilişim ortam güvenliği: Kurum ve kuruluşlar, uzaktan çalışma modelleri için hazırladıkları politikalarda bulut bilişim gereksinimlerini tanımlamalı ve bu gereksinimlere uygun güvenlik yöntemlerini ayrıntılı bir şekilde belirlemelidir.

Uzaktan Çalışmada Artan Güvenlik Olayları

Oltalama e-postaları: Kurum dışı alanlarda çalışanlar, oltalama e-postalarında bulunan linkler aracılığıyla yönlendirilen sahte sayfalara daha çok maruz kalırlar. Bu yol ile saldırganlar, çalışanları istedikleri sayfaya yönlendirmekte ve kişisel bilgiler saldırganların eline geçmektedir.

Zararlı alan adları: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin araştırmasına göre Koronavirüs salgını ile ilgili 4000 tane alan adının alındığı ve bunların 320'sinin zararlı web siteleri olduğu görülmüştür. Ulusal Siber Olaylara Müdahale Merkezi (USOM) zararlı alan adları listesinde ise 100'den fazla alan adının Koronavirüs ile ilgili sözcükler içerdiği görülmüştür. Bu alan adlarının özellikle Türkiye'de yaşayan kişileri ve kurumları hedef alması önemli bir noktadır. Aynı şekilde yabancı dillerde de dolandırıcılık amacıyla alan adlarının alındığı görülmektedir.

Android casus yazılımları: Benzer şekilde Korona virüs salgını döneminde hastalıklarla ilgili istatistiksel bilgiler sağlayan zararlı bir uygulamanın Google Play Store harici kaynaklardan dağıtıldığı görülmüştür. John Hopkins Üniversitesi tarafından hazırlanan Koronavirüs haritasındaki bilgileri kullanıcılara yansıtan uygulama, arka planda SpyMax adlı uzaktan yönetim aracını (RAT) barındırmaktadır. Yapılan detaylı araştırmada benzer şekilde Koronavirüs temalı ve benzer yapıda Android uzaktan yönetim araçları barındıran birden fazla uygulama olduğu belirlenmiştir.

Video konferans uygulamaları: Uzaktan çalışma modelinde internet üzerinde görüşme ihtiyacının artmasıyla beraber video konferans uygulama kullanımı yaygınlaşmıştır. Bu tür iletişim uygulamalarına olan yoğun talebi gören saldırganlar, uygulamaları yeniden paketleyerek kötü amaçlı yazılımlarını yaymak için kullanmaktadır. Genellikle reklam geliri elde etmek amacıyla yapılan bu saldırılar, kullanıcıların gizliliğini tehlikeye atmaktadır.

BİLGEM YTE Uzaktan Çalışma ve Dijital Kabiliyet Rehberleri

Uzaktan çalışma her ne kadar 4857 sayılı İş Kanunu'nda yapılan değişiklikler sonucu düzenlenmiş olsa da özellikle Covid-19 salgını sonrası daha çok uygulama alanı bulmuştur. Kurum ve kuruluşların yerleşik çalışma alanları için oluşturdukları güvenlik kontrollerinin uzaktan çalışma ortamlarında da uygulanması ayrıca daha önemli hale gelmiştir. Uzaktan çalışma dijital kabiliyetine yönelik olarak BİLGEM Yazılım Teknolojileri Enstitüsü tarafından hazırlanan Uzaktan Çalışma Rehberi'nin, kurum ağına güvenli uzaktan erişim, harici sistemler ile çalışma, veri yedekleme, taşınabilir bilgi varlıklarının şifrelenmesi, bulut bilişim ortam güvenliği, uzaktan çalışma ile ilgili yasal düzenlemeler gibi seviyelendirilmiş içeriklerinin referans alınması, bu çalışma yöntemini kullanan kurumların daha verimli ve güvenli şekilde çalışması için yardımcı olacaktır.

TÜBİTAK BİLGEM YTE tarafından hazırlanan Dijital Kabiliyet Rehberleri kullanılarak, kurumların dijital dönüşüm ihtiyaçları doğrultusunda eğitim ve rehberlik hizmeti sunulmaktadır. Ülkemiz koşul ve ihtiyaçlarını göz önünde bulunduran, uluslararası çalışmaları dikkate alan rehberler ile kurumların dijital olgunluğu ve çalışan yetkinliğinin artırılması ve bu sayede dijital kurumsal kapasitenin geliştirilmesine katkı sağlanması amaçlanmaktadır. Rehberlerin, etkinlik ve bilgi güvenliğine yönelik dikkate alınması önerilen unsur ve alternatifler ile birlikte bilgi ve yönlendirmeler de yer almaktadır. . Rehberlerin www.dijitalakademi.gov.tr'den açık erişimi sağlanmaktadır.

Uzak Erişim Güvenliğinde Milli Çözüm

Milli VPN

> Milli VPN çözümü, TÜBİTAK-BİLGEM tarafından geliştirilmiş ve kullanıma sunulmuştur.

Muttalip Tulgar - Başuzman Araştırmacı / BİLGEM İGBY

Yeni Koronavirüs (COVID-19) kaynaklı küresel salgın, hayatın her alanında önemli değişikliklere neden olmuştur. Salgınla mücadelede ön plana çıkan sosyal mesafe kavramı ile çalışma şartları yeni bir boyut kazanmış, mekân bağımlılığı ortadan kalkarak uzaktan veya evden çalışma modeli daha da önemli bir hal almıştır.

Salgın hızlı bir şekilde dijital dönüşümü de adeta zorunlu hale getirmiştir. Bu dijital dönüşüm, siber uzayın taşıdığı tehdit ve riskleri de artırarak yeni saldırı yüzeylerinin ortaya çıkmasına neden olmuştur. Özellikle uzaktan çalışma modelinde mobil cihazların ve iletişim kanallarının şifreli olmaması veya şifrelemenin milli kripto çözümleri ile sağlanmaması, ulusal bilgi güvenliği açısından da önemli sorunları beraberinde getirmiştir.

Bu tür tehditleri bertaraf etmek için uç nokta güvenliği, ağ güvenliği ve iletişim güvenliği için Kamunun ve özel kurumların, Millî Açık Anahtar Altyapısı (MA3) [1] gibi tamamıyla yerli ve milli kriptografik çözümler kullanmaları, gizlilik dereceli haberleşmelerini yerli ve milli kripto sistemleri ile geliştirilen güvenli ağ cihazları (AGC) [2] üzerinden gerçekleştirilmeleri önem arz etmektedir.

Kurum ağlarına uzaktan erişimde en çok tercih edilen yöntem VPN (Virtual Private Network) [3] teknolojisidir. Bu yöntem ile kullanıcının, internet üzerinden iki nokta arasında sanal özel ağ oluşturarak bağlantı kurmak istediği uzak noktadaki sunucu veya kaynağa erişmesi güvenle sağlanmaktadır. VPN, İnternet ortamında kriptolu bir tünel açarak içinden iletilen bilginin şifreli olarak taşınmasını sağlar. Bu şifreli ağ trafiğinin içeriği dışarıdan görüntülenemez olup sadece kimlik bilgileri kontrol edilip doğrulanan kullanıcılar, uzaktaki sunucuyla iletişime geçebilmektedir.

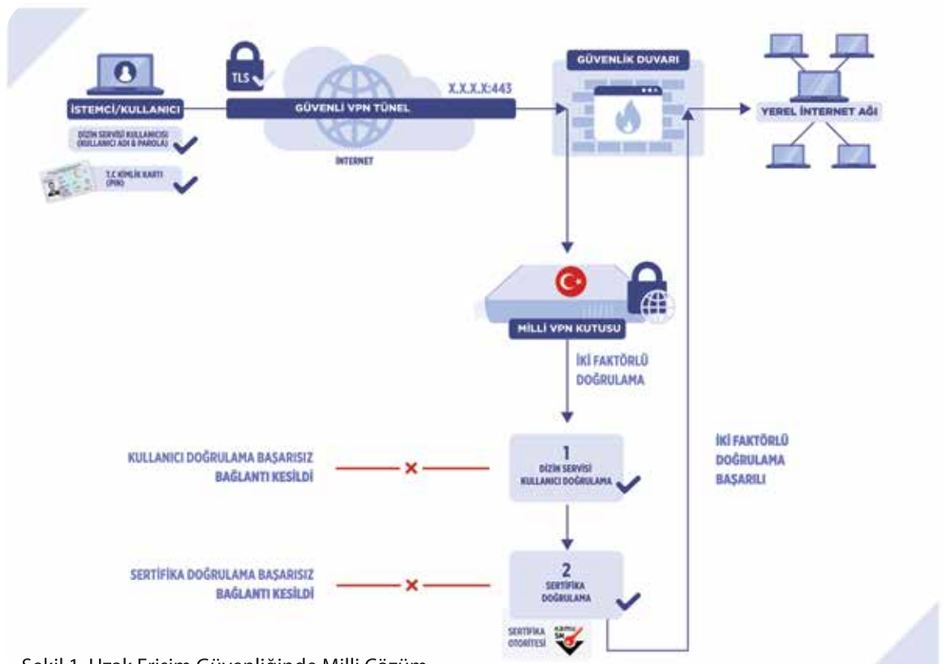
VPN her ne kadar uzak erişim konusunda güvenli bağlantı imkânı sunsa da, kurum kaynaklarına açılan arka kapı olma özelliğiyle bazı güvenlik riskleri de içermektedir. Normal şartlarda birçok fiziksel ve çevresel güvenlik önlemlerinin alınarak sağlandığı kurum bilgi varlıklarının mahremiyeti, uzaktan erişim yöntemi ile basit bir kullanıcı adı ve parola ile bir anda ortadan kalkabilmektedir. Bu yüzden basit parolalar ve bilgi güvenliği farkındalığı yeterli seviyede olmayan kullanıcılar, uzaktan erişimin en ciddi güvenlik risklerinin oluşmasına neden olmaktadır.

Bu tür riskleri azaltmak için VPN erişimlerinde 2FA (Two-factor Authentication) veya MFA (Multi-factor Authentication) yani iki faktörlü veya çok faktörlü kimlik doğrulama teknolojilerinin devreye alınması gerekmektedir. MFA, kullanıcıların belirli bir bilişim sistemine erişirken kimlik doğrulama için iki ya da daha fazla kanıt sağlayarak erişimin gerçekleştiği bir yöntemdir. [4] Çok faktörlü kimlik doğrulama unsurları şunları içermektedir: Kullanıcının bildiği bir şey, kullanıcının sahip olduğu bir şey ya da kullanıcının olduğu (biyometrik veri) bir şey.

2FA / MFA teknolojisi ile sağlanan VPN bağlantılarında, basit ve tahmin edilebilir parola kullanımlarından kaynaklanan parola gizlilik ihlalleri, tek başına sistemleri ele geçirme adına yeterli olmayıp ikinci veya üçüncü kimlik doğrulama yöntemleri de saldırganlar tarafından aşılması gereken bir engel olarak ortaya çıkmaktadır. Böylelikle uzak erişim güvenliğinde çok katmanlı koruma ile saldırganların işleri daha da zorlaşmaktadır.

Milli VPN

Milli VPN çözümü, TÜBİTAK-BİLGEM tarafından geliştirilmiş ve kullanıma sunulmuştur. Şekil 1'de kurumların yerel internet ağındaki kaynaklara uzaktan güvenli olarak erişebilecekleri milli VPN



Şekil 1. Uzak Erişim Güvenliğinde Milli Çözüm

çözümü gösterilmektedir. VPN bağlantıda erişim güvenliğinin iki faktörlü doğrulama ile sağlandığı bu modelde, internet yerel ağına dışarıdan erişecek her kullanıcı, dizin servisinde var olan kullanıcı adı ve parola bilgisini kullanmaktadır. Kullanıcı, bu ilk aşamada iki faktörlü kimlik doğrulamanın unsurlarından olan "kullanıcının bildiği bir şey" olarak kullanıcı adı ve parola bilgisinin güvenliğini de sağlamakla sorumludur.

Uzak erişim sırasında kullanıcının dizin servisindeki kullanıcı adı ve parola bilgisini doğru girmesi durumunda, iki faktörlü kimlik doğrulamanın ikinci aşamasına geçilir. Bu aşamada iki faktörlü kimlik doğrulamanın bir diğer unsuru olan "kullanıcının sahip olduğu bir şey" olarak T.C. Kimlik Kartı devreye girer. İkinci aşamada kullanıcının bir kimlik sertifikasına sahip olduğu ve sertifikanın geçerli olup olmadığı doğrulanır. VPN servisi, bu aşamada T.C. Kimlik Kartı ile iletişim kurar ve kimlik kartının PIN kodunu ister. Eğer girilen PIN kodu doğru ise T.C. Kimlik Kartı içerisindeki sertifikanın geçerli olup olmadığı, gerçek zamanlı olarak internet üzerinden sertifika otoritesine yapılan OCSP (Online Certificate Status Protocol) sorgusu ile kontrol edilir.

T.C. Kimlik Kartı içerisindeki sertifika geçerli ve aktif ise sertifika sahibinin T.C. kimlik numarasının, dizin servisindeki kullanıcı adında tanımlı T.C. kimlik numarası bilgisi ile eşleşip eşleşmediği kontrol edilir. Eğer bu eşleşme de başarılı olursa, kullanıcı kurumun kullandığı güvenlik duvarına (firewall) yönlendirilerek, kurum tarafından belirlenen güvenlik politikaları ve erişim yetkileri kapsamında yerel internet ağına güvenle erişmesi sağlanır.

Özellikle kamu kurumlarında hâlihazırda güvenlik nedeniyle internete açık olmayan bazı kapalı ağların yapısı, salgın sonrası uzaktan çalışma gerekliliği ile yeniden ele alınmaktadır. Ağların gizlilik seviyeleri yeniden değerlendirilmekte ve uzaktan çalışmaya uygun olacak şekilde kurum bilgi varlıkları dikkatlice gözden geçirilmektedir.

Bu hassas dönemde, uzaktan çalışma ve uzaktan erişim güvenliği de ulusal bilgi güvenliği açısından bir önem kazanmıştır. Bu bağlamda, uç nokta güvenliği, ağ güvenliği ve iletişim güvenliği alanlarında ulusal siber güvenlik ekosisteminin yaygınlaştırılarak yerli ve milli çözümlerin kullanılması neredeyse zorunlu hale gelmiştir.

KAYNAKÇA
1. https://ma3.bilgem.tubitak.gov.tr/
2. https://bilgem.tubitak.gov.tr/tr/icerik/agc-g-gigabit-ag-guvenlik-cihazi
3. https://en.wikipedia.org/wiki/Virtual_private_network
4. https://en.wikipedia.org/wiki/Multi-factor_authentication

TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

Sanal Siber Güvenlik Laboratuvarı

Sanal Siber Güvenlik Laboratuvarı ve Tatbikat Altyapısı; siber güvenlik alanında nitelikli insan gücü geliştirmek, yurtdışı bağımlılığı azaltmak ve açık kaynak ekosistemini desteklemek için geliştirilen bulut temelli bir altyapıdır. BİLGEM Siber Güvenlik Enstitüsü tarafından geliştirilen bu altyapı ile ağ cihazları ve bilgisayarları içeren topolojiler tasarlanabilmekte ve kullanıcının tasarıma uygun ortamlara hızlı bir şekilde erişebilmesi sağlanmaktadır.

Sanal Siber Güvenlik Laboratuvarı ve Tatbikat Altyapısı, siber güvenlik eğitim, test, tatbikat ve analiz projelerinde ihtiyaç duyulacak kullan-at sanal çalışma ortamları için ortak altyapıları hızlı ve düşük maliyetle oluşturabilmektedir.

Yetenekler

- Sunucu sanallaştırma altyapısı
- Hızlı, güvenli ve izole laboratuvar erişimi
- Görsel laboratuvar tasarım ara yüzü
- Kullanıma hazır laboratuvar ortamı şablonları
- Uzmanlar tarafından hazırlanan sanal makine imajları
- Yeni sanal makine imajları oluşturma
- Kullanıcı gruplarına göre kota yönetimi

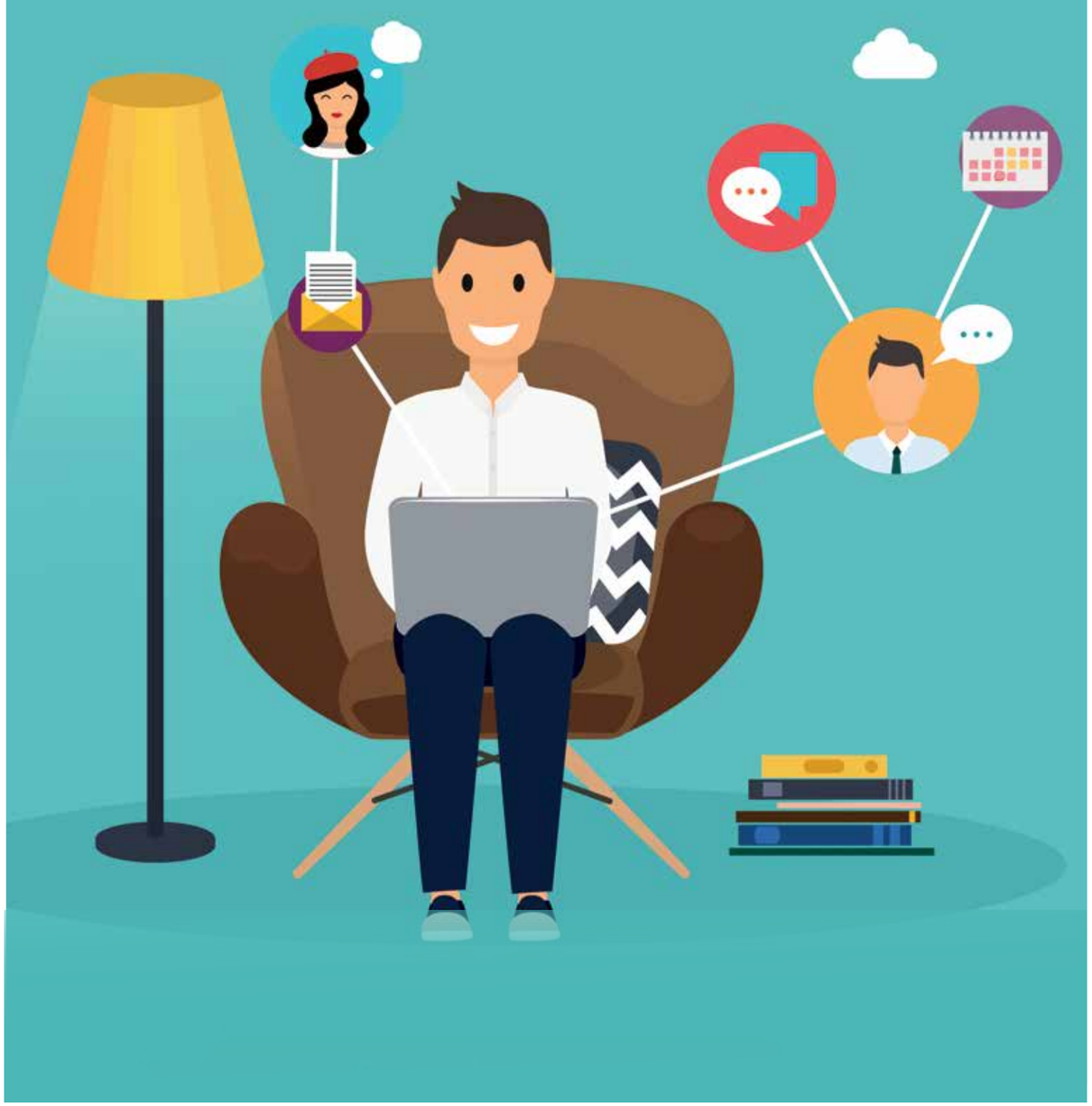
Kullanım Alanları

- Siber güvenlik analiz laboratuvarı
- Adli analiz laboratuvarı
- Uygulamalı eğitim ortamı
- Siber güvenlik yarışmaları ve tatbikatları

www.sge.bilgem.tubitak.gov.tr
www.bilgem.tubitak.gov.tr

Uzaktan **Çalışma** Güvenliği

"Uzaktan çalışma güvenliği, bilgi güvenliği alanının bir alt kümesidir."



Gül Aydın – Başuzman Araştırmacı / BİLGEM

Uzaktan çalışma, kişinin kurumu dışında çalışabilmesine imkan veren bir çalışma yöntemidir. Uzaktan çalışma, söz konusu işin çoğu zaman teknolojik iletişim araçlarının ve yazılımların desteğiyle evden veya kurumu dışında bir yerden yerine getirilmesidir. Uzaktan çalışma esnasında kurumun bilgisine ulaşılır. Bilgi ise kurumun en kıymetli varlıklarından biridir.

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasara uğratılmasını önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur.

√ **Gizlilik (Confidentiality):** Bilgilerin yetkisiz erişime veya ifşaya karşı korunmasını ifade eder. Gizlilik özelliği sadece bilgiye erişim yetkisine sahip kişilerin erişmesini sağlar.
√ **Bütünlük (Integrity):** Bilginin yetkisiz değişiklik veya imhadan korunması anlamına gelir. Bütünlük özelliğinin amacı, bilginin doğru, eksiksiz ve bozulmamış olmasını sağlamaktır.
√ **Erişilebilirlik (Availability):** Bilginin, talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir.

Bu çerçevede, uzaktan çalışma güvenliği, bilgi güvenliği alanının bir alt kümesi olarak düşünülmelidir.

Uzaktan Çalışma Riskleri

√ Kurum ağına şifresiz erişilir ise trafiği dinleyen üçüncü şahısların saldırılarına maruz kalma
√ Kullanılan parolalar, dokümanlar ve diğer hassas verilerin saldırganların eline geçmesi
√ Kurumların siber saldırılarla karşı karşıya kalması
√ Saldırganların kurum ağına erişmesi
√ Saldırganların oltalama saldırıları ya da kripto virüsleri gibi benzeri saldırılar

Güvenlik Önlemleri

Uzaktan çalışma esnasında oluşabilecek yukarıda yazılı riskleri bertaraf etmek için kurumlar ve çalışanlar tarafından bir dizi önlem alınmalıdır.

Kurumsal Önlemler

√ Uzaktan çalışma için sağlanacak erişim, mümkün olduğunca kurum tarafından sağlanan bilgisayar, telefon ve benzeri teknolojik araç gereçler ile yapılmalıdır. Bu cihazlarda bulunan yazılımların güncelliği kurum tarafından takip edilmeli aksi takdirde güvenlik zafiyetlerine sebebiyet verebileceği bilinmelidir.

√ Kurum uzaktan çalışma konusunda çalışanlarına farkındalık eğitimleri vermelidir. Uzaktan çalışma modelinin, hali hazırda yapılan işin mahiyetinde bir değişikliğe sebebiyet vermeyecek olduğunu ve bu kapsamda normal şartlarda asgari düzeyde dikkat edilen tüm hususlara dikkat ve özen gösterilmeye devam edilmesi gerektiği hatırlatılmalıdır. Çalışanların, uzaktan çalışma modeli öncesinde riayet ettikleri başta gizlilik olmak üzere tüm yükümlülüklerine riayet etmeye devam etmeleri gerektiği anlatılmalıdır. Bu noktada varsa alınması gereken tüm teknik önlemler alınmalıdır.

√ Çalışan kuruma erişimde mümkün olduğunca VPN Virtual Private Network (Sanal Özel Ağ) kullanmalıdır. VPN, temel olarak ağlara uzaktan erişim sağlayan bir sistemdir. VPN kullanıcısı, bulunmadığı bir noktadaki ağa erişebilir, veri aktarımında bulunabilir. VPN istemcisi, iki nokta arasında sanal bir ağ sürücüsü oluşturur. Daha sonra kullanıcıya karşıdaki ağdan bir IP verir. Kullanıcı bu IP ile izin verilen bağlantılara erişebilir. Temel anlamıyla internete başka bir IP adresi üzerinden bağlanılmasını sağlayan hizmettir.

VPN, bağlantıyı güvenli hale getirir ve herhangi bir ağa bağlanırken bağlantıyı şifreler ve kimlik tespitini engeller. VPN sistemi gönderilip alınan tüm verileri kendisi şifrelediğinden 3. şahısların ne yapıldığını görmesine izin vermeyen bir güvenlik sistemi olarak da kullanılabilir. VPN erişiminde gizliliğin korunması ve sistem devamlılığı için kurum güvenlik politikaları aynı şekilde uygulanmalıdır. VPN erişimi olmadan uzak masaüstü bağlantısı yöntemiyle ofis ağına bağlanılması engellenmelidir. Güvenilir bir VPN uygulaması, tüm kullanıcılar için geçerli güçlü

> Uzaktan çalışma modeli, pek çok kişi ve kurum için bilgi güvenliğinin sağlandığı ve ilgili riskler kontrol altına alındığı sürece uygun bir çalışma yöntemidir.

şifreleme ve çok aşamalı kimlik doğrulama mekanizmalarına sahip olmalıdır. Milli VPN çözümü, TÜBİTAK-BİLGEM tarafından geliştirilmiş ve kullanıma sunulmuştur.

√ Çalışanlara, kurumsal e-posta kullanımı teşvik edilmeli, zaruret olmadıkça bireysel e-posta kullanımına izin verilmemelidir.
√ Yazıcı kullanımı durumunda, dokümanın gizlilik derecesine göre uygun yazıcıya yönlendirme için-çalışanlar yetkilendirilmelidir.
√ Kullanıcı hesaplarının güçlü parolalarla korunması sağlanmalıdır. Uzaktan çalışma durumunda riskler artacağından, parolaların sık değiştirilmesi sağlanmalıdır. Bu konuda kurum parola politikasına uyulmalıdır.
√ Kurum sistemlerine erişimlerde ayrıcalıklı yetkilere sahip kullanıcı hesaplarının sayısı kısıtlanarak yalnızca gereksinim duyan kullanıcılara yetkiler tanınmalıdır. Ayrıcalıklı yetkilere sahip kullanıcı hesaplarının parolaları, güvenli ortamlarda saklanmalı ve bu parolaların belirli sıklıkta değiştirilmesini sağlayacak düzenlemeler yapılmalıdır.
√ Uzaktan çalışanlar için kurum tarafından onaylanmış depolama platformları, iletişim / video konferans araçları, proje yönetim araçları gibi uygulamalar kullanılmalıdır. Yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bunun dışındaki uygulamaların sistemlere yüklenmesi engellenmelidir.
√ Kurum, çalışanlardan işe girişlerde bilgi güvenliği taahhütnamesi alındığı durumlarda, taahhütnamede uzaktan çalışma modeli hakkında sınırları belirleyen bilgilendirme yapmalıdır.
√ Kurum, uzaktan erişim için yetkilendirilmiş kurum çalışanlarını ve bağlantı detaylarını kayıt altına almalıdır (loglama).
√ Kurum, ilişik kesen çalışanının uzaktan erişim uygulamalarını ve parolalarını derhal devre dışı bırakmalıdır.
√ Kurum, uzaktan kurum ağına erişecek bilgisayarların işletim sistemini, yamalarını ve antivirüs yazılımlarını güncel tutmalıdır.
√ Kurum, yüksek önemdeki sistemlere erişimlerde 2FA Two-factor autentication (İki adımlı kimlik doğrulama) adı verilen iki kademeli güvenlik doğrulaması kullanmalıdır. 2FA, iki adımlı doğrulama veya TFA olarak da bilinen İki Faktör Kimlik Doğrulaması, yalnızca bir şifre ve kullanıcı adı değil, aynı zamanda "çoklu faktör kimlik doğrulaması" olarak bilinen ekstra bir güvenlik katmanıdır. Sadece kullanıcının akıllı telefon, tablet ya da 2FA kimlik doğrulaması için özel olarak üretilmiş cihazlara gönderilen ve tamamen rastgele olarak belirlenen şifreler ile hesaplara giriş yapılabilmektedir.
√ Uzaktan çalışma durumlarında toplantıların yapılabilmesi için çalışanlara kurumları tarafından güvenli toplantı ortamları önerilmelidir. Toplantılar için kullanılacak aracı programların uçtan uca şifreleme yaptığı kontrol edilmelidir. Çevrimiçi ortamlarda gerçekleştirilen toplantılar için Kişisel Verilerin Korunması Kanunu'nun belirlediği yetki ve sorumluluklar dikkate alınmalı ve çalışanlar bilgilendirilmelidir.

Çalışan Önlemleri

√ Çalışanlar; bilgi varlığının gizlilik derecesi / sınıflandırılması hakkında yetkinliğe sahip olmalıdır. Gizlilik derecesi, bilmesi gereken kişiler dışındakilere açıklanmasının veya verilmesinin millî güvenlik veya kişisel güvenlik açısından sakıncalı görülen bilgi varlığının, ülke menfaatine, gerçek ve tüzel kişiler ile kamu kurum/kuruluşlarına zarar vermesini önlemek amacıyla önem derecesine göre sınıflandırılması ve adlandırılması şeklinde açıklanabilir. Bilgi varlıkları, bilginin niteliğine, tutulduğu ortama, saklanmasına, sunulmasına, işlenmesine ya da aktarılmasına ilişkin hususlar göz önünde bulundurularak sınıflandırılır.

√ Bilgi varlığının gizlilik derecesine göre işlenmesi, saklanması, taşınması ve transferi konusunda bilgi sahibi olmalıdır.
√ Bilgisayarlarına onaysız yazılım yüklememelidir.
√ Bilgisayarlarında lisansız yazılım kullanmamalıdır.
√ Kötücül yazılımların, bilginin bütünlüğünü bozma, gizliliğini ifşa etme ve erişilebilirliğini engelleme sonuçlarını doğurabileceğinin farkında olmalıdır.
√ Sosyal mühendislik amaçlı faaliyetlerde bulunmamalıdır.
√ Güçlü parola kullanmalı ve kimseyle paylaşmamalıdır.
√ Tespit ettikleri bilgi güvenliği ihlallerini kurum yetkililerine bildirmelidir.
√ Kurumsal cihazları/ortamları, başka kimselerin kontrolsüz kullanımına izin vermemelidir.
√ Kurum varlıklarına erişim sağlarken erişim kontrol politikalarını göz önünde bulundurmalıdır.
√ Kişisel taşınabilir ortamlar/cihazlar üzerinden kurum ağına erişim sağlamamalıdır (kurumca izin verilen veya zorunlu durumlar hariç).
√ Kurum bünyesinde onaysız olarak teknik açıklık taraması ve saldırı/sızma faaliyetlerinde bulunmamalıdır.
√ Kurum bünyesinde uygulanan güvenlik önlemlerini devre dışı bırakabilecek faaliyetler yapmamalıdır.

Genel Kurallar

Güvenlik önlemleri çerçevesinde kurumun sektörü, sektördeki çalışma alanı, büyüklüğü, çalışan sayısı ve bulunduğu bölgeye göre aşağıdaki kurallar uzaktan bağlantı için uygulanabilir. Bu kurallar, bir kurumun uzaktan bağlantı politikaları olarak düşünülebilir.

Uzaktan Erişim Kuralları

√ Kurum çalışanı farklı bir fiziksel lokasyondan, kurum ağı ve sistemlerine erişimi için VPN (Sanal Özel Ağ) kullanır.
√ Kurum ağına VPN ile bağlanmak isteyen kullanıcılar gerekli formları doldurarak, kullanım kurallarını okuduğunu ve uymayı kabul ettiğini taahhüt eder. Formda, erişmek istedikleri kaynak ve servis bilgileri belirtilir.
√ Uzaktan erişim talepleri ilgili yöneticilerin ıslak imzalı onayı ile yerine getirilir.
√ Dış tarafların çalışanına verilecek olan uzak bağlantı yetkilerinden ilgili yönetici sorumludur.
√ Onaylanan uzaktan erişim talebi Bilgi Sistemleri Ağ Yöneticisi tarafından karşılanır.
√ Kurum uygulamalarına, sistemlerine ve ağ bileşenlerine uzaktan erişim aktiviteleri kayıt altına alınır.
√ Kurum iç ağına uzaktan bağlantı yapılamaz.

Uzaktan Çalışma Kuralları

Uzaktan bağlantıya (VPN) izin verilen kurumlarda;
√ Kurum çalışanı uzaktan çalışılacak ve/veya VPN bağlantısı yapılacak ağın güvenliğinden emin olur.
√ Halka açık olan ağlardan kurumsal iş bilgisayarları ile kablolu/kablosuz bağlantı kurulmaz ve VPN bağlantısı yapılmaz.
√ İş bilgisayarı dışındaki çalışanın şahsi kullanıma ait bilgisayarlar ile kurum ağına VPN bağlantısı kurulamaz. Kurumsal iş bilgisayarları ile yapılan VPN bağlantılarında bilgisayara uygulanan güvenlik kontrollerinin (antivirüs yazılımı, işletim sistemleri güvenlik yamaları vb.) güncel ve çalışır olduğundan emin olunur.
√ Dış taraf çalışanının uzaktan kurum ağına bağlanması gerektiği durumlarda sadece ihtiyaç duyulan kaynaklara erişim sağlanır.
√ Kurum ağına uzaktan bağlantı sırasında bilgi varlıklarının gizliliğine, bütünlüğüne, erişilebilirliğine zarar gelmesi durumunda, bu zarardan bağlantıyı yapan kullanıcı sorumludur.
√ Uzaktan erişim için yetkilendirilmiş kullanıcı bu hakkı diğer kurum çalışanı veya üçüncü taraf kişilere kullandırmaz.
√ Çalışanlar ve dış taraflar yaptıkları VPN bağlantısının ifşa olması/hesaplarının ele geçirilmesi/hali hazırda var olan zararlı yazılımın kasıtlı kasıtsız kurum ağına bulaştırılması ile ilgili doğacak yasal sorumluluklardan kendileri/birim sorumlusu sorumludur.

Sonuç

Gelişen sosyal ve ekonomik koşullar ile teknolojik yenilikler, sosyoekonomik yaşamı ve çalışma hayatını büyük ölçüde etkilemektedir. Endüstri toplumlarında teknolojide ve üretim sistemlerinde meydana gelen değişmeler, uluslararası rekabet, artan işsizlik gibi faktörler çalışma sürelerinde esneklik yapılması gerekliliğini ortaya çıkarmıştır. Yaşamakta olduğumuz salgın da bu ihtiyacı katlamıştır.

Uzaktan çalışma modeli, pek çok kişi ve kurum için bilgi güvenliği sağlandığı ve ilgili riskler kontrol altına alındığı sürece uygun bir çalışma yöntemidir. Şüphesiz ki her sektör ve çalışma alanı için farklı riskler vardır. Bu itibarla, bu yazının kapsamında daha ziyade genel nitelikteki risklere değinilmiş olup, sektörel bazlı oluşabilecek diğer risklerin doğru analiz edilmesi ve gerekli önlemlerin alınabilmesi en doğru yöntem olacaktır.

KAYNAKÇA

-Tübitak BİLGEM Erişim Kontrol Kılavuzu
-Tübitak BİLGEM Bilgi Güvenliği Taahhütnamesi

TEMPEST
Bilgi İçeren Kaçakların Denetimi

> TEMPEST, Amerikan Hava Kuvvetleri'nin gizliliğini kaldırarak yayınladığı bir dokümanda "Transient Elektromagnetic Pulse Emanation Standard" ifadesini oluşturan kelimelerin baş harfleri olarak tanımlanmıştır.

Cantürk Karadeniz – Başuzman Araştırmacı / BİLGEM TDBY

TEMPEST, gizlilik dereceli bilgi işleyen cihazlardan kaynaklanan istenmeyen elektromanyetik enerji yayılımlarının araştırılması, incelenmesi ve bu yayılımların kabul edilebilir seviyede denetim altına alınması olarak tanımlanabilir. TEMPEST kaçakları, bilgi içeren kaçaklar olarak ifade edilebilir.

- TEMPEST kaçakları, istem dışı olarak oluşur.
- TEMPEST kaçakları, belli frekanslarda bilgi taşıyan işaretlerdir.
- TEMPEST kaçakları, kablo üzerinden veya havadan yayılır.
- TEMPEST kaçakları ilk ele geçirildiğinde anlamlı görünmeyebilirler. İşaret işleme teknikleri sonucu elde edilen bilgiler, ÖZEL ve üstü gizlilik dereceli açık bilgileri içerebilir.

TEMPEST, Amerikan Hava Kuvvetleri'nin gizliliğini kaldırarak yayınladığı bir dokümanda "Transient Elektromagnetic Pulse Emanation Standard" ifadesini oluşturan kelimelerin baş harfleri olarak tanımlanmıştır. "Bilgi içeren kaçaklar (Compromising Emanations)" terimi ilk kez, 2007 tarihinde gizliliği kaldırılan, 1972 yılında yayımlanmış "Cryptologic Spectrum" dergisinde çıkan "TEMPEST: A signal problem" adlı makalede yer almıştır [1].

ÖZEL ve üzeri gizlilik dereceli bilgi işleyen elektrikli bir cihaz çalışırken içerisinde kullanılan birçok devre ve komponent elektromanyetik enerji yayar. Bu enerji hem havada yayılır, hem de ortamda bulunan iletkenler olan güç kabloları, telefon hatları, işaret hatları ve metal kalorifer borularından da yayılabilir. Bu emisyonlar analiz edildiğinde cihazın işlediği gizli bilgiler elde edilebilir. Bu durum sadece kripto cihazları için değil, gizli bilgi işleyen bilgisayar, monitör, yazıcı, tarayıcı, faks, telefon ve fotokopi gibi cihazlar için de geçerlidir. Yine benzer şekilde gizli bilgi işleyen gemi, uçak, uydu vb. sistem ve platformların TEMPEST testlerinin de yapılması gerekmektedir.

TEMPEST ile İlgili Önemli Terimler

Gizlilik dereceli bilgilerin işlendiği, iletildiği veya saklandığı sistemlerde Haberleşme Güvenliği (COMSEC), İletim Güvenliği (TRANSEC), Kripto Güvenliği (CRYPTOSEC) ve TEMPEST olarak üç alt maddeye ayrılabilir.

TEMPEST kapsamında 'Kırmızı', 'Siyah' ve 'Bilgi içeren kaçak' terimlerinden bahsetmek gerekir.

Kırmızı: ÖZEL ve üzeri gizlilik seviyeli açık bilgiyi taşıyan sistemleri, cihazları, devre elemanlarını, işaret hatlarını ve KIRMIZI cihazların bulunduğu bölgeleri ifade etmektedir.

Kırmızı örnekler

- Kriptolanmamış gizlilik dereceli bilgi taşıyan her çeşit hat, tel ya da fiber optik bütün kablolar.
- Kriptolanmamış gizlilik dereceli bilgiyi işleyen bütün teçhizat (Kriptografik teçhizat dahil).
- Kırmızı ve siyah sistemler arasında geçiş noktasında çalışan filtreler.
- Kırmızı hatlardan veya teçhizattan herhangi birinin bulunduğu bölge.
- Emniyet toprağı ve kablosu.

Siyah: ÖZEL ve üzeri gizlilik seviyeli açık bilgi barındırmayan veya ÖZEL ve üzeri gizlilik seviyeli açık bilgiyi kriptolanmış olarak barındıran sistemleri,

Şekil 1. Cihaz ve Platform Örnekleri

> **Gizlilik dereceli bilgilerin işlendiği, iletildiği veya saklandığı sistemlerde Haberleşme Güvenliği (COMSEC); İletim Güvenliği (TRANSEC), Kripto Güvenliği (CRYPTOSEC) ve TEMPEST olarak üç alt maddeye ayrılabilir.**

cihazları, devre elemanlarını ve işaret hatlarını ifade eder. KIRMIZI cihazların bulunmadığı bölgeler ise SİYAH bölge olarak tanımlanır.

Siyah örnekler

- Sadece Tasnif Dışı ya da kriptolanmış gizlilik dereceli bilgi taşıyan tel ya da fiber optik bütün hatlar.
- Tasnif Dışı ya da sadece kriptolanmış bilgiyi ileten ve işleyen bütün teçhizat (Kripto teçhizatının kriptolanmış çıkışı dahil).
- Güç birimleri, güç bataryaları, güç sağlayan her çeşit teçhizat.
- İçinde kriptolanmamış gizlilik dereceli bilginin bulunmadığı bölgeler.

Bilgi içeren kaçaklar: Sistem veya cihaz tarafından ortama yayılan emisyonların ele geçirilip incelenmesinin ardından elde edilen ÖZEL ve üzeri gizlilik seviyeli bilgi kaçağı olarak tanımlanabilir.

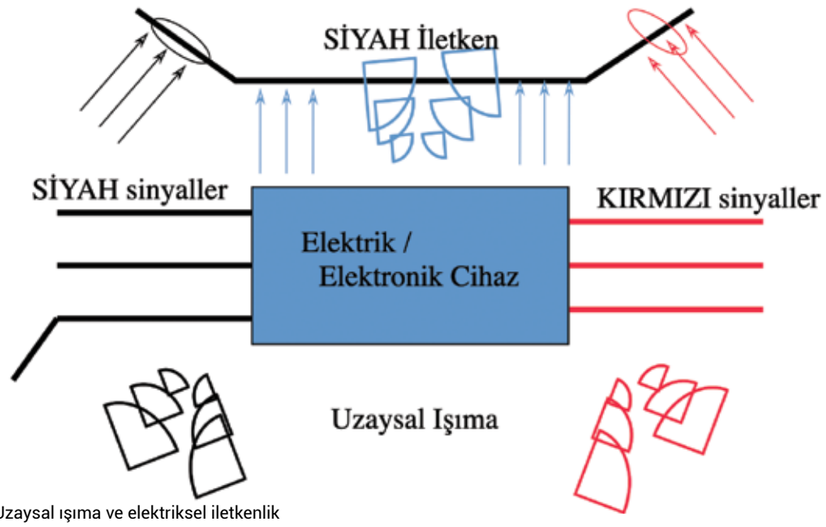
Elektromanyetik Girişim ve Elektromanyetik Uyumluluk

TEMPEST konusunu daha iyi anlayabilmek için Elektromanyetik Girişim (Electromagnetic Interference - EMI) ve Elektromanyetik Uyumluluk (Electromagnetic Compatibility - EMC) konularından kısaca söz etmek gerekir.

Elektronik cihazlar işlevlerini yerine getirirken ortama istemsiz yayılan enerji, etrafta bulunan diğer cihazların fonksiyonlarını istemsiz bozucu etkiler yaratabilir. Bununla birlikte, etrafta bulunan diğer cihazların çalışmaları esnasında yayılan emisyonlar nedeniyle kullandığımız elektronik cihaz da etkilenebilir. Bu emisyonlardan etkilenme sonucunda cihaz veya sistemlerin çalışmalarında bozulma ya da kötüleşme olmasına Elektromanyetik Girişim adı verilir. Cihazların diğer cihazlar üzerinde EMI nedeniyle kötüleşmeye neden olmadan ve ortamda bulunabilecek enerjiden etkilenmeden çalışmaya devam edebilmesine ise Elektromanyetik Uyumluluk denir.

Elektronik devrelerde işaretlerin gerilim seviyelerindeki değişim esnasında tüketilen enerjinin bir kısmı elektromanyetik dalga olarak ortama yayılır. Kullanıcının isteği dışında elektromanyetik olarak dış ortama yayılan ve ele geçirilmesi istenmeyen bilgiler gerçek zamanlı olarak işlenebilir veya kaydedilebilir. Bu yayılan dalgalar bilgi ile ilişkili işaret kaçaklarını da içerebilir. Eğer elde edilen bu işaret ÖZEL ve üzeri gizlilik dereceli bilgi içeriyor ise buna "bilgi içeren kaçak" denir.

Örnek olarak gizli bir konuda doküman yazan bir bilgisayar ekranını düşünülebiliriz (Şekil 2). Bu sistemin oluşturabileceği elektromanyetik enerji, ortamda yayılmak için çeşitli kaçak yollar bulabilir ve bu enerjinin ulaşabileceği noktaları tahmin



Şekil 2. Uzaysal ışıma ve elektriksel iletkenlik

etmek oldukça zordur. Bilgisayar ve özellikle monitörden yayılan ve kontrol edemediğimiz enerji, başkaları tarafından ele geçirilerek ekran görüntüsü oluşturulabilir. Bu durumda bilgi güvenliği ihlal edilmiş olur ve bu ihlal bir TEMPEST tehdidi oluşturur.

TEMPEST araştırmaları, yayılımların içinde gizlilik dereceli bilgi olup olmadığını inceler. TEMPEST önlemleri ise cihaz ve binalardan yayılabilecek yayılımların makul seviyede tutulabilmesini sağlar [2].

TEMPEST Önlemleri

Elektromanyetik yolla oluşan bilgi güvenliği ihlallerini ortadan kaldırmak için öncelikle kaçak oluşum yollarını incelemek gerekir. Kaçaklar, bilgi işleyen cihazdan doğrudan uzaysal ışıma ile yayılabileceği gibi aynı zamanda cihazın kablolarından veya ortamdaki anten görevi görebilecek diğer iletkenler üzerinden de yayılabilir (Şekil 2).

Uzaysal ışıma ile oluşan kaçakların ele geçirilebilmesi için kimi zaman uygun frekansta çalışan bir anten kullanmak yeterli olabilir. Elektriksel iletkenlik yoluyla oluşan kaçaklar için ise bir akım probu kullanılabilir. Cihaz üzerinde EMI ve EMC konusunda alınan önlemler aynı zamanda TEMPEST önlemlerinin de bir kısmını içerir, ancak TEMPEST konusu, cihazların elektromanyetik enerjiden etkilenme özelliklerini veya cihazların diğer cihazlar üzerinde yarattığı bozucu etkileri içermez.

> **TEMPEST araştırmaları, yayılımların içinde gizlilik dereceli bilgi olup olmadığını inceler. TEMPEST önlemleri ise cihaz ve binalardan yayılabilecek yayılımların makul seviyede tutulabilmesini sağlar.**

Uzaysal ışıma yoluyla ve elektriksel iletkenlik yoluyla oluşan bilgi kaçaklarının ortadan kaldırılması için tedbirler alınmalıdır. Bu tedbirler EMI ve EMC tedbirleriyle aynıdır.

Uzaysal ışıma yoluyla oluşan bilgi kaçaklarının ortadan kaldırılması için önce kaçağa neden olan kaynak bulunur. Kaynak üzerinde çalışmalar yapılarak emisyon seviyesi bastırılır.

İletkenlik yoluyla oluşan bilgi güvenliği ihlalerinde de yine benzer biçimde kaynak bulunur. Ardından kaynağın ürettiği emisyon seviyesi azaltılır.

Genel olarak TEMPEST önlemlerini aşağıdaki şekilde sıralayabiliriz:

1. Gizlilik dereceli bilgi işleyecek cihaz ve sistemleri test etmek.
2. Cihazların kullanılacağı bina ve tesislerin TEMPEST tesisat kurallarına göre uygunluğunu sağlamak.

3. Cihaz ve bina uyumlandırması yapmak.
4. Tesisat kurallarına göre cihazları doğru yerleştirmek.
5. Doğru tipte kablo kullanmak.
6. İletkenlik yoluyla kaçak oluşmaması için uygun güç ve işaret hattı filtreleri kullanmak.
7. Doğru topraklama yapmak.
8. Gerekirse gizlilik dereceli bilgi işlenen bölgeleri elektromanyetik olarak izole etmek.

Cihaz TEMPEST Değerlendirmesi

Cihazların TEMPEST testleri, Genelkurmay Başkanlığı tarafından MST 401-1 (B) "Türk Silahlı Kuvvetleri TEMPEST Test Standartları" dokümanı referans alınarak gerçekleştirilmektedir[3]. Bu doküman NATO tarafından yayımlanan SDIP-27/2 "NATO TEMPEST Requirements And Evaluation Procedures" dokümanının milli eşdeğeridir. Bu dokümanlarda Seviye A, Seviye B ve Seviye C olmak üzere üç ayrı cihaz TEMPEST değerlendirme seviyesi tanımlanmıştır ve ÖZEL ve üzeri gizli bilgi işleyen bütün cihazların bu standarda göre testleri yapılmalıdır.

Kripto cihazları ve TEMPEST özellikli olarak tasarlanan cihazlar, ilgili dokümanın "SEVİYE A" gereksinimlerine göre test edilmelidir. Bu gereksinimlere göre hem Elektrik Işıma testleri hem de İletkenlik Işıma testleri birlikte yapılmalıdır. Kripto cihazlarının, işlediği bilginin gizlilik derecesi dikkate alındığında en sıkı kurallara göre test edilmesi gerekmektedir.

Standartta üç adet cihaz TEMPEST değerlendirme seviyesi belirlenmiştir:
"SEVİYE A" en düşük ışımaya karşı gelen sınır değeridir. TEMPEST kaçak riskinin kabul edilebilir seviyede kalmasını sağlar. Seviye A, cihaz ve ortak sistemlerin MY401-1(B)'de belirtilen şartlara göre kurulumu yapıldığı takdirde, 8 metrenin ötesinde TEMPEST kaçak riskinin kabul edilebilir seviyede kalmasını sağlar.

"SEVİYE B" orta seviye ışıma sınır değeridir. Seviye B, cihaz ve ortak sistemlerin MY401-1(B)'de belirtilen şartlara göre kurulumu yapıldığı takdirde, TEMPEST kaçak riskinin 20 metrenin ötesinde kabul edilebilir seviyede kalmasını sağlar.

"SEVİYE C" ise en yüksek sınır değeridir. Seviye C ise cihaz ve ortak sistemlerin MY401-1(B)'de belirtilen şartlara göre kurulumu yapıldığı takdirde, 100 metrenin ötesinde TEMPEST kaçak riskinin kabul edilebilir seviyede kalmasını sağlar. Seviye C koşulları, sabit yerleşke ve hareketli platform içindeki taktiksel verilerin TEMPEST korumasını belirtmektedir.

Bina TEMPEST Değerlendirmesi

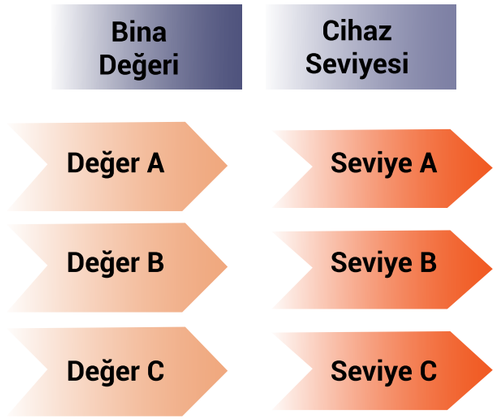
Bina TEMPEST değerlendirmesi, gizli bilgilerin işleneceği binaların elektromanyetik zayıflatma seviyelerinin ölçülmesi ile belirlenir. Bina değerlendirme sonucunda binalara da Seviye A, Seviye B ve Seviye C olmak üzere üç ayrı değer verilir. "Seviye A" en kötü zayıflatma değeri olan bina, "Seviye C" ise ekranlama etkinliği en iyi olan binalara verilmektedir.

Bina TEMPEST değerlendirmesi genel olarak ölçümlerin alınması, değerlendirilmesi ve bina bölgelendirme haritalarının oluşturulması adımlarından oluşmaktadır. Bina TEMPEST değerlendirmesi ölçmelerinde, ölçüm frekans aralığında çalışan antenler, işaret üreteçleri ve alıcılarının kullanılması gerekir.

Öncelikle ölçüm yapılacak bölgede ilgili frekans bandında çalışan bir anten ve alıcı kullanılarak ortam ölçümü yapılır. Dış ortamda belirli mesafeden işaret üretilip anten vasıtasıyla ortama yayınım yapılır. Alıcı anten ile gelen işaret ölçülerek referans ölçüm elde edilir. Doğal olarak dış ortamda radyo, televizyon, telsiz ve GSM yayınları bulunmaktadır. Değerlendirme yapılırken bu emisyonlar dikkate alınır. Daha sonra verici anten bina içine yerleştirilerek aynı ölçüm tekrarlanır. Referans ölçüme göre binaların ekranlama etkinliği ve binanın TEMPEST değeri belirlenir.

Cihazların Doğru Yerleştirilmesi

Bina ve cihaz değerlendirmesi, cihazların çalışma ortamlarının doğru belirlenmesi ve genel TEMPEST tesisat kuralları, Genelkurmay Başkanlığı



Şekil 3. Cihazın Uygun Bölgede Kullanılması

tarafından yayımlanan MY 401-1(B) "Türk Silahlı Kuvvetleri TEMPEST Yönergesi" ne göre yapılmaktadır[4]. Bu doküman NATO tarafından yayımlanan SDIP-29 "Facility Design Criteria and Installation of Equipment for the Processing of Classified Information" dokümanın milli eşdeğeridir. Bu dokümanda, ÖZEL ve üzeri gizli bilgileri işlemede kullanılan cihazların, bulundukları ortamda TEMPEST kaçağına neden olmaması için nerelere ve nasıl yerleştirilmeleri gerektiği belirtilmektedir.

Bilgi güvenliği kapsamında gizli bilgi işleyen cihazlar test edildikten sonra bu cihazların yerleştirileceği binalar ve çalışma ortamları da çok önemlidir. Cihaz değerlendirme seviyesi en iyi olan cihaz ekranlama etkinliği düşük olan binalarda ve ofislerde TEMPEST tesisat kuralları doğrultusunda kullanılabilir. Zayıflatma seviyesi çok düşük binalarda sıkı şekilde testleri yapılmış cihazlar kullanılmalıdır. Bu nedenle cihaz ve bina değerlerinin birlikte kullanılarak TEMPEST açısından daha düşük risklere sahip tesisler yapılmalıdır. Cihazların uygun bölgelerde kullanılması ile maliyet etkin TEMPEST açısından önlemler alınabilir (Şekil 3).

BİLGEM TEMPEST Test Laboratuvarı

Türk Silahlı Kuvvetlerinin TEMPEST ve EMC konusunda ihtiyaçlarının karşılanması ve standartlarının oluşturulması için 1995 yılında TÜBİTAK UEKAE bünyesinde TEMPEST ve EMC Laboratuvarı kurulmuştur. İlk resmi TEMPEST testi 2000 yılında gerçekleştirilmiştir.

Laboratuvarımız, 2000 yılından itibaren gerek TÜBİTAK gerek özel sektör tarafından geliştirilen cihazlarda, başta anahtar verisi olmak üzere diğer tüm arayüzlerde kaçaklar tespit etmiş ve bu kaçakların ortadan kaldırılması için danışmanlık hizmeti vermiştir.

Şekil 4: Test Ortamı

Şekil 5: Sinyal Analizör

BİLGEM'de NATO TEMPEST standartları temel alınarak milli standartlar oluşturulmuş ve bu standartlara uygun testler yapabilecek test altyapısı kurulmuştur. (Şekil 4 ve Şekil 5).

TEMPEST konusunda Türkiye'nin gereksinimlerini karşılayacak bilgi birikimi kazanılmıştır ve çeşitli kuruluşlara bu konuda destek verilmektedir.

BİLGEM TEMPEST Test Laboratuvarı, SDIP 29/2 ve MY401-1(B) kapsamında ülkedeki tüm kamu kurumları savunma sanayi firmalarına kurulum, danışmanlık hizmeti ve TEMPEST uygunluk raporu vermektedir.

BİLGEM TEMPEST Test Laboratuvarı, SDIP 27/2 ve MST 401-1(B) standartlarına göre TEMPEST testlerini gerçekleştirmektedir. Türk Silahlı Kuvvetleri bünyesinde kullanılacak bütün kripto cihazları, TEMPEST korumalı cihazlar, uydu yer istasyonu ve gemi gibi askeri platformlar da laboratuvarımız tarafından test edilmektedir.

KAYNAKÇA

[1] USA National Security Agency, TEMPEST: A Signal Problem: Cryptologic Spectrum, 1972.
[2] UEKAE Dergisi Cilt 2 Sayı 3, Mayıs-Ağustos 2010. https://bilgem.tubitak.gov.tr/sites/images/bilgem/dergi/03_UEKAE.pdf
[3] MY 401-1(B), Türk Silahlı Kuvvetleri TEMPEST Yönergesi
[4] MST 401-1(B), Türk Silahlı Kuvvetleri TEMPEST Test Standartları

TEMPEST Tesis Değerlendirmesi ve Bina Ölçüm Sistemi

"TEMPEST Bina Değerlendirmesi, bina içindeki bir kaynaktan çıkan elektromanyetik (EM) ışımanın, bina ve çevresindeki serbest uzay tarafından hangi seviyede zayıflatıldığının belirlenmesidir."

Dr. Hasan Seçkin Efendioğlu – Başuzman Araştırmacı / BİLGEM TDBY

Günümüzde bilgi güvenliği, bilişim teknolojilerinin en kritik konularındandır. TEMPEST, bilgi güvenliğinin haberleşme güvenliği alt başlığı altında, elektromanyetik emisyon güvenliği kapsamında değerlendirilmektedir. TEMPEST, gizlilik dereceli bilgi işleyen elektronik cihazlardan kaynaklanan elektromanyetik bilgi kaçakları olarak ifade edilebilir. Bunları önlemeye yönelik birçok ülke yatırımlar yaparak özel TEMPEST donanımları kullanmakta, TEMPEST testleri gerçekleştirmekte ve farklı güvenlik kuralları uygulamaktadır. Bu kapsamda standartlar oluşturulmakta ve bilimsel araştırmalar yapılmaktadır. TEMPEST önlemleri hem gizlilik dereceli bilgi işleyen cihazlara hem de bu cihazların kullanıldığı bina veya tesislere uygulanmaktadır.

Gizli bilgilerin bulunduğu/saklandığı/iletildiği bilgisayarlar, ekranlar, yazıcılar, tarayıcılar, klavyeler vb. bütün cihazlar, çoğu zaman piyasadan satın alınmış, herhangi bir TEMPEST önlemi bulunmayan cihazlardır. Marka ve modellerine göre cihazların elektromanyetik ışıma özellikleri büyük farklılıklar gösterebilir. Bu cihazların gizli bilgilerin işlenmesinde kullanılmadan önce test edilmeleri gerekir.

Cihazlar, Genelkurmay Başkanlığı ve NATO standartlarına göre cihaz değerlendirmesine tabi tutulurlar. Genelkurmay Başkanlığı TEMPEST testleri standardında A, B ve C olmak üzere üç ayrı sınır değerine karşılık gelen cihaz seviyesi tanımlanmıştır. Ticari pazar cihazları, MST 401-1(B) standardının Elektrik Işıma test yöntemlerine göre test edilir. "A" en düşük ışımaya karşılık gelen sınır değeri ve "C" ise en yüksek sınır değeridir [1]. Önlemler alınarak tasarlanmış özel TEMPEST uyumlu cihazlar da askeri ve güvenlik amaçlı olarak kullanılmaktadır. Bu tip TEMPEST uyumlu kripto cihazı, bilgisayar, verici ve yazıcı gibi farklı cihazlar ise kapsamlı TEMPEST testlerine tabi tutulurlar.

TEMPEST Tesis Değerlendirmesi

TEMPEST tesis değerlendirmesi ile ilgili bilgiler Genelkurmay Başkanlığı tarafından yayınlanan MY 401-1(B) Türk Silahlı Kuvvetleri yönergesinde yer almaktadır [2]. Tesis değerlendirmesi konusundaki bilgiler NATO tarafından yayınlanan SDIP-28/2 dokümanı ile eşdeğerdir [3]. TEMPEST tesis değerlendirmesinin ilk safhası bina TEMPEST değerlendirmesidir. Bina değerlendirmesi, bina içindeki bir kaynaktan çıkan elektromanyetik (EM) ışımanın, bina ve çevresindeki serbest uzay tarafından hangi seviyede zayıflatıldığının belirlenmesidir. Bu değerlendirmede, bina içindeki bir kaynaktan çıkan EM ışımanın bina dış yüzeyine ulaşıncaya kadar uğrayacağı zayıflama ile bina dış duvarından denetlenebilir uzayın sınırına kadar uzanan mesafedeki toplam zayıflatmanın yerinde ölçülmesi gerekir. TEMPEST emniyeti açısından toplam zayıflatmanın mümkün olduğunca yüksek seviyede olması tercih edilen bir özelliktir. Zayıflatması yüksek olan bölgelerde, TEMPEST seviyesi daha düşük olan cihazların kullanılması mümkündür.

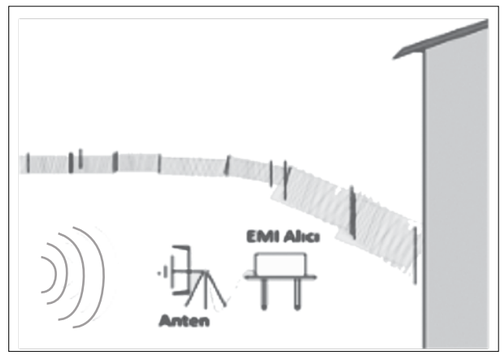
Binaların zayıflatma etkinliği, binanın mimarisi, yapıldığı malzemenin cinsi, duvarlarının kalınlığı, taşıdığı metal yoğunluğu, pencere açıklıkları gibi özelliklere bağlıdır. Ayrıca, ışıma yapan kaynağın bina içerisinde nerede konumlandığı, yabancı binalara olan uzaklığı, çevresinde bulunabilecek ve ışımaya karşı yansıtıcı özellikleri ile ışımanın yönlendirilmesinde etkili olabilecek metal elemanlar, denetlenebilir uzay dışına uzanan rastlantısal iletkenlik etkisi yaratabilecek atık su boruları, havalandırma kanalları, kalorifer tesisatı gibi iletkenler, binaların zayıflatma etkinliği üzerinde rol oynamaktadır.

TEMPEST Bina Değerlendirme Ölçümleri

Binalarda kullanılacak cihazların yerleştirildiği noktalar, elektromanyetik kaçak oluşmaması için dikkatlice belirlenmelidir. Bu yüzden binaların istenmeyen emisyonları ne kadar zayıflattığı test edilerek belirlenmelidir. Bina TEMPEST değerlendirmesinde bina bölgelendirme haritaları oluşturulmaktadır [4]. Ölçümler yapılırken, test planına göre, bina içinde ve dışında yer alan noktalar arasında frekansa bağlı olarak EM ışıma zayıflamaları ölçülmektedir. Bu zayıflama değerleri ile öngörülmüş zayıflatma sınır değerlerinin karşılaştırılması ile bina TEMPEST değeri tayin edilir. TEMPEST bina değerlendirme ölçümleri ortam, referans ve zayıflatma ölçümleri olmak üzere üç adımdan oluşur.

Ortam Ölçümü

Bina değerlendirmesinde ilk ölçüm ortam ölçümüdür. Şekil 1'de görüldüğü gibi ortam ölçüm düzeneği anten ve alıcı cihazdan oluşur. Öncelikli olarak ortam emisyonları ölçülerek var olan çevre gürültüsü kaydedilir. Ortam ölçümleri, çevre gürültü seviyesi ve yerel işaretlerin test sonuçlarını etkilemeyeceğinden emin olmak için yapılır. Ortam ölçümü ile testler için uygun frekanslar belirlenir. Daha sonraki bütün referans ve zayıflatma ölçümleri bu frekanslarda yapılır.

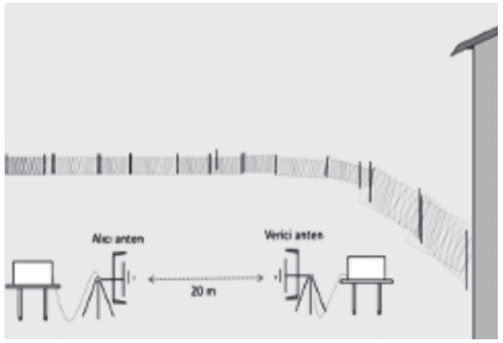


Şekil 1. Ortam ölçüm düzeneği

Referans Ölçümü

TEMPEST bina değerlendirmesinde ortam ölçümünden sonra referans ölçümü gerçekleştirilir. Referans ölçüm düzeneği, verici ve alıcı sistemlerden oluşmaktadır. Verici sistem, sinyal üreteci ve verici antenden; alıcı sistem ise alıcı anten ve EMI alıcıdan oluşmaktadır (Şekil 2). Referans ölçümlerinde verici ve alıcı antenler karşılıklı olarak birbirlerine 20 metre mesafede olacak şekilde konumlandırılır. Belirli bir frekans aralığında ve bu aralıktaki farklı frekans noktalarında verici anten vasıtası ile belirli bir güç uygulanarak gönderilen sinyaller, alıcı anten yardımı ile ölçülerek kayıt altına alınır. Bu işlem açık bir alan-

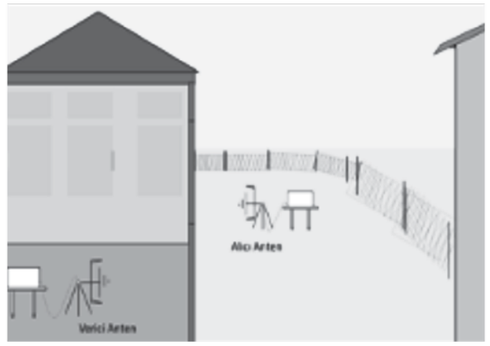
da yapılır. Referans ölçümlerinin amacı kablo, anten, konektör gibi sistem bileşenlerinden kaynaklanan zayıflatma ve hataların giderilerek sistemin kalibre edilmesidir [4]. Referans ölçümü sonuçları, zayıflatma ölçüm verisi ile karşılaştırma yapmak için referans olarak kullanılır.



Şekil 2. Referans ölçüm düzeneği

Zayıflatma Ölçümü

Bina zayıflatma ölçümleri, bina TEMPEST değerlendirmesinin son adımına karşılık gelmektedir. Zayıflatma ölçüm düzeneği Şekil 3'te gösterilmiştir. Verici anten bina içinde gizli bilginin işlendiği konumlara sırasıyla yerleştirilir. Bina veya bölge dışında kritik konumlar belirlenerek alıcı anten bu konumlara yerleştirilir. Bu işlem, tesis içinde ve

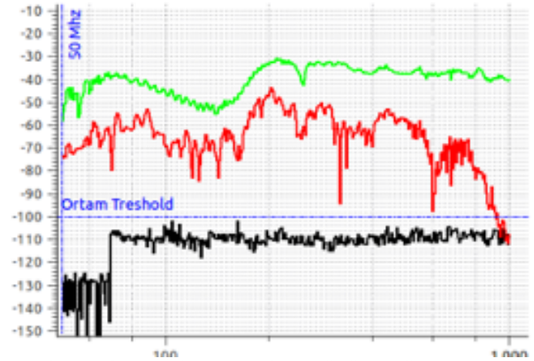


Şekil 3. Bina zayıflatma ölçüm düzeneği

dışında seçilen her bir nokta için tekrarlanarak ölçümler yapılır. Bütün kablo uzunlukları, kazanç ayarları ve varsa yardımcı bileşenler referans ve zayıflatma ölçümlerinde aynı kalmalıdır. Ölçümlerde antenler metal yüzeylerden uzak tutulmalıdır.

BİLGEM TEMPEST Bina Değerlendirme Sistemi

TÜBİTAK BİLGEM tarafından geliştirilen TEMPEST bina değerlendirme sistemi yardımı ile alınan ölçümlerin sonuçları Şekil 4'te gösterilmiştir. Siyah, yeşil ve kırmızı çizgili grafikler sırasıyla ortam, referans ve zayıflatma ölçümlerinin sonuçlarını temsil etmektedir. Şekil 4'te görülebileceği gibi ortam ölçümünde "ortam threshold" olarak yazılan bir limit değeri belirlenmiştir ve bu limiti geçmeyen frekans-



Şekil 4. Ortam, referans, zayıflatma ölçüm grafikleri

lar test için güvenli noktalar olarak kabul edilmiştir. Ölçümler, 10MHz'den 1GHz'e kadar, logaritmik artan 400 farklı frekans noktasında gerçekleştirilmiştir.

Bina TEMPEST değerlendirmesi, bina içindeki çeşitli yerlerden yayımlanan elektromanyetik işaretlerin, bina dışındaki noktalardan ölçülen zayıflatma seviyeleri ile kontrollü uzay sınırı içinde referans olarak alınan noktalar arasından ölçülen seviyeler karşılaştırılarak yapılır. Zayıflatma değerleri aşağıdaki formüle göre hesaplanır:

$$Zayıflatma(dB) = V_{Ref} - V_{Att} + 20log\ (\ (a+b)\ /\ a)$$

Burada, V_{Ref} referans ölçüm sonucu, V_{Att} zayıflatma ölçüm sonucu, a verici anten ile alıcı anten arasındaki mesafe, b de alıcı anten ile kontrollü bölge arasındaki mesafedir.

Bina TEMPEST Değeri

Referans ve zayıflatma ölçüm sonuçları kullanılarak ölçümü yapılan bina veya bölgenin bina değeri belirlenebilir. Bu değer, referans ve zayıflatma ölçüm sonuçlarının ve yayılım yolunun teorik zayıflatmasının birlikte düşünülmesiyle ve ölçüm sonuçlarının yukarıda yazılı zayıflatma formülünde kullanılmasıyla bulunur. Bina değerleri A, B ve C olabilir. A en az, C ise en fazla zayıflatma sağlayan binaya karşılık gelmektedir.

TEMPEST Tesisat Kuralları

Gizli bilgilerin işlendiği binaların ve gizli bilgileri işleyen cihazların değerlerinin belirlenmesi, cihaz ve bina değerlerinin birlikte kullanılarak TEMPEST açısından daha düşük risklere sahip tesislerin yapılmaya çalışılması, TEMPEST bilgi güvenliği açısından en efektif yöntemdir. Bu yöntemde TEMPEST bina değeri iyi olan bölgede TEMPEST cihaz değeri kötü olan cihaz kullanılır veya TEMPEST bina değeri kötü olan bölgede TEMPEST cihaz değeri iyi olan cihaz kullanılır.

Bina değeri iyi olan bir bölgeye sahip olduğumuzda, bu bölgeden havaya yayılım yoluyla bilgi kaçakları oluşma olasılığının çok düşük olduğunu biliyoruz demektir. Bu bölgede cihazların TEMPEST değerlerinin en iyi olması gerekmeyebilir. Ancak bulunduğumuz bölgenin bina değerini doğru seçmemiz gerekir.

Genelkurmay Başkanlığı tarafından yayımlanan MY 401-1(B) yönergesi ve NATO SDIP-29/2 [5] standardında cihazların doğru bölgelere yerleştirilmesi, bina ve cihaz değerlendirmesi ve genel tesisat kuralları yer almaktadır. Cihazların bulundukları bölgelere göre diğer cihaz/kablolardan ne kadar uzağa yerleştirilmeleri gerektiği, güç/veri kablolarının sağlaması gereken özellikler, güç hatlarında filtre kullanılması gerekip gerekmediği, gerekiyorsa bu filtrelerin özellikleri, ekranlı yapılar kullanılması gerekiyorsa bu tür yapıların sağlaması gereken özellikler gibi farklı bazı kurallar, bu yönerge ve standartlardaki kurallara örnek olarak verilebilir. TEMPEST önlemi alan uzmanlar, belirtilen standart ve yönergeler çerçevesinde, ilgili tesis ve binaların durumlarına göre farklı önlemler alabilirler.

Sonuç

TEMPEST önlemleri, sadece cihaz TEMPEST testleri ve cihazların uygun tasarımıyla sınırlı değildir. Aynı zamanda bu cihazların kullanıldığı bina veya bölgelerde de farklı önlemler alınması gerekmektedir. TEMPEST tesis değerlendirme önlemleri kapsamında yapılan bina değerlendirme ölçümleri sonucunda hassas bilginin işlendiği bölgeler için bina TEMPEST değerleri belirlenir. Bu değerler kullanılarak binanın bütünü için bir TEMPEST değer haritası oluşturulur. Böylece elektromanyetik bilgi kaçağı oluşmaması için kullanılacak cihazlar belirlenir. TEMPEST seviyesi kötü olan bölgelerde TEMPEST seviyesi iyi olan cihazlar, TEMPEST seviyesi iyi olan bölgelerde ise daha düşük TEMPEST seviyesi olan cihazlar kullanılabilir. Tesiste gizli verinin işlendiği bütün bölümlerde TEMPEST tesisat kuralları sıkı biçimde uygulanır.

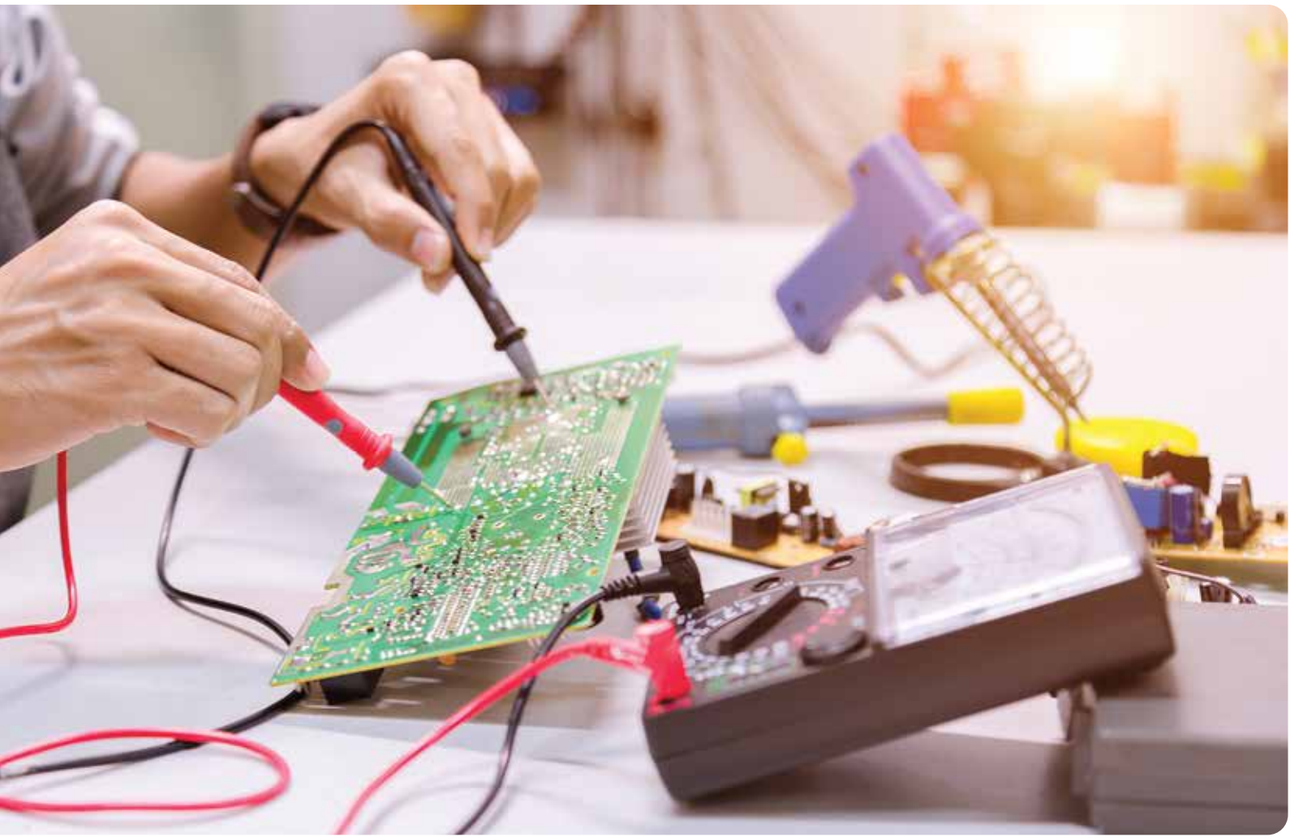
KAYNAKÇA

[1] A. H. Kumbasar, "TEMPEST," UEKAE Dergisi, Cilt 2, Sayı 3, 2010.
[2] MY 401-1 (B), Türk Silahlı Kuvvetleri TEMPEST Yönergesi, 2016.
[3] SDIP 28/2, NATO Zoning Procedures, 2014.
[4] B. Türetken ve A. H. Kumbasar, "Bina TEMPEST Değerlendirme Kriterleri ve Ölçüm Sistemi," UEKAE Dergisi, Cilt 2, Sayı 3, 2010.
[5] SDIP 29/2, Selection and Installation of Equipment for the Processing of Classified Information, 2014.

COMSEC ve Yan Kanal Analizi Faaliyetleri

Ebru Akalp Kuzu-Başuzman Araştırmacı, Uğur Ramazan Kılavuz-Uzman Araştırmacı / BİLGEM TDBY

> Yan Kanal Analizi (YKA), sayısal bir elektronik devrede çalışan şifreleme algoritmasına ait gizli parametre, anahtar, algoritma akışı gibi bilgilerin, cihazın yan kanal olarak adlandırılan giriş ve çıkışlarından faydalanılarak elde edilmesidir.



Yan Kanal Analizi (YKA), sayısal bir elektronik devrede çalışan şifreleme algoritmasına ait gizli parametre, anahtar, algoritma akışı gibi bilgilerin, cihazın yan kanal olarak adlandırılan giriş ve çıkışlarından faydalanılarak elde edilmesidir. Sayısal devreler doğası gereği, çalıştırdıkları algoritmayla ilgili şekilde güç tüketir, ısınır, ses çıkarır veya elektromanyetik yayılım yaparlar. Bu şekilde ortaya çıkan fiziksel değişimlerin hepsi yan kanal çıkışı olarak isimlendirilir. Devrenin, normal giriş çıkışları dışındaki saat, güç girişleri ve hatta devrenin tüm yüzeyi standart dışı sinyallerin uygulanmasına olanak sağlayan birer Yan Kanal girişidir. Bu yan kanallar sayesinde, şifreleme işlemleri sırasında oluşan ara değerler hakkında bilgi sahibi olmak ve algoritma anahtarını parça parça elde etmek mümkündür.

YKA saldırıları literatüre Paul Kocher tarafından 1995 yılında tanıtılmıştır. O zamandan günümüze YKA konusunda akademik olarak geniş bir literatür ve çalışma alanı oluşmuştur. Zaman Analizi (ZA), Basit/Farksal Güç Analizi (BGA, FGA), Basit /Farksal Elektromanyetik Yayınım Analizi, Ses Tabanlı Analiz, Şablon Analizi gibi klasik YKA türleri, yan kanal çıkışlarının gözlenmesine dayandığı için edilgen YKA olarak sınıflandırılır. Algoritma işleyişi sırasında devrenin güç, saat hattına temaslı veya temassız olarak çentik ve sinüs harmonikleri uygulama, devre yüzeyine EM(Elektro Manyetik), lazer ya da iyon atışları yapma sonucunda oluşan hatalı algoritma çıktılarını analiz eden Basit ve Farksal Hata Analizi yöntemleri ise etken YKA olarak sınıflandırılır. Tüm bu klasik YKA türlerinin yanı sıra, yapay zekânın temelinde bulunan güçlü istatiksel yöntemler, etken ve edilgen yan kanal analizinde etkili şekilde kullanılabilmektedir.

YKA Çeşitleri

YKA'da Zaman Analizi (ZA), Basit/Farksal Güç Analizi (BGA, FGA), Basit /Farksal Elektromanyetik Yayınım Analizi gibi edilgen metotlar yer alırken diğer yandan etken olarak gruplandırılan Basit ve Farksal Hata Analizi yöntemleri yer almaktadır.

Basit Güç/EM Analizi

Güç veya güce bağlı değişen bir büyüklüğün (akım, gerilim, elektromanyetik yayılım) bir ya da birkaç adet ölçümünün gözle incelenmesi sonucu yapılan analizdir. Cihazın içerisinde nasıl bir algoritma çalıştığı veya bazı şifreleme algoritmaları için şifreleme anahtarlarının ne olduğu basit güç analizi ile bulunabilir. Tek veya birkaç ölçümden oluşmasından dolayı ölçümün düzgün bir şekilde olabilecek en az gürültü ile alınması gerekliliği, uygulamasını zorlaştırmaktadır. Ancak uygulamada zor olması, buna karşın önlem alınmaması anlamına gelmemelidir.

> Devrenin normal giriş çıkışları dışındaki saat, güç girişleri ve hatta tüm yüzeyi, standart dışı sinyallerin uygulanmasına olanak sağlayan birer Yan Kanal girişidir.

Basit güç analizi, düzgün ölçüm alınması mümkün olan basit entegre devreler ve karmaşık olmayan sistemlerde iyi sonuçlar vermektedir. Sistemler karmaşık hale geldiğinde, yani gizli bilgilerin işlenmesi ve şifrelenmesi dışında cihaza sistem gereksinimlerinden dolayı çok daha fazla görev verildiği durumlarda, aktif olarak değişen transistor ve diğer devre elemanları durumları çok daha kaotik hale gelmektedir. Bu gibi durumlarda, olumsuz çevresel etkenlere rağmen, daha güçlü istatistiksel yöntemler kullanan farksal güç analizi, gizli bilgilerin ortaya çıkarılmasında etkili bir yöntemdir[1].

Saldırgan, algoritma koşturumu sırasında, devrenin ara durumlarındaki sinyal değişimlerini düşünerek, oluşacak kaçak hakkında bir teorik model oluşturur. Bu teorik modeller genelde, alt anahtar parçasının işlem gördüğü saat vuruşundaki güç tüketim değerinin anlık değeri bir olan bit sayısı, yani

"Hamming Weight" ya da anlık bit değişim sayısı yani "Hamming Distance" değeri ile doğru orantılı olduğu varsayımına dayanmaktadır[2].

Saldırganın doğru teorik güç modelini oluşturması için ilgilendiği anahtar parçasını doğru tahmin etmiş olması gerekir. Doğru anahtar kestirimine ait teorik güç modeli, elde ettiği gerçek ölçümle yüksek ilintiye sahip olur. Bu sayede şifreleme adımında kullanılan anahtar, parçalar halinde tahmin edilip doğruluğu sınanarak kırılmış olur. Sistem davranışlarına ait teorik güç modeli oluştururken de anahtarın tamamı değil de daha küçük, yönetilebilir parçaları üzerinde hipotez oluşturma yaklaşımı kullanılmaktadır. Bu sayede gerçek ölçümlerle karşılaştırılması gereken teorik güç modeli sayısı azaltılmış olduğundan çalışma kolaylığı sağlanmaktadır.

Zaman Tabanlı Saldırılar

Saldırganın donanıma erişim imkânının olduğu gömülü sistemlerde elektromanyetik yayılım ve güç tüketimi en önemli yan kanal zayıflıklarındır. Bu iki analizin yanında, zamanlama tabanlı saldırılar da özellikle ağ tabanlı sistemlerde çok daha uygulanabilir bir nitelik kazanmaktadır[7,8]. 2003 yılında Stanford Üniversitesi'nde yapılan araştırma[3], uzaktan yerel ağ üzerinden SSL kütüphanesine ait gizli anahtarların zaman tipi YKA ile kırılabileceğini göstermiştir. Bu araştırma, SSL Kütüphanesi üzerinde ciddi geliştirme ve güncellemelerin yapılmasına sebep olmuştur. Hızlı önbellek (cache memory) kullanan sistemler için ayrıca bir zaman tipi YKA bulunmaktadır. Sistemde çalışan kod bölümlerindeki kayda değer performans farklılıkları, algoritmada kullanılacak verinin hızlı önbellekten mi yoksa ana bellekten mi okunduğuna dair ipuçları içermektedir. Erişilmek istenen veri okunacağı zaman önbellekte yüklü ise hızlı okunmakta ve işlenmekte, ana bellekte ise daha yavaş okunmakta ve işlenmektedir. Bu şekilde yapılacak olan analizlerle okunan veri ve yapılan işlemler hakkında bilgi elde edilebilmektedir[4,9]. Bu tür saldırılar, saldırganın kendi kodunu yükleyebildiği ve mevcut uygulamalar arası davranışı izleyebildiği çok işlemcili sistemlerde kullanılabilir.

Erime ve Görüntü Saldırıları

Son dönemin güncel açıklıklarından olan erime ve görüntü (Meltdown and Spectre) saldırıları, temelde önbellekteki zaman tabanlı yan kanal zafiyetidir. Aktif olarak kullanımda olmasından dolayı bütün modern bilgisayarları, işlemcileri, işletim sistemlerini, mobil cihazları ve bulut sistemlerini etkilemektedir. Meltdown saldırısında, cihazlara yüklü zararlı yazılım ve uygulamalar bellekte ve işletim sisteminde ulaşmaması gereken yerlere erişim sağlayarak cihaz ve kişi için olan gizli bilgilere erişmektedir[5,6].

Modern işlemciler, uygulamaların kullandığı bellek alanlarını ve çıkartacağı sonuçları daha hızlı işlem yapabilmesi için önceden hesaplar. Buna "Speculative Execution" adı verilir. Spectre saldırısı, işte modern işlemcilerin bu özelliklerini kötüye kullanan zaman tabanlı bir YKA saldırısıdır. Saldırganlar, sisteme yükledikleri art niyetli yazılımlarla, spekülatif şekilde doğru programların çalışması sırasında gerçekleşmeyecek olan işlemlerin gerçekleşmesini sağlar. Bu şekilde spekülatif çalışma sonucu oluşan zamanlama bilgilerini kullanarak da diğer uygulamaların gizli verilerine erişirler[6].

TEMPEST ve Siber Güvenlik Saldırıları

Tüm bu standart YKA kanallarına artık TEMPEST ve Siber güvenlik kanalları da eklenerek daha güçlü YKA tipleri ortaya konmaktadır. Normalde YKA kaçağını ölçebilmek için cihaza temas etmek ya da yakın alan EM ölçümleri almak gerekmekte iken, TEMPEST antenleri ve çeşitli sinyal işleme yöntemleri kullanılarak uzaktan da YKA saldırıları uygulanabilir hale gelmiştir [12].

Hatta TEMPEST, Siber Güvenlik ve YKA disiplininin beraber çalıştığı ilginç saldırılar kayıtlara geçmiştir. Örneğin faraday kafesi içinde ve hiçbir ağ bağlantısı olmayan bir bilgisayardan, işlemci yükünü değiştirerek yapılan manyetik yayınımı kontrol eden bir zararlı uygulama, dış dünyaya YKA bilgisi kaçırmada kullanılabilmektedir[13]. Bugün cebimizdeki telefonlar bile taşıdıkları donanımlar ile birer YKA ölçüm ve analiz aracı haline gelmiştir. Literatürde, ses tabanlı YKA kaçağını ölçmek için bir cep telefonunun kullanıldığı çalışmalar vardır [14]. Cep telefonu mikrofonu ile yapılan ölçüm yardımı ile bir diz üstü bilgisayarda çalışmakta olan 2048 bit RSA uygulaması anahtarı elde edilebilmiştir.

YKA saldırılarından korunmak için saklama tabanlı ve maskeleme tabanlı koruma önlemleri mevcuttur [2]. Ancak, yan kanal zayıflıklarını kapatmak için kullanılan çeşitli maskeleme yöntemlerinin de, yapay zekâ kullanılarak kırılabildiğini gösteren çalışmalar mevcuttur[11].

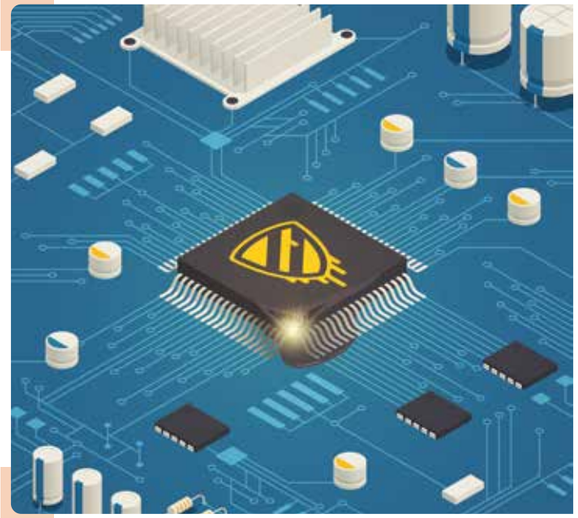
FIPS 140-2 ve onun muadili olan ISO19790 gibi kripto modülleri için güvenlik gereklerini belirleyen standartlarda, YKA saldırılarına karşı dayanıklılık önemli bir yer tutmaktadır. YKA saldırılarının tüm gömülü şifreleme cihazları için de önemli olduğunun görülmesinden dolayı, COMSEC cihaz testlerinde de YKA saldırıları uygulanmaya başlanmıştır. Bugün COMSEC ürün geliştiricileri de, bu durumu göz önünde bulundurarak, YKA'ya dayanıklı maskeli algoritmalar ve diğer önlem türlerini içeren tasarımlar geliştirmektedir.

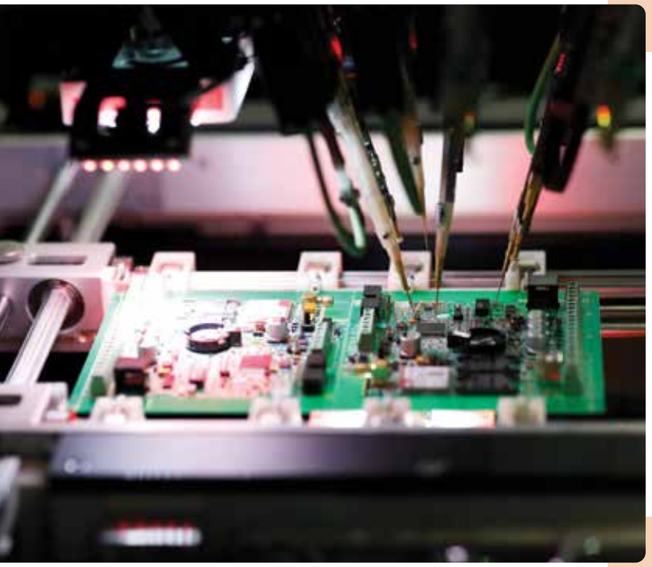
> **"YKA saldırılarının tüm gömülü şifreleme cihazları için de önemli olduğunun görülmesinden dolayı, COMSEC cihaz testlerinde de YKA saldırıları uygulanmaya başlanmıştır. Bugün COMSEC ürün geliştiricileri de, YKA'ya dayanıklı maskeli algoritmalar ve diğer önlem türlerini içeren tasarımlar geliştirmektedir."**

BİLGEM'de YKA Çalışmaları

TÜBİTAK BİLGEM'de YKA çalışmaları, YİTAL tarafından tasarlanan milli akıllı kart tümdevresinin (UKTÜM), EAL5+ seviyesine uyumlu olarak Ortak Kriterler Sertifikası sürecine girmesi amacıyla 2006'da başlatılmıştır.

Ve bu amaçla OKTEM'de geliştirilen ölçüm ve analiz yazılımları, OKTEM ve YİTAL Laboratuva-





rına kazandırılan hazır YKA cihazlarının yanı sıra, UEKAE Lazer Ekibi tarafından, tümdevrelere hata analizi tipi saldırılarda kullanılan ve o zamanki eşdeğerlerine üstünlükler içeren bir lazer cihazı tasarlamıştır. Bu cihaz hala kullanılabilir durumdadır.

BİLGEM'de uygulanan ilk pratik YKA saldırısı, YİTAL ekibi tarafından FPGA tabanlı bir AES devresinden toplanan güç eğrilerinin OKTEM ekibi tarafından FGA saldırısı uygulanarak kırılması ile gerçekleştirilmiştir. Kazanılan bu bilgi birikimi ve sürdürülebilir iş yeteneğinin yanı sıra, çalışmaların kısa vadedeki en önemli sonucu, Türkiye'nin 2010 senesinde Ortak Kriterler Sertifika Üreticisi ülke konumuna yükselmiş olmasıdır. Bu sertifikayı alabilmek için TSE, kendisine bağlı bir Common Criteria (CC) laboratuvarı olan OKTEM laboratuvarının, UKTÜM testleri sırasında yaptığı ve yoğunluklu olarak YKA ve kurcalama tipi saldırılarını içeren çalışmaları kapsamında uluslararası denetleme sürecinden başarıyla geçmiştir. Deneyimlenen süreç ve akabinde ulaşılan bu sonuç Kurumumuzun da içinde olduğu önemli bir başarı olarak nitelendirilebilir.

Bu çalışmaların devamında, OKTEM ve YİTAL ekipleri, tümdevrelere YKA dayanıklılık testlerini gerçekleştirme ve YKA saldırılarına dayanıklı tümdevre ve şifreleme algoritması geliştirme konularında önemli bir bilgi birikimine ulaşmıştır. Kazanılan bu bilgi birikimi ile Kurumumuzdan çeşitli akademik tez çalışmaları, literatüre giren yayınlar hatta patentler ortaya çıkmıştır. Pek çok ülkeye de YKA konusunda eğitim çalışmaları gerçekleştirilmiştir ve halen devam etmektedir. Bu çatı altında yetişen pek çok araştırmacı ile birlikte bu konuda yetkinliğe sahip üniversitelerin yanı sıra başka üniversiteler de bu konu ile tanışmış ve etkin çalışmalar yapmıştır.

BİLGEM TDBY olarak YKA altyapımız, yeniden bir güncelleme sürecine girmiş durumdadır. Gerek duyulan cihazlar laboratuvarımıza kazandırılmakta ya da milli olanaklarla, BİLGEM'deki uzman personeller ve Üniversitelerden uzman hocalardan alınan danışmanlıklarla güncellenmektedir. YKA'nın aslında TEMPEST, EMI-EMC ve Kripto Analiz bacakları olan bir konu olması ve BİLGEM TDBY'nin tüm bu disiplinleri kendi altında toplamış köklü laboratuvarlara sahip olması nedeniyle geleceğin YKA saldırılarını yapmaya aday bir konumda olduğumuzu düşünmekteyiz.

Hedeflerimiz arasında BİLGEM TDBY'de tüm disiplinlerin katkı sağladığı çok daha güçlü YKA yöntemlerinin geliştirilmesi, hem bu yöntemlerin, hem de bu yöntemlerde kullanılan düzeneklerin, analiz yazılımlarının, geliştirilen karşı önlemlerin ürünleştirilmesi bulunmaktadır. Biz araştırmacılar Ar-Ge problemleri hiç tükenmeyen, çok disiplinli boyutları olan böyle bir konuda çalışma imkânına sahip olmanın bir ayrıcalık olduğunun farkındayız.

KAYNAKÇA

1. https://paulkocher.com/doc/DifferentialPowerAnalysis.pdf
2. S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, 2007.
3. https://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf
4. http://cryptocode.net/docs/c38.pdf
5. https://meltdownattack.com/meltdown.pdf
6. https://spectreattack.com/spectre.pdf
7. https://arstechnica.com/information-technology/2015/09/storing-secret-crypto-keys-in-the-amazon-cloud-new-attack-can-steal-them/
8. https://news.softpedia.com/news/cachebleed-openssl-vulnerability-affects-intel-based-cloud-servers-501229.shtml
9. https://bestsecuritysearch.com/android-devices-armaged-don-cache-attack/
10. https://paulkocher.com/doc/TimingAttacks.pdf
11. https://eprint.iacr.org/2018/053.pdf
12. https://resources.fox-it.com/rs/170-CAK-271/images/Tempest_attacks_against_AES.pdf
13. MAGNETO: Covert Channel between Air-GappedSystems and Nearby Smartphones via CPUGenerated Magnetic Fields
14. https://www.cs.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

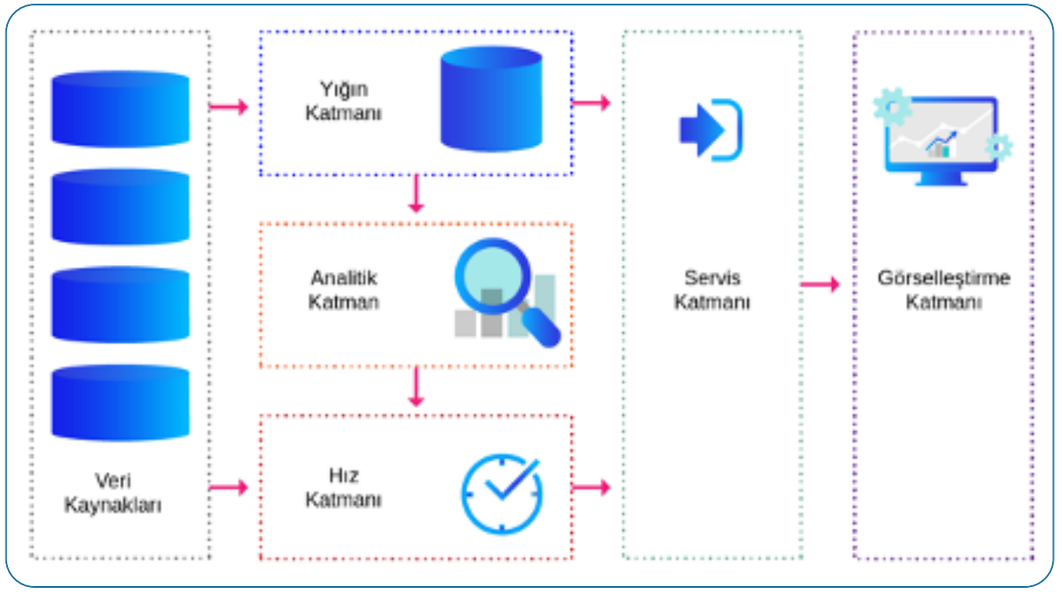
TÜİK Büyük Veri İleri Analitik Projesi

TÜİK Büyük Veri İleri Analitik Projesi ile, Türkiye İstatistik Kurumu (TÜİK) bünyesinde internet sitelerinden toplanan ve diğer kaynaklarla sağlanan kategori ve alt kategori bilgisi ile etiketlenmiş günlük fiyat bilgisinin ve iş ilanlarının yığın ve akan veri olarak büyük veri ekosisteminde depolanması, işlenmesi ve analiz edilmesini sağlayan sistemin tasarlanması amaçlanmaktadır.

Sistem sayesinde, indikatör seçimi, enflasyon tahminleme ve iş ilanından pozisyon ve yetenek sınıflandırması yapılması ve sonuçların görselleştirilmesi mümkün olacaktır.

İnternet sitelerinden toplanan ve diğer kaynaklardan alınan verilerin akan veri biçiminde büyük veri ortamına aktarılması ve aktarılan verilerin yığın ve akan veri olarak analiz edilmesini sağlamak amacıyla Lambda mimarisi kullanılacaktır.

Sistem geliştirme aşamasında, küçük ölçekli demo kurulum TÜBİTAK BİLGEM B3LAB Prototip Veri Merkezi'nde yapılacaktır.



Lambda mimarisi

Kuantum Bilgisayarlar ve Kriptoloji

> 1980'lerde Benioff ve Feynman, kuantum mekaniği ile bilgi saklanabileceği ve işlenebileceği fikrini ortaya attı. Bu fikir o dönem için çok ütopik karşılansa da, günümüzde kuantum bilgisayarlar olarak karşımıza çıktı.

Dr. Kamil Otal - Uzman Araştırmacı / BİLGEM UEKAE

Bilgisayarlar, akıllı telefonlar, tabletler vb. birçok cihaz ile günlük hayatımızda kişisel bilgilerimizi kolayca saklayabilir, işleyebilir ve birbirimize iletebiliriz. Bütün bu cihazlarda hesaplama ve depolama birimi, bit olarak ifade edilir. Bir bitlik hafıza, aynı anda 0 ve 1 değerlerinden yalnızca birini saklayabilir ve dolayısıyla hafızada hangi değer saklıysa ancak o değer işlenebilir. Günlük hayatımızın vazgeçilmez bir parçası olan bu cihazlardaki bit bazlı çalışma prensibi, bellek ve hız kapasitesindeki baş döndürücü gelişmeye rağmen, bilgisayarın icat edildiği ilk günlerden bu yana değişmemiştir.

Peki, bütün hesaplama araçları bit bazlı çalışma prensibiyle işlem yapmak zorunda mı? Bundan yaklaşık kırk sene önce, kuantum fizikçileri Benioff ve Feynman, elektron veya foton gibi atom altı parçacıkların manyetik alanlarının ya da polarizasyonlarının yönleri kullanılarak bilgi saklanabileceği ve işlenebileceği fikrini önerdiler. Bu fikir o dönem için çok ütopik karşılansa da, günümüzde kuantum bilgisayarlar olarak ete kemiğe bürünmüş bir şekilde karşımıza çıktı.

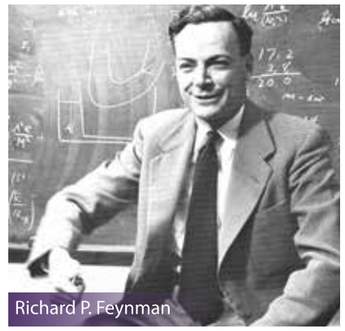
Kuantum Bilgisayarların Çalışma Prensibi

Kuantum bilgisayarlarda atom altı parçacıkların belirli davranışları esas alınır. Çalışma prensibi, klasik bilgisayarlardaki gibi sadece 0 veya sadece 1 değeri taşıyabilen bitlere değil, aynı anda hem 0 hem de 1 değerini taşıyabilen kuantum bitlere (kübitlere) dayanır. Bir kübit ölçüldüğünde belirli bir olasılıkla 0 ve başka bir olasılıkla 1 değeri gözlemlenir. Ölçüm yapmadan hangi değerin gözlemleneceği bilinemez ve ölçüm yaptıktan sonra kübitin başka bir değer alması mümkün değildir. İşte bu hem 0 hem de 1 değerini alabilme özelliğine süperpozisyon, ilk ölçüm yapıldığında belirli bir değer gözlemlenmesine de o değere çökme (collapse) denir.

Dolayısıyla, 10 kübit üzerinde işlem yaparak o 10 kübitin alabileceği 2^10=1024 farklı değer için işlem yapmış oluruz. En son ölçüm yapıldığında 10 kübitlik süperpozisyon, bu 1024 durumdan birine belirli bir ihtimalle çökecektir ve işlemlerin sonucu bu çöken değer olacaktır. Dolayısıyla kuantum bilgisayarda çalışan algoritmalar (kuantum algoritmalar) deterministik değildir, her çalıştırmada aynı sonucu vermeyebilir.

Kuantum algoritmalar, genellikle kübitlerin süperpozisyonlarındaki her bir değerin ihtimali üzerinde aritmetik yapar ve istenen değerin ihtimalini artıracak şekilde komutlar içerirler. Belli sayıda yineleme sonucunda, istenen değerin ihtimalinin kayda değer derecede yüksek olması beklenir. Bu yinelemelerin sonunda ölçüm yapılırsa, kübitlerin süperpozisyonunun istenen değere büyük bir ihtimalle çöktüğü görülecektir.

Kuantum Bilgisayarların Avantaj ve Dezavantajları



Richard P. Feynman

Kübitlerde 0 ve 1 değerinin aynı anda taşınabilmesi, kuantum bilgisayarlara yüksek paralel işlem yapabilme kapasitesi sağlar. Bu avantaj sayesinde, kuantum bilgisayarların çeşitli zor optimizasyon problemlerini çözmek gibi amaçlar için kullanılarak askeri ve endüstriyel alanda hizmet edebileceği düşünülüyor.

Kuantum bilgisayarların en temel dezavantajı ihtiyaç duyulan fiziksel ortamdır. Kuantum bilgisayarların mutlak sıfıra (-273 °C) çok yakın bir sıcaklıkta çalışması gerekir ve bu sıcaklıklar uzayda ulaşılabilecek en soğuk seviyedir. Bunu sağlamak için büyük ve güçlü soğutucu sistemlerine ihtiyaç duyulur. Dolayısıyla, kuantum bilgisayarların akıllı telefonlar veya masaüstü bilgisayarlar gibi doğrudan kişisel olarak kullanılamayacağı, ama internet üzerinden klasik bilgisayarlara uzaktan güçlü hesap hizmeti sunabileceği, bu açıdan bakıldığında ilerde kuantum bilgisayarların ve klasik bilgisayarların bir arada kullanılabileceği söylenebilir.

Kuantum Bilgisayarların Gelişim Durumu

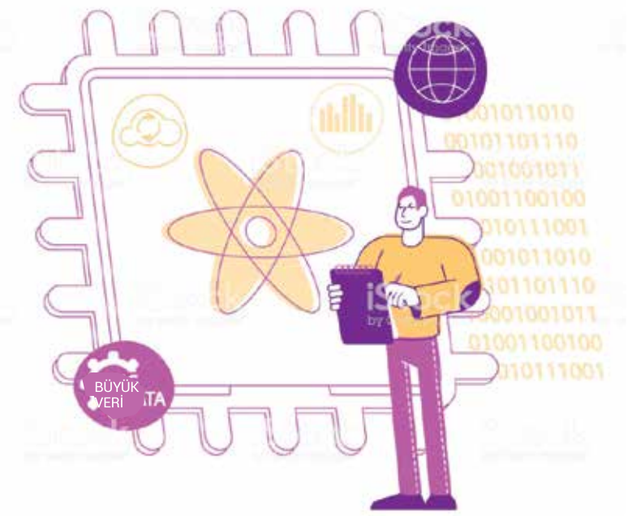
21. yüzyılın başından bu yana, dünya üzerinde birçok şirket ve araştırma kurumu tarafından çeşitli kuantum bilgisayarlar üretilmekte ve geliştirilmektedir. Bu çerçevedeki son gelişmelerden önemli olan ikisini şöyle özetleyebiliriz.

- IBM şirketi 2019 yılında 53 kübitlik kuantum bilgisayar ile internet üzerinden hizmet sunmaya başlayacağını belirtti.
- Yine 2019 yılında, Google firması ürettiği bir kuantum bilgisayarla kuantum üstünlüğü (quantum supremacy) gerçekleştirdiğini iddia etti. (Kuantum üstünlük, klasik bilgisayarlar ile makul süreli bir çözümü olmayan bir problemin kuantum bilgisayar ile çözüldüğünü göstermektir.)

Kuantum Bilgisayarların Kriptoloji ve Bilgi Güvenliği Üzerine Etkileri

Hayatımızın çeşitli alanlarında kişisel bilgilerimizi başkalarıyla paylaşma gereği duyarız ama ilgili kişi haricindekilerin bu bilgileri öğrenmesini istemeyiz. Bu amaçla çeşitli kriptolojik teknikleri bilgisayarlarımızda ve akıllı telefonlarımızda kullanırız. Örneğin e-postalarımızda, bankacılık işlemlerimizde, hatta bazı mesajlaşma uygulamalarında AES ve ECC gibi şifreleme ve imzalama tekniklerini farkında olmadan da olsa kullanırız. Bu teknikler temelde matematiksel olarak çözümü zor problemlere dayanır ve klasik bilgisayarlarla bu problemlerin çözümü imkânsıza yakın olasılıktadır. Bu sebeple yıllardır güvenle bu yöntemleri kullanmaktayız.

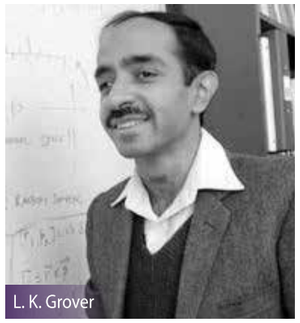
Peki, kuantum bilgisayarlar yüksek hesaplama kapasiteleriyle oyuna girerek bu düzeni etkileyebilir mi? Gündemde olan bu konuda birçok olumsuz senaryodan bahsediliyor. Genel olarak, kuantum bilgisayarların günümüzde kullanılan her türlü şifreleme algoritmasını kırabildiği, buna çözüm olarak da şifreleme yaparken kuantum teknolojisi kullanılması gerektiği şeklinde yaygın bir yanlış algı karşımıza çıkmakta. Oysa günümüzde kullanılan şifreleme algoritmalarının bazıları kuantum bilgisayarlarla yapılabileceği öngörülen ataklara dayanıklı görünüyor. Diğerlerinin yerine de kuantum bilgisayarların kıramayacağı zorlukta problemlere dayanan algoritmalar kullanılarak bu sorunun üstesinden gelinebilir.



Bu konuyu anlamak için öncelikle tehdidin niceliğini anlamamız gerekir. Kuantum tehdidini aşağıda iki farklı ana kriptografik algoritma grubunda ayrı ayrı inceleyeceğiz.

Simetrik Kriptolojide Kuantum Tehdidi

Mesajı şifrelemek için kullanılan anahtar ile şifrelenmiş mesajı açmak için kullanılan anahtarın aynı olduğu veya birbirlerinden kolayca elde edilebildiği şifreleme algoritmalarına simetrik şifreleme algoritmaları denir. İnternet tarayıcılarında ve bulut sistemlerinde kullanılan AES ile 3G teknolojisinde kullanılan KASUMİ gibi şifreleme algoritmaları bu tarz algoritmalara örnek olarak gösterilebilir. Ayrıca özet fonksiyonları gibi bazı kriptografik algoritmalar da bu kapsamda değerlendirilir.


L. K. Grover

Simetrik algoritmaları kırmak amacıyla muhtemel anahtarların hepsini tarama işlemi, anahtar boyuna göre üstel (exponential) bir hesap gücü gerektirir. Örneğin 128-bit anahtar kullanan AES algoritmasıyla şifrelenen mesajları kırmak için 2^{128} farklı anahtarla deneme yapmak gereklidir.

Grover'in tasarımına göre, kuantum bilgisayarlarda bu anahtar tarama işlemi kareköksel miktarda azaltılabilir. Örneğin, 128-bit anahtar kullanan AES algoritmasıyla şifrelenmiş mesajları elde etmek için $\sqrt{2^{128}}=2^{64}$ işlem yeterlidir. Bu durum, saldırgana bir avantaj sağlamasına rağmen problemin zorluğunu üstel zamanlı olmaktan çıkarmaz. Yani n bitlik anahtarı kırma işleminin masrafı klasik bilgisayar için 2^n iken kuantum bilgisayar için yalnızca $2^{(n/2)}$ olur. Bu tehlikenin üstesinden gelmek için daha uzun anahtar boyu kullanan algoritmalar kullanmak yeterlidir. Örneğin 128 bitlik anahtarla çalışan AES algoritması yerine 256 bit anahtarla çalışan AES algoritması kullanılabilir. Böyle bir değişikliğin masrafı, birçok uygulama için ihmal edilebilir miktarda düşüktür.

Asimetrik Kriptolojide Kuantum Tehdidi

Mesajı şifrelemek için kullanılan anahtar bilindiğinde, şifrelenmiş mesajı çözmek için kullanılan anahtarı elde etmenin imkânsıza yakın zorlukta olduğu şifreleme algoritmalarına asimetrik şifreleme algoritmaları denir. Bu algoritmalarda şifreleme anahtarı karşı tarafa gizli olarak iletilmez, açıktan paylaşılır. Bu tarz algoritmalar bazı durumlarda büyük avantaj sağladığı için birçok yerde kullanılır. Elektronik imzalarda kullanılan ECDSA ve şifrelemede kullanılan RSA gibi algoritmalar bu tarz algoritmalara örnek olarak verilebilir.


Peter Shor

Günümüzde kullanılan asimetrik algoritmaları kırmak amacıyla klasik bilgisayarlarda kullanılabilecek şekilde tasarlanan algoritmaların hepsi üstel zamanlı olarak çalışır. Öte yandan, kuantum bilgisayarlarda çalışacak şekilde tasarlanan ve çarpanlara ayırma problemi ile ayrık logaritma problemine dayalı asimetrik şifreleme algoritmalarını, polinomsal zamanda kıran Shor algoritması sebebiyle günümüzde kullanılan ECC ve RSA gibi asimetrik şifreleme algoritmalarının önemli bir kısmı, ciddi miktarda tehlike altına girmiştir. Çünkü daha uzun anahtar boyu kullanarak güvenliği verimli bir şekilde artıramayız, böyle bir uygulamada kuantum bilgisayarı olan saldırganın gücünün ve imkânlarının ötesine gidememiş oluruz. Saldırgan, daha fazla kübitli kuantum bilgisayarlar kullanarak yine algoritmayı kırabilecek noktaya gelebilir. Bu tehdidi ortadan kaldırmak için, kuantum bilgisayarlarda polinomsal zamanda çözülemeyen başka problemlere dayalı asimetrik algoritmalar kullanılabilir.

Bu konuda Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) 2016 yılında bir yarışma süreci başlattı. Süreçte, günümüzde kuantum bilgisayarlar ile polinomsal zamanda çözülemeyen

- Kafes tabanlı (Lattice-based),
- Kod tabanlı (Code-based),
- Özet tabanlı (Hash-based),
- Çok değişkenli polinom tabanlı (Multivariate polynomial-based),
- İzojeni tabanlı (Isogeny-based) vb. matematiksel problemlere dayalı yeni asimetrik şifreleme ve imzalama algoritmalarının seçilerek standartlaştırılması hedefleniyor. Sürecin takvimi şu şekildedir:

- Ağu. 2016: İlk çağrı yapıldı.
- Kas. 2017: İlk başvurular tamamlandı. Toplamda 23 imzalama ve 59 şifreleme algoritması için başvuru yapıldı.
- Oca. 2019: İlk aşama tamamlandı. Başvuran algoritmalardan 9 imzalama ve 17 şifreleme algoritması ikinci aşamaya geçti.
- 2022-2024: Sürecin tamamlanması ve standart olarak belirlenen algoritmaların açıklanması bekleniyor.

Bu sürecin sonucunda ortaya çıkacak algoritmaların, mevcut asimetrik şifreleme algoritmalarının yerine doğrudan kullanılması beklenmiyor. Bunun yerine, mevcut algoritmalarla birlikte hibrit olarak kullanılması planlanıyor. Bu yöntemle, bu yeni algoritmalar için ilerde çıkması muhtemel ataklara karşı dayanıklılık hedefleniyor. Nitekim böyle bir deneyimi, Google firması 2016 yılında Chrome isimli tarayıcısında klasik asimetrik yöntemlerden ECC ve kuantuma dayanıklı olduğu düşünülen yöntemlerden NewHope'u beraber kullanarak başarıyla gerçekleştirdi .

Sonuç olarak, kuantum bilgisayarların kriptoloji ve bilgi güvenliği üzerine etkilerinin, çeşitli medya organlarında iddia edildiği şekilde yıkıcı nitelikte olmayacağı, yine matematiksel problemler ve klasik bilgisayarlar kullanılarak gerekli güvenliğin sağlanmasının mümkün olacağı söylenebilir.

KAYNAKÇA

1. P. Benioff (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics. 22 (5): 563–591.
2. R. P. Feynman (1982). "Simulating physics with computers". International Journal of Theoretical Physics. 21 (6/7): 467–488.
3. L. K. Grover (1996). "A fast quantum mechanical algorithm for database search". Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212.
4. P. W. Shor (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134.
5. https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization (23 Haz. 2020)
6. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html (10 Haz. 2020).

Portreler

1. R. P. Feynman: https://upload.wikimedia.org/wikipedia/commons/0/06/Richard_Feynman_1959.png
2. P.Shor: https://upload.wikimedia.org/wikipedia/commons/e/ed/Peter_Shor_2017_Dirac_Medal_Award_Ceremony.png
3. L. K. Grover: https://miro.medium.com/max/214/1*rszsLVucZRbhSTuOWan3ag.jpeg

Açık Anahtar Altyapısı Temelleri ve Milli Uygulamalar

> Açık Anahtar Altyapısı (AAA), kimlik doğrulama, güvenli veri alışverişi ve güvenli veri depolama gereksinimi olan varlıkların bilgi güvenliğini sağlamak amacıyla kullanılacak asimetrik anahtar çiftlerini ve bu anahtarlara ait elektronik sertifikaları üretmek ve yönetmek için kullanılan sistemlerdir.

Cem Gümüş - Başuzman Araştırmacı, Mehmet Berber – Başuzman Araştırmacı / BİLGEM UEKAE

Açık Anahtar Altyapısı (AAA), kimlik doğrulama ve güvenlik amacıyla kullanılacak elektronik sertifikaların üretilmesi, dağıtılması, kullanılması ve yaşam döngülerinin yönetilmesi için kullanılan sistemlere verilen addır. AAA sistemleri ile ilgili ilk çalışmalar 1970'lerin başında başlamış olsa da, etkin olarak kullanılması 1996 yılında SSL 3.0 standardının [1] yayımlanması sonrasındadır. Ülkemizde bu alandaki ilk çalışmalar 1990'ların sonlarına rastlar [2].

AAA sistemlerinin gelişmesi ve kullanım alanlarının artması üzerine, bu sistemlerin gereksinimlerinin milli yazılım ve donanımlarla karşılanabilmesi amacıyla 1999 yılında TÜBİTAK bünyesinde çalışmalar başlamıştır. TÜBİTAK BİLTEN (UZAY) [3] ve TÜBİTAK BİLGEM UEKAE [4] Milli Açık Anahtar Altyapısı (MA3) [5] grubu tarafından ayrı ayrı yürütülen çalışmalar 2004 yılında birleştirilerek MA3 grubuna devredilmiştir. Geliştirilen yazılımlar ilk olarak, aynı yıl içinde Türk Silahlı Kuvvetleri bünyesinde, güvenli şifreli haberleşme ve dosya koruma için kullanılmaya başlamıştır.

5070 sayılı Elektronik İmza Kanunu'nun [6] 2004 yılında kabul edilmesi ile birlikte kamu kurumlarının ihtiyacı olan elektronik sertifikaları üretmek amacıyla, 2005 yılında Kamu Sertifikasyon Merkezi (Kamu SM) [7] kurulmuştur. Elektronik İmza Kanunu'nun kabulü sonrası, elektronik imza kullanımının yaygınlaşmasına katkı sağlamak için MA3 grubu tarafından E-İmza Kütüphaneleri (MA3 API) [8] geliştirilmiştir.

BİLGEM UEKAE bünyesinde geliştirilen yazılım ve donanımlar; 2013 yılı itibariyle Kuzey Kıbrıs Türk Cumhuriyeti'nde başlanan KKTC Kimlik Kartı (KKTCKK), 2016 yılından itibaren kullanılmaya başlanan Türkiye Cumhuriyeti Kimlik Kartı (TCKK) [9] ve 2018 yılında devreye alınan Türkiye Cumhuriyeti e-Pasaport projelerinde dışa bağımlılığı en aza indirmeyi amaçlamıştır.

Açık Anahtar Altyapısı (AAA) Görevleri ve Bileşenleri

Açık Anahtar Altyapısı (AAA), kimlik doğrulama, güvenli veri alışverişi ve güvenli veri depolama gereksinimi olan varlıkların bilgi güvenliğini sağlamak amacıyla kullanılacak asimetrik anahtar çiftlerini ve bu anahtarlara ait elektronik sertifikaları üretmek ve yönetmek için kullanılan sistemlerdir. AAA sistemlerinin en büyük faydaları, iletişimde yaşanan;

√ Verinin Gizliliği (Confidentiality of Content)
√ Verinin Bütünlüğü (Integrity of Content)
√ Kimlik Doğrulaması (Authentication of Origin)
√ İnkâr Edilemezlik (Non-repudiation)
problemlerine çözüm üretebilmesidir (Şekil 1)

AAA Sistemlerinin Başlıca Görevleri

√ Kimlik doğrulamasının yapılması
√ Anahtarların doğru ve güvenilir bir şekilde oluşturulması

√ Anahtarların güvenli olarak saklanması
√ Anahtarların güvenli olarak geri kazanılabilmesi
√ Sertifika yaşam döngüsünün yönetilmesi
√ Sertifikaların doğrulanabilmesi için gerekli verilerin oluşturulması

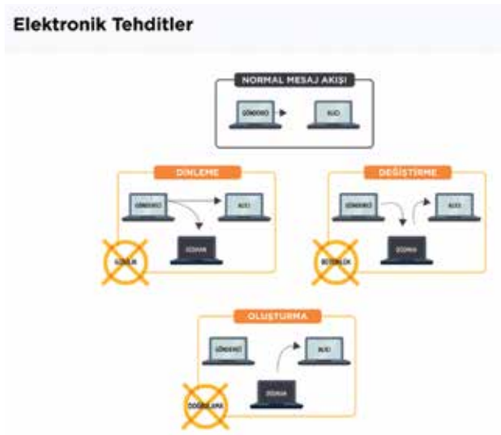
AAA Temel Bileşenleri

Varlık

Kimlik doğrulama, güvenli veri alışverişi veya güvenli veri depolamaya ihtiyaç duyan insanlar ve cihazlardan oluşan gruptur. Gerçek veya tüzel kişi olabileceği gibi ağ veya web sunucuları da bu grupta yer alabilir.

Asimetrik Anahtar Çifti

Varlıklara verilen açık ve özel anahtarlardan oluşan asimetrik anahtar çiftini ifade eder. Sistemin en



Şekil 1. İletişim güvenlik problemleri

Şekil 2. Akis Kart

Şekil 3. N-DIRAK DGM cihazı

kritik bileşenlerindendir. Üretiminin güvenli bir kaynak tarafından yapılması ve özel anahtarın, Donanım Güvenlik Modülü (DGM) ve akıllı kart gibi güvenli cihazlarda tutulması büyük önem arz etmektedir. Özel anahtar, varlık için şifrelenen verinin çözülmesi ya da varlık adına imzalama işlemlerinde kullanılır. Sahip olduğu kritik görevlerden dolayı, özel anahtarın sadece sahibi olan varlık tarafından kullanılması veya erişilebilir durumda olması gerekmektedir.

Elektronik Sertifika

Varlık kimlikleri ile varlığa ait asimetrik anahtar çiftini ilişkilendiren ve kullanım koşullarını gösteren elektronik veridir. Sertifika Makamı adı verilen güvenilir yayımcılar tarafından üretilir ve imzalanır.

Sertifika Makamı

Bir kullanıcı grubu tarafından güvenilen, varlıklar için sertifika ve anahtar çiftini üreten, sertifikanın askıya alınması, askıdan indirilmesi veya iptal edilmesi işlemlerini yöneten, sertifikaların iptal edilmesi sonucu oluşturulan Sertifika İptal Listelerini (SİL) imzalayan sunucudur.

Kayıt Makamı

Varlık ve sertifika kayıtları üzerinde kayıt, güncelleme, onaylama vb. işlemlerin yapılmasını sağlayan sunucudur.

Anahtar Koruma Araçları

Varlıklara ait sertifika ve anahtar çiftlerinin güvenli olarak saklanabilmesi ve kullanılabilmesini sağlayan donanımlara verilen isimdir.

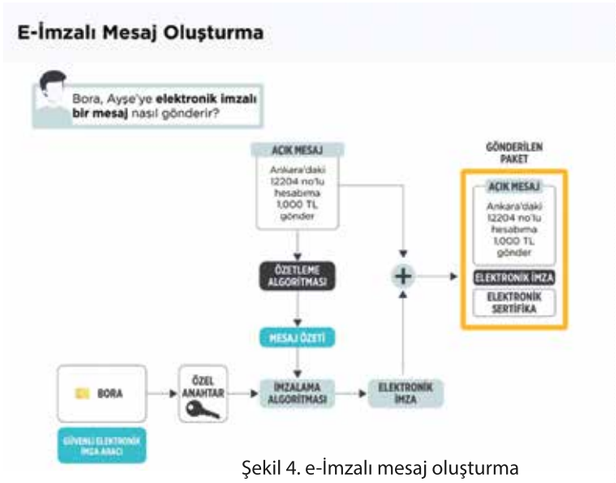
"AAA sistemlerinin gelişmesi ve kullanım alanlarının artması üzerine, bu sistemlerin gereksinimlerinin milli yazılım ve donanımlarla karşılanabilmesi amacıyla 1999 yılında TÜBİTAK bünyesinde çalışmalar başlamıştır."

Akıllı Kart ve Donanım Güvenlik Modülü (DGM) en yaygın kullanılan donanımlardır.

Akıllı kartlar, genellikle kredi kartı boyutunda, içinde özel ve açık alanları bulunan donanımlardır. Akıllı kart, içinde bulunan özel alanlara yetkisiz erişime izin vermez ve bu alana yazılan özel anahtarların dışarı çıkmamasını sağlar. Yetki doğrulaması yapıldıktan sonra, özel anahtarların özelliklerine göre imzalama veya şifre çözme işlemlerini yapabilir. DGM'lere göre performansı kısıtlıdır.

Donanım Güvenlik Modülü (DGM), sisteme veya varlığa ait özel anahtarların güvenli bir şekilde saklanabilmesini ve içinde bulunan rasgele sayı üreteci ile güvenilir anahtar çifti üretilmesini sağlayan yüksek performanslı donanımlardır. Akıllı kartlara göre hızlıdır ve daha çok anahtar saklayabilme özelliğine sahiptir. Bu özelliklerinden dolayı maliyeti akıllı kartlara göre çok yüksektir.

TÜBİTAK BİLGEM UEAKE tarafından milli olarak geliştirilen AKİS [10] Kart (Şekil 2) ve N-DI-



Şekil 4. e-İmzalı mesaj oluşturma

Şekil 5. e-İmzalı mesaj doğrulama

RAK HSM [11] cihazı (Şekil 3) birçok projede aktif olarak kullanılmaktadır.

Sertifika İptal Listesi (SİL)

Sertifika Makamı tarafından imzalanan, içinde bir nedenden dolayı iptal edilerek geçersiz duruma gelmiş sertifikaların bilgilerinin bulunduğu ve sertifika doğrulamada kullanılan dosyalardır.

Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP)

Sertifika Makamı tarafından üretilmiş sertifikalara ait durum bilgisinin anlık olarak sorgulanabilmesini sağlayan sunucudur.

Açık Anahtar Altyapısı Kullanım Alanları

AAA tarafından üretilen elektronik sertifikalar günlük hayatta elektronik imzalama, şifreleme ve zaman damgası gibi alanlarda sıkça kullanılmaktadır. Bu hizmetleri sırasıyla inceleyelim.

Elektronik İmza ve Sunduğu Hizmetler

Elektronik imza, dijital ortamda bir elektronik verinin, Elektronik İmzalama Sertifikasına sahip varlık tarafından onaylandığını ya da kabul edildiğini göstermektedir. Elektronik imza, verinin içeriği kullanılarak oluşturulur ve bu sayede verinin değiştirilmediğini ispat eder.

Elektronik İmza işleminde, özet alma fonksiyonları kullanılarak verinin özeti alınır ve bu özet varlığa ait özel anahtar kullanılarak imzalanır. Elektronik İmza ile bir veri imzalandığında, veri üzerinde;

- √ Veri Bütünlüğü,
- √ Kimlik Doğrulama,
- √ İnkâr Edilemezlik sağlanmış olur.

Elektronik imza oluşturabilmek için, imzalama işlemini yapacak varlığa ait özel anahtar, açık anahtar ve bu anahtarlar için üretilmiş elektronik sertifikası bulunmalıdır.

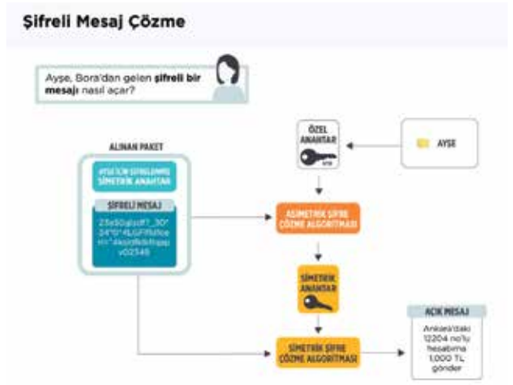
Verinin değişmediğini ve veri bütünlüğünün korunduğunu kanıtlamak için yapılan Elektronik İmza işleminde, imzalanacak verinin boyutunun yüksek olması nedeniyle hız ve kaynak gibi problemler yaşamamak için özet fonksiyonları kullanılır.

Özet fonksiyonu, farklı uzunluktaki verilerden, matematiksel fonksiyonlar kullanarak, o veriye özel, sabit uzunlukta bir değer üretme işlemine verilen addır. Tek yönlü çalışan bir fonksiyondur. Özet değer ile veri arasında bir ilişki kurulamamakta ve özet değerinden veriye ulaşılamamaktadır. Veri üzerinde yapılan ufak bir değişiklik sonrası veri için özet fonksiyonu çalıştırılırsa, özet değeri tamamen farklı olmaktadır. Bir veri elektronik olarak imzalandıktan sonra, veri üzerinde yapılan herhangi bir değişiklik, elektronik imzanın doğrulanamamasına neden olacaktır.

Elektronik İmzalı Mesaj Oluşturma

Elektronik imzalı yapılacak mesajlaşma işleminde, ilk olarak imzalanacak mesajın özeti alınarak özet değeri hesaplanır. Elektronik imzalama işlemini yapacak varlığa ait özel anahtar kullanılarak özet de-

Şekil 6. Şifreli mesaj oluşturma



Şekil 7. Şifreli mesaj çözme

ğeri imzalanır. Mesaj, elektronik imza ve imzalama işleminde kullanılan anahtara ait elektronik sertifika birleştirilip imzalı veri paketi oluşturularak alıcıya gönderilir (Şekil 4).

Elektronik İmzalı Mesaj Doğrulama

Elektronik imzalı olarak gelen bir mesajın doğrulanması işleminde, ilk olarak imzalı veri paketi içinden imzalama yapan varlığa ait sertifika alınarak geçerlilik kontrolleri yapılır. Sertifikanın geçerliliği ve güvenilir bir kök tarafından üretilip üretilmediği kontrol edildikten sonra, sertifika içinden açık anahtar alınır. Açık anahtar ile Elektronik İmza verisi doğrulanır. Elektronik imza doğrulaması sonucu elde edilen onaylanmış özet ile mesajın özeti karşılaştırılır. Bu özet değerleri aynı olursa imza doğrulanmış olur (Şekil 5).

Şifreleme ve Sunduğu Hizmetler

Verinin, araya girecek kötü niyetli kişiler tarafından ele geçirilse bile anlamlı bir bilgi edinilmesini önleyecek biçimde değiştirilmesi işlemine şifreleme denilmektedir. Şifreleme işleminde simetrik kriptografi ve asimetrik kriptografi beraber kullanılmaktadır. Simetrik kriptografi, asimetrik kriptografiye göre hızlıdır, fakat tek başına kullanıldığında anahtar yönetimi zordur. Asimetrik kriptografide ise anahtar yönetimi kolaydır, fakat şifreleme hızı simetrik kriptografi ile şifrelemeye göre yavaştır. Bu nedenle iki yöntem birleştirilerek, iki yöntemin de avantajlarından yararlanılmaktadır.

Şifreli Mesaj Oluşturma

Şifreli mesaj oluşturma işleminde, önce yeni bir simetrik anahtar üretilir. Üretilen bu simetrik anahtar kullanılarak mesaj şifrelenir. Mesaj şifreleme işlemi tamamlandıktan sonra, mesajı şifrelemekte kullanılan simetrik anahtar, mesajın gönderileceği varlığın

> **BİLGEM UEKAE bünyesinde 2000 yılından beri faaliyet göstermekte olan MA3 grubu, AAA sistemlerinde kullanılmak üzere standartlara uyumlu çeşitli yazılımlar geliştirmiş ve geliştirmeye devam etmektedir.**

açık anahtarı kullanılarak şifrelenir. Şifreli veri ve şifrelenmiş simetrik anahtar birleştirilerek şifreli mesaj paketi oluşturulur ve güvenli mesajlaşma yapılacak varlığa gönderilir (Şekil 6).

Şifreli Mesaj Çözme

Şifreli mesajın çözülmesi işleminde, şifreli mesaj paketinden ilk olarak şifreli simetrik anahtar verisi alınır. Şifreli simetrik anahtar verisi, verinin şifrelendiği varlığa ait özel anahtar ile çözülür ve mesajı şifrelemekte kullanılan simetrik anahtar elde edilir. Şifreli mesaj paketi içinden simetrik anahtar ile şifrelenmiş veri alınır. Simetrik anahtar kullanılarak şifreli mesaj çözülür ve mesaj elde edilir. Bu sayede mesaj güvenli bir şekilde taşınmış olur (Şekil 7).

Zaman Damgası ve Sunduğu Hizmetler

Zaman Damgası verinin belli bir tarihte mevcut ve değişmemiş olduğunu kanıtlamak için kullanılmaktadır. 5070 sayılı Elektronik İmza Kanunu'na göre Zaman Damgası; bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından Elektronik İmza ile doğrulanan kaydı ifade etmektedir.

Zaman Damgası alınması işleminde; damgalanacak verinin özeti hesaplanır ve zaman damgalama işlemini yapacak sunucuya gönderilir. Zaman Damgası Sunucusu, kendisine gelen veriyi ve güvenilir bir kaynaktan aldığı zaman bilgisini birleştirip imzalar ve talebi yapan varlığa geri gönderir. Bu sayede verinin, Zaman Damgası alındığı tarihte var olduğu kanıtlanabilir.

Açık Anahtar Altyapısı Uygulamaları

TÜBİTAK BİLGEM UEKAE bünyesinde 2000 yılından beri faaliyet göstermekte olan MA3 grubu, AAA sistemlerinde kullanılmak üzere standartlara uyumlu çeşitli yazılımlar geliştirmiştir ve geliştirmeye devam etmektedir. Bu yazılımlar aşağıda kısaca anlatılmıştır.

MA3 API

ETSI (AB) Standartları'nda Elektronik İmza atılmasını sağlayan milli yazılım kütüphanesidir [8]. PKCS11 uyumlu akıllı kartlarla çalışmayı sağlamakta, Temel İmza (ES-BES), Zaman Damgalı İmza (ES-T), Uzun Dönemli İmza (ES-XL) ve Arşiv İmza (ES-A) gibi birçok imza tipini ve CAdES, PAdES ve XAdES gibi imza formatlarını desteklemektedir.

ESYA (Elektronik Sertifika Yönetim Altyapısı)

Uluslararası standartlara uygun olarak, elektronik sertifikaya gereksinim duyan varlıkların ve bu varlıklar için üretilen elektronik sertifikaların yaşam döngüsünün yönetilmesini sağlayan ulusal yazılımdır. Certificate Issuing and Management Components (CIMC) Protection Profile uyumlu Common Criteria EAL 4+ sertifikasyonu bulunmaktadır.

Zaman Damgası Sunucusu

RFC 3161 standartlarına uygun olarak Zaman Damgası üretilmesini sağlayan sunucudur. Network Time Protocol (NTP) desteği vardır. Yük dengeleme ve eş zamanlı istekleri paralel işleme için Master/Slave modunda çalışabilme yeteneği bulunmaktadır. Müşteri yönetiminin kullanıcı dostu arayüz ile yapılmasını sağlar.

İmzager

Elektronik İmza oluşturulmasını, mevcut imzaların görüntülenip doğrulanmasını, imza eklenmesini ve yönetilmesini sağlayan masaüstü uygulamasıdır [12]. Seri, paralel, ayrık, tümleşik gibi birçok imza tipini desteklemektedir. Gelişmiş imza tipleri için Zaman Damgası desteği de bulunmaktadır.

Kermen

Sertifika tabanlı asimetrik şifreleme ve imzalama özelliklerini kullanarak, kullanıcılara verileri güvenli bir şekilde saklama ve paylaşma olanağı sunan masaüstü yazılımıdır.

KAYNAKÇA

[1] https://tools.ietf.org/html/rfc6101
[2] "Türkiye için bir Açık Anahtar Altyapısı Modeli", Bilişim 98, TBD 15. Bilişim Kurultayı, 1998, Istanbul, sayfa 354 – 361
[3] https://uzay.tubitak.gov.tr
[4] https://bilgem.tubitak.gov.tr
[5] https://ma3.bilgem.tubitak.gov.tr
[6] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf
[7] http://kamusm.gov.tr
[8] https://yazilim.kamusm.gov.tr/?q=/node/14
[9] https://www.nvi.gov.tr/tc-kimlik-karti
[10] http://www.akiskart.com.tr
[11]https://bilgem.tubitak.gov.tr/tr/icerik/network-hsm-ag-tipi-donanim-guvenlik-modulu
[12] https://yazilim.kamusm.gov.tr/?q=/node/5

Güvenli Yazılım Geliştirme Süreçleri ve Olgunluk Modelleri

> **Bir yazılımın temel amacı, müşterinin ya da hedef kitlenin istekleri/ihtiyaçları doğrultusunda güvenliği tasarlanmış işlevsellik sunmaktır.**

Süleyman Muhammed Arıkan - Uzman Araştırmacı, Tolga Yılmaz - Uzman Araştırmacı, Özgür Yürekten - Başuzman Araştırmacı / BİLGEM SGE

Bilişim sistemleri tarafından kullanılan yazılımlar; programlar, kütüphaneler, dijital ortam, çevrimiçi dokümanlar ve veri gibi bileşenlerden meydana gelir. Bileşenlerin farklı donanım ve işletim sistemlerinde çalıştığı, farklı programlama dilleri (Java, C#, Python vb.) ile geliştirildiği, farklı derleyiciler ve bütünleşik geliştirme ortamları (IDE) ile oluşturulduğu ya da farklı girdi çıktı dilleri (JSON, XML vb.) üzerinden kullanıldığı düşünüldüğünde karmaşık, katmanlı bir yapının karşımıza çıktığı görülebilir.

Bu katmanlar, yazılımı birçok açıdan dış müdahalelere karşı hassaslaştırmasına rağmen çoğu yazılım geliştirme projesinde, yazılımların güvenliğine işlevsellikle aynı oranda önem verilmemektedir. Bir yazılımın temel amacı, müşterinin ya da hedef kitlenin istekleri/ihtiyaçları doğrultusunda güvenliği, tasarlanmış işlevsellik sunmaktır. Fakat yazılımların güvenliği tasarım ve geliştirme aşamasında çoğunlukla dikkate alınmamakta, daha sonra eklenebilecek bir özellik ve ikincil bir uğraş konusu olarak algılanmaktadır. Bu durum da yazılım ürünlerinde telafisi zor ve giderilmesi maliyetli güvenlik açıklarına sebep olmaktadır. Bu sorunları önlemek, yazılımın bilgi güvenliği saldırılarına (bütünlük, erişilebilirlik, gizlilik) karşı daha dirençli çalışmasını sağlamak ve saldırı/tehdit altındayken işlevlerini doğru bir şekilde yerine getirmeye devam etmesi için yazılım güvenliği pratikleri kullanılmalıdır.

Yazılım Geliştirme Yaşam Döngüsü

Yazılım güvenliği; bir yazılımın tüm parçalarıyla birlikte geliştirilmesi, çalışır hale getirilmesi, müşteriye sunulması, işletilmesi ve sonlandırılması gibi süreçlerin tümüyle ilişkilidir. Dolayısıyla yazılımda güvenliği sağlamak için Yazılım Geliştirme Yaşam Döngüsü (YGYD) süresince yazılım güvenliği pratikleri uygulanmalıdır.

YGYD; müşteri beklentilerini karşılayan, zaman ve maliyet tahminlerine göre tamamlanan kaliteli yazılımlar üretmek amacıyla kullanılır. Yazılımlar için; planlama, analiz, tasarım, geliştirme, test, kurulum ve bakım gibi temel aşamaların tümü YGYD kapsamındadır. Bu aşamalar modelden modele farklılık gösterebilir. Yazılım geliştirme sürecinde sıklıkla tercih edilen yaşam döngüsü modellerine; şelale (waterfall) modeli, tekrarlı ve artımlı (iterative and incremental) model, spiral model, v-modeli, prototip modeli ve büyük patlama (big bang) modeli örnek olarak gösterilebilir.

Şelale modeli, birbirinin peşi sıra ilerleyen, seri süreçlere sahip, basit ve uygulaması, kolay bir model olduğundan gereksinimleri tam anlamıyla anlaşılan projelere oldukça uygundur.

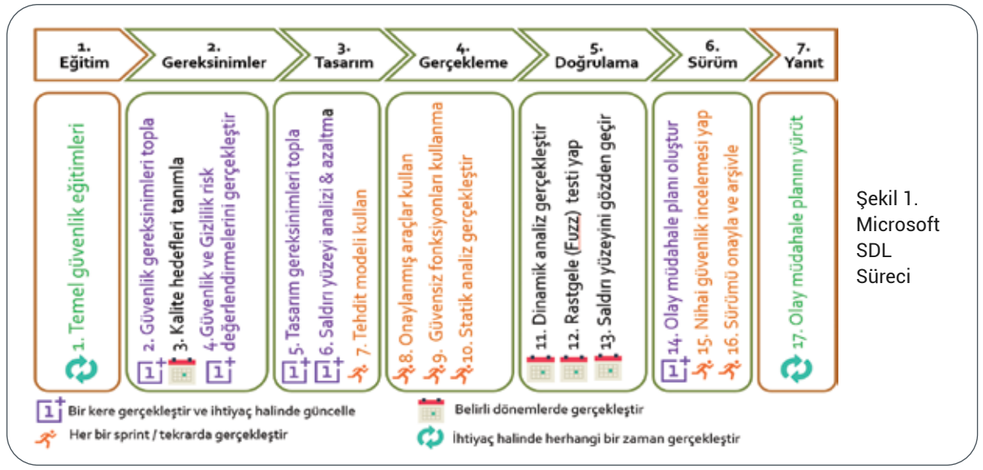
Tekrarlı ve artımlı model, başlangıç aşamasında hızlıca çalışır halde prototip fonksiyonların geliştirilebildiği, müşterinin erken aşamalarda geri dönüş vermesine imkan sağlayan ve paralel geliştirme planlamasına müsait yapısından dolayı karmaşık ve büyük projeler için kullanılabilen bir modeldir.

Spiral modelde, yazılımlar parçalı olarak geliştirildiği için süreçler daha şeffaftır ve müşteri, erken aşamalarda ürünü kısıtlı olarak kullanabildiğinden geri dönüşte bulunabilir.

V modeli, test aktivitelerinin erken aşamalarda başlamasından dolayı problemlerin daha çabuk fark edilebilmesini sağlayan, uygulaması basit bir modeldir.

Prototip model, müşteri memnuniyetini daha erken aşamada sağlayarak yazılımın reddedilme ihtimalini azaltan ve eksik olan parçaların çabuk fark edilebildiği bir modeldir.

Büyük patlama modeli ise; belirli bir süreç takip etmeden, tam anlamıyla belirli olmayan gereksinimleri yazılıma dönüştürmeyi amaçlayan, yüksek riske sahip bir model olduğundan, küçük ölçekli/kısa süreli projeler için denenebilir bir modeldir.



Şekil 1. Microsoft SDL Süreci

Süreçler ve Olgunluk Modelleri

Kurum ve proje ihtiyaçları göz önünde bulundurularak yazılım geliştirme sürecinde kullanılmasına karar verilen YGYD boyunca, yazılım güvenliği pratiklerini uygulamak ve mevcut durumu analiz etmek amacıyla, ticari veya kar amacı gütmeyen kuruluşlarca sunulmakta olan çeşitli güvenli yazılım geliştirme süreçlerinden ve olgunluk modellerinden faydalanılabilir.

Süreçler güvenli yazılıma ulaşmak için gerçekleştirilecek çeşitli faaliyetleri tanımlarken, olgunluk modelleri güvenlik açısından yazılımın farklı yönlerini ölçebilecek analiz yöntemleri sunar. Bu çerçevede, güvenli yazılım geliştirme için tanımlanmış süreç ve olgunluk modellerine Microsoft SDL, OWASP SAMM, BSIMM ve SAFECode örnek olarak gösterilebilir.

Microsoft SDL

Microsoft Security Development Lifecycle (SDL), geliştiricilerin daha güvenli yazılımlar oluşturmalarına ve geliştirme maliyetlerini düşürmelerine yardımcı olan bir yazılım geliştirme sürecidir. Klasik spiral modele dayanan Microsoft SDL, güvenlik ve gizliliği erken safhada ve gelişim sürecinin tüm aşamalarında göz önünde bulundurur. İlk sürümünün sunulduğu 2008 yılından bu zamana; bulut, nesnelerin interneti (internet of things) ve yapay zekâ gibi farklı teknolojiler için çeşitli güncellemeler yapılmıştır. Microsoft yazılım kültürüne güvenlik ve gizlilik yerleştirmede kritik rol oynayan Microsoft SDL, bütünsel ve pratik bir yaklaşım sunarak geliştirme sürecinde radikal değişiklikler gerektirmez. Bünyesinde barındırdığı 7 faz ve 17 pratik Şekil 1'de gösterilmiştir.

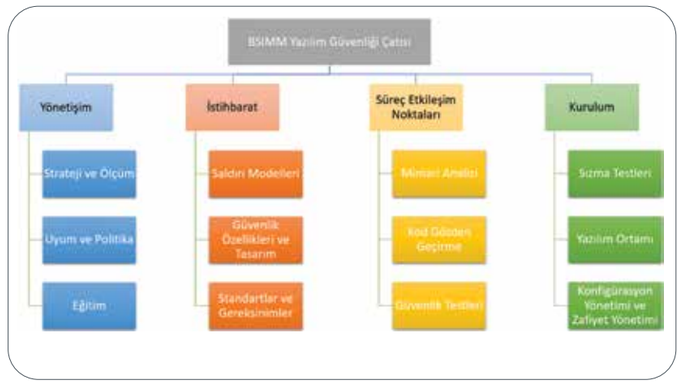
BSIMM

The Building Security In Maturity Model (BSIMM) yazılım güvenliği çatısı, yazılım güvenliği için yapılması gereken faaliyetleri tanımlamaktan ziyade, sektörde yer alan firmalar tarafından uygulanmakta olan mevcut faaliyetleri raporlamaktadır. Modelin 2020 yılı itibari ile güncel olan BSIMM10 versiyonunda, 122 firma ile yapılan görüşmelerin sonuçları bulunmaktadır. Görüşmeler neticesinde tespit edilen faaliyetler yönetişim, istihbarat, süreç etkileşim noktaları ve kurulum olmak üzere 4 adet bilgi alanı altında gruplandırılır. Bu kapsamda; bir yazılım güvenliği sürecini yönetmek ve ölçmek için yönetişim, ilgili bilgilerin toplanması ve işlenmesi için istihbarat, yazılım geliştirme çıktıları ve süreçlerine ilişkin analiz ve güvence sağlamak için süreç etkileşim noktaları, yazılımın kurulum ve bakım faaliyetleri için ise kurulum bilgi alanından faydalanılabilir.

BSIMM yazılım güvenliği çatısında, her bir bilgi alanı 3 uzmanlık alanına, her uzmanlık alanı da 3 seviyeye ayrılırken her seviye 2 ila 6 arasında eylem barındırmaktadır. İlgili bilgi ve uzmanlık alanları Şekil 2'de görülebilir.

SAFECode

SAFECode, etkin yazılım güvencesi yöntemlerinin geliştirilmesi yoluyla bilgi ve iletişim teknolojisi ürünlerine ve hizmetlerine duyulan güveni artırmak için 2007 yılında Nokia, SAP, Symantec, Microsoft, EMC ve Juniper Networks işbirliği ile, endüstri tarafından yönlendirilen ve kâr amacı gütmeyen bir konsorsiyum olarak kurulmuştur. Yazılım, donanım ve hizmetlerin daha güvenli geliştirilmesi/sağlanması için işletilebilecek en iyi faaliyetleri belirlemeyi hedeflemektedir. Alan uzmanlarının tecrübelerine dayanarak belirlenen en iyi faaliyetler; Güvenli Yazılım Geliştirme için Temel İlkeler, Yazılım Güvence Değerlendirme İlkeleri ve Bulut Uygulamalarının Güvenli Geliştirilmesi için İlkeler gibi çeşitli yayınlar üzerinden paylaşılmaktadır. Paylaşılan tüm yayınlara, SAFECode'un resmi web sitesi üzerinden ücretsiz olarak ulaşılabilir.



Şekil 2. BSIMM Bilgi ve Uzmanlık Alanları

OWASP SAMM

The Open Web Application Security Project (OWASP), kar amacı gütmeden yazılım güvenliğini geliştirmeye odaklanmış bir organizasyondur. Dünya çapındaki kuruluşlara, üniversitelere ve bireylere yazılım güvenliği için tarafsız ve pratik bilgiler sunmak amacıyla, yazılım güvenliği konusunda birçok uzmanın görüşü doğrultusunda bilgi tabanlı belgeler yayımlar. Bazı OWASP ürünlerine; OWASP Top 10, Offensive Web Testing Framework (OWTF), Application Security Verification Standart (ASVS) ve The Software Assurance Maturity Model (SAMM) örnek olarak gösterilebilir.

Yazılım güvenliği için bir strateji oluşturmak ve uygulamak için kullanılan SAMM, kuruluşların karşılaştığı risklere odaklanan bir çerçevedir. Bu çerçeve ile bir organizasyondaki güvenlikle ilgili yapılması gereken faaliyetler tanımlanabilirken, mevcut yazılım güvenliği faaliyetleri de değerlendirilebilir. Ayrıca, dengeli bir yazılım güvenliği güvence programı oluşturulabilir ve/veya mevcut yazılım güvenliği güvence programında iyileştirmeler yapılabilir.

SAMM modelinde, kuruluş için olgunluk seviyeleri tanımlanarak güvenlik pratiklerinin kazanılması için yol haritası çizilir. Bu kapsamda, her güvenlik pratiği için üç olgunluk seviyesine (1,2 ve 3) ek olarak bir başlangıç seviyesi (0) tanımlanmıştır. İlgili pratik için; modelin kullanılmasından önce kurumun durumunun ölçüldüğünü belirten 0. Seviye, deneme uygulamalarının yapıldığını belirten 1. Seviye, modelin etkin olarak uygulandığını belirten 2. Seviye ve modelin tüm detayları ile uygulandığını belirten 3. Seviye düzeyleri tanımlanmıştır. İlgili iş fonksiyonları ve güvenlik pratikleri Şekil 3 üzerinde gösterilmiştir.

Sonuç

Gerçekleşmesi muhtemel saldırılara karşı çeşitli önlemlere sahip, saldırıyı önleyemese dahi saldırıya rağmen çalışma sürecini doğru bir şekilde devam ettirebilecek mimariyi/tasarımı kullanan yazılımın geliştirilmesi amacıyla, güvenli yazılım geliştirme süreçleri ve olgunluk modellerinden faydalanılabilir. Mevcut süreçler, yazılım yaşam döngüsü boyunca göz önünde bulundurulması ve/veya uygulanması gereken güvenlik faaliyetlerini tanımlamaktadır. Bu güvenlik faaliyetleri yardımıyla, güvenli yazılım geliştirme ile ilgili süreçler daha kolay işletilebilir.

Şekil 3. OWASP SAMM İş Fonksiyonları ve Güvenlik Pratikleri

Mevcut olgunluk modelleri ise, yazılım güvenliği pratiklerinin ne derecede uygulandığını ortaya koyan, derecelendirmeye dayalı ölçüm modelleri sunmaktadır. Bu modeller kullanılarak, yazılımın geliştirme sürecinde uygulanan güvenlik pratiklerinin durumu ölçülebilir. Çalışmaya konu olan güvenli yazılım geliştirme süreçleri ve olgunluk modelleri ışığında:

- Ağırlıklı olarak endüstri pratiklerini takip etmek ve uygulamak için BSIMM,
- Güvenli yazılım geliştirme pratiklerini ağırlıklı olarak hazır araçlar ile takip etmek için Microsoft SDL,
- Kurumsal güvenli yazılım geliştirme olgunluğunu, başarı kriterleri, kontrol listeleri ve değerlendirme metodolojileri kullanarak artırmak için OWASP SAMM,
- Çalışmaları, en temel düzeydeki güvenli yazılım geliştirme faaliyetlerini dikkate alarak yürütmek için SAFECode yayınlarının kullanılması, uygun birer seçenek olarak görülmektedir.

KAYNAKÇA

1. https://www.microsoft.com/en-us/sdl
2. https://www.bsimm.com/
3. https://safecode.org/
4. https://www.owasp.org/index.php/OWASP_SAMM_Project
5. BİLGEM Güvenli Yazılım Geliştirme Kılavuzu Rev1.1

Siber Güvenliğin Koruması Gereken Yeni Alan:

Yapay Zekâ

> Yapay zekâ artık sadece araştırma merkezleri ve üniversitelerde kullanılır olmaktan çıkmış; lojistik, sağlık, otonom araçlar gibi birçok ticari alanda da kullanılmaya başlanmıştır.

Doç. Dr. Ferhat Özgür Çatak – Başuzman Araştırmacı / BİLGEM SGE

Yapay zekâ konusu, kökeni çok eskilere dayanıyor olsa da en büyük ilerlemesini son 10 yılda gerçekleştirmiştir. Artık sadece araştırma merkezleri ve üniversitelerde kullanılır olmaktan çıkıp lojistik, sağlık, otonom araçlar gibi birçok ticari alanda da kullanılmaya başlanmıştır. Günümüzde bu kadar yaygınlaşmasının başlıca nedenlerinden bir tanesi, günümüz bilgisayarlarının hesaplama gücünün, bu algoritmaların tasarlandığı zamana göre çok ilerlemiş olmasıdır. Sahip olduğumuz yüksek kapasiteli bilgisayarlar ve depolama üniteleri sayesinde, algoritmaların ihtiyaç duyduğu yüksek miktarda veriyi kayıt altına alarak sadece bilgisayarların merkezi işlemcilerinde değil, aynı zamanda grafik kartlarının sahip olduğu grafik işleme birimleri (Graphical Processing Unit – GPU) kullanılarak eğitim aşaması gerçekleştirilmekte ve günler veya haftalar sürecek bu faz, saatler veya dakikalar seviyesine düşürülebilmektedir.

Arkalarındaki matematiksel temeller birkaç on yıl önce geliştirilmiş olsa bile, güçlü GPU'ların nispeten yeni ortaya çıkışıyla beraber, bu alanda yer alan araştırmacılar, karmaşık makine öğrenme sistemlerini denemek ve oluşturmak için gerekli hesaplama gücünü yeni elde etmişlerdir. Bugün, bilgisayarla görü için kullanılan VGG19, ResNet, DenseNet ve Inception gibi son teknoloji modelleri, birkaç milyon parametre içeren derin sinir ağlarından oluşmaktadır ve sadece on yıldır mevcut olan bir donanıma dayanmaktadır.

Yapay zekâ alanında gerçekleşen bu göz kamaştırıcı ilerlemeye rağmen, diğer yeni teknolojilerin göz ardı ettiği ve ilerleyen zamanlarda büyük problemler yaşadığı güvenlik konusu, yine ihmal edilmektedir. TCP/IP protokolü, ilk tasarlandığı zaman, ölçek olarak oldukça az sayıda bilgisayarın bağlı olduğu bir ağ üzerinde olması nedeniyle güvenlik konusu düşünülmeden geliştirilmiştir. İnternet'in ölçek ve karmaşıklığının hızla artmasıyla beraber, tasarımcıların öngöremediği bu protokol eksikliklerinden faydalanan saldırganlar, günümüzde etkilerini hala sürdürebilmektedir.

Benzer bir durum yapay zekâ için de geçerlidir. Makine öğrenme algoritmalarının hemen hemen tamamı, çeşitli güvenlik zafiyetleri içermektedir. Genellikle bu saldırıların tümü algoritmanın eğitim veya sınıflandırma aşamalarında saldırgan girdi örneklerini (adversarial instances) kullanarak modelin manipülasyonunu hedeflemektedir.

Saldırgan girdi örnekleri, makine öğrenme modellerini kandırmak için tasarlanmış kötü niyetli girdilerdir. Bir saldırganın bakış açısıyla, yanlış sınıflandırılmış bir örnekle bir tespit sistemini atlatmaya ya da makine öğrenmesi modelini eğitim aşamasında tutarlı bir şekilde yanlış sınıflandıracak şekilde öğrenmeye zorlayabilirler.

Örnek Saldırı

Günlük yaşantımızdan bu duruma verilebilecek en iyi örnek siber güvenlik bileşenleridir. Kurumsal ağlar üzerinde makine öğrenme modellerine dayalı olarak çalışacak IPS/IDS sistemlerinin, kurulum yapıldıkları yaklaşık 3 ay süresince ağ üzerinde veri toplama ve öğrenme sürecine devam edeceği, ilgili ticari üreticiler tarafından belirtilmektedir. Bu 3 aylık eğitim süresince ağ içerisinde yer alan bir saldırgan veya saldırganın geliştirdiği bir zararlı yazılım, pozitif örnek olarak işaretlenecek olan anomali hareketleri, ağ paketleri üzerinde yapacağı etiket değişikleri ile yaptığı işlemlerin zararsız olarak işaretleyebilir. Bu durumda, 3 ay sonunda kullanılacak olan zararlı ağ tespit modeli, hatalı veriyle eğitilmiş olacağı için hatalı sınıflandırma işlemi yapacaktır. Bu tip saldırılara etiket değişikliği saldırısı (label flipping attack) adı verilmektedir ve eğitim aşamasında geçmektedir.

Ek olarak saldırgan, girdi örneklerinde manipülasyonlar yaparak modeli atlatabilir. Buna verilebilecek örneklerden bir tanesi, ikili sınıflandırma yöntemlerinden olan lojistik regresyon yönteminin atlatılmasıdır. Lojistik regresyon çok kısa olarak anlatılacak

$$p(y=1) = \frac{1}{1+e^{-(w^T x+b)}}$$

Lojistik regresyon denklemi

x	2	-1	3	-2	2	2	1	-4	5	1	Girdi (Input)
w	-1	-1	1	-1	1	-1	1	1	-1	1	Ağırlık (Weights)
$w^T x$	-2	1	3	2	2	-2	1	-4	-5	1	Sonuç (Result): -3

Tablo 1: Manipüle edilmemiş girdi örneğinin lojistik regresyon model sonucu

x	2	-1	3	-2	2	2	1	-4	5	1	Girdi (Input)
w	-1	-1	1	-1	1	-1	1	1	-1	1	Ağırlık (Weights)
$\hat{x}$	1.5	1.5	3.5	-2.5	2.5	1.5	1.5	-3.5	4.5	1.5	Saldırgan (Attacker)
$w^T \hat{x}$	-1.5	-1.5	3.5	2.5	2.5	-1.5	1.5	-3.5	-4.5	1.5	Sonuç (Result): 2

Tablo 2: Saldırgan tarafından manipüle edilmemiş girdi örneğinin lojistik regresyon model sonucu

olursa, doğrusal bir denklem kullanarak sonucun 0.5'ten büyük olması durumunda örneği pozitif, 0.5'ten az olması durumunda negatif olarak işaretlemektedir (saldırı örneği olarak ifade edilirse; pozitif sonuç saldırı var, negatif sonuç ise normal davranış şeklindedir).

Örnek olarak, sahip olduğumuz ağ saldırısını tespit edebilen lojistik regresyon sınıflandırma modelinin ağırlıkları (w) ve sınıflandırma yapılacak olan girdi örneği (ağ paketi x) Tablo 1'de gösterilmektedir. Son satırda ağırlık sonucu -3 çıkmaktadır. Lojistik regresyon denkleminde yerine koyulmasıyla elde edilen sonuç 0.0474, yani %4,74 olasılıkla pozitif veya başka bir deyişle yaklaşık %95 olasılıkla negatif etikete sahiptir. Girdi örneğimiz üzerinde bazı değişiklikler yaptığımız durum Tablo 2'de gösterilmektedir.

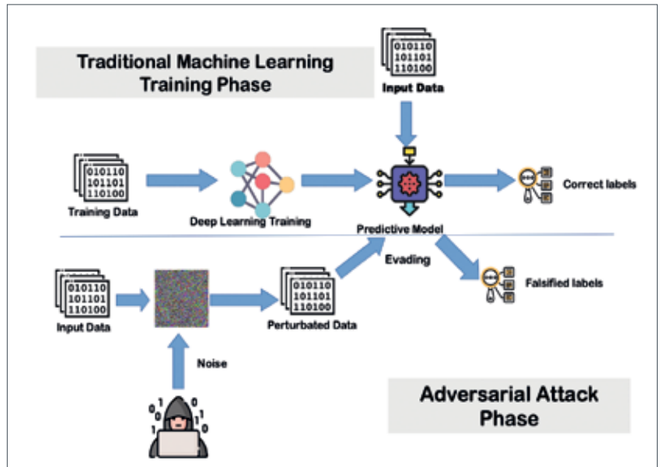
Bazı değişikliklerle elde edilen sonuç 2 olmaktadır. Denklemde yerine koyduğumuzda elde edilen sonuç 0.88, yani %88 olasılıkla pozitif, %12 olasılıkla negatif çıkmaktadır. Bu şekilde saldırgan, gerçek durumda yaklaşık %5 olan olasılığı %88 oranına artırmayı başarmıştır.

Saldırgan Makine Öğrenmesi Yöntemleri

Siber güvenlikte yer alan CIA gizlilik, bütünlük, erişilebilirlik (Confidentiality, Integrity, Avaliability) bakış acısıyla saldırgan makine öğrenmesi Tablo 3'te gösterilmiştir.

Saldırganın Yeteneği	Saldırganın Hedefi		
	Gizlilik (Confidentiality)	**Bütünlük (Integrity)**	**Erişilebilirlik (Availability)**
Test Verisi	Model atlatma saldırısı		Model hırsızlığı, model çıkarımı
Eğitim Verisi	Zehirleme; arka kapı (backdoor) veya sinir ağı trojani (neural network trojan)	Zehirleme; sınıflandırma hatasının maksimize edilmesi	

Tablo 3. Saldırgan makine öğrenme yöntemlerinin sınıflandırılması



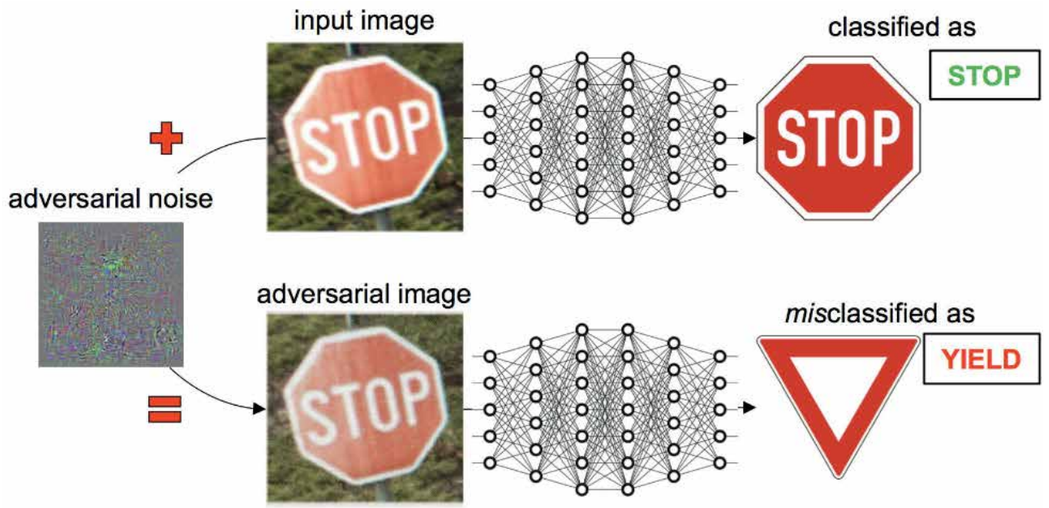
Şekil 1. Örnek bir makine öğrenme modeli saldırısı

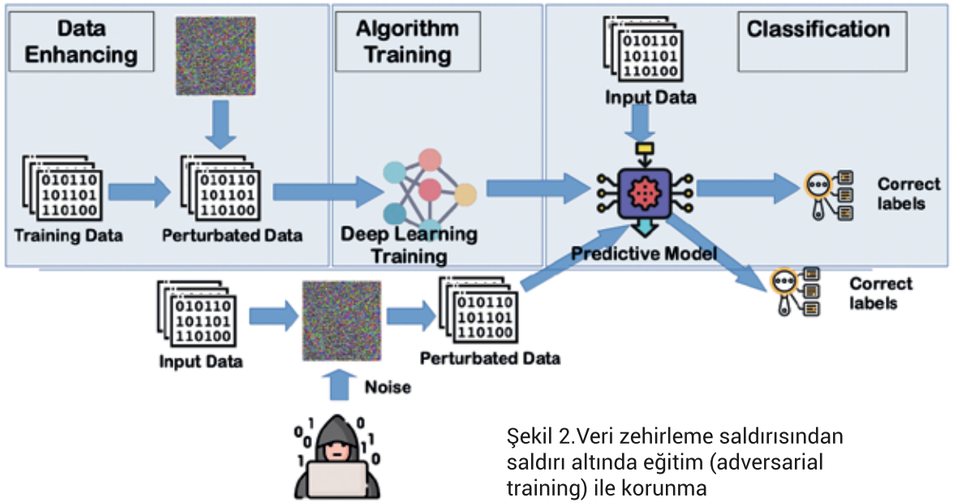
Saldırgan girdi örnekleri, bir makine öğrenme modelinin doğru şekilde sınıflandırdığı temiz bir görüntünün, makine öğrenme modeli tarafından yanlış sınıflandırılmasına neden olacak küçük bir bozulma eklenerek olusturulan yeni görüntülerdir. Bu saldırılar hedefli ve hedefsiz olmak üzere ikiye ayrılmaktadır. Hedefsiz bir saldırı ile modelin sınıflandırma performansını düşürmek amaçlanırken, bir hedefli saldırıyla modelin sadece belirli sınıfa ait sonuç üretmesi istenmektedir. Bu saldırıya örnek olarak, otonom bir araç üzerinde trafik işaretlerini algılayan ve buna göre davranacak modeli verebiliriz. Eğer modele yapılacak olan saldırı ile DUR (STOP) işaretini YOL VER (YIELD) olarak sınıflandırması sağlanır ise ölümcül bir kazaya neden olunabilir. Örnek bir saldırı akışı Şekil 1'de gösterilmiştir.

Saldırı Araçları

Bu tip örneklerin oluşturulması ve modellere saldırı gerçekleştirilebilmesi amacıyla açık kaynak kodlu çeşitli kütüphaneler bulunmaktadır. Makine öğrenme modellerine saldırılar, bu araçlar kullanılarak oldukça kolay bir şekilde gerçekleştirilebilmektedir. Cleverhans[1] ve IBM Adversarial Robustness Toobox[2] bu alanda en çok kullanılan araçlardır. Bu araçların her ikisi de Tensorflow, Keras, PyTorch, Scikit-Learn gibi makine öğrenmesi alanında çok kullanılan algoritma kütüphanelerinin tamamına saldırı gerçekleştirebilmektedir. Github adreslerinde yer alan yeterli örnekleriyle saldırıların nasıl gerçekleştirilebileceği anlatılmaktadır. Saldırgan makine öğrenmesi (adversarial machine learning) alanında en çok kullanılan ve bu araçlarda da gerçekleştirimleri bulunan saldırı algoritmaları şunlardır:

- Fast-Gradient Sign Method Attack
- Targeted-Fast Gradient Sign Method Attack
- Basic Iterative MethodAttack
- DeepFool Attack
- Jacobian-based Saliency Map Attack





Şekil 2.Veri zehirleme saldırısından saldırı altında eğitim (adversarial training) ile korunma

Korunma Yöntemleri

Model eğitilirken veya sınıflandırma aşamasında yaşanacak olan bu tip saldırılar için yapılabilecek ilk çözüm, saldırı altında eğitimdir (adversarial training). Özellikle görüntü sınıflandırma alanında oldukça sık kullanılan veri zenginleştirme (data augmentation) yöntemine benzer bir yaklaşımdır. Bu yaklaşımla bilinen bütün saldırı yöntemleri ile saldırgan örnekler oluşturularak, eğitim aşamasında kullanılacak olan veri kümesine bu saldırgan örnekler doğru etiketleri ile beraber eklenerek modelin oluşturulması hedeflenmektedir. Bu şekilde ileride modele yapılacak olan saldırılara karşı daha dayanıklı hale gelecektir. Şekil 2'de bu tip saldırıdan korunmak için gerekli olan adımlar gösterilmektedir.

İkinci olarak kullanılacak savunma yöntemi rassal girdi dönüşümüdür (random input transformation). Bu savunma yöntemi kullanılarak, girdi resimlerinin boyutlarının rassal olarak küçültülmesi, sıfır doldurma (zero padding) ile genişletmek gibi yöntemler uygulanmaktadır.

Kullanılabilecek başka bir yöntem ise kriptografik yöntemlerdir. Bu yöntemler, özellikle birden fazla veri kaynağının olduğu öğrenme aşamasında sistemin manipülasyonunun önüne geçilmesi açısından önem taşımaktadır. Homomorfik şifreleme, şifreli veriler üzerindeki aritmetik işlemlerin yapılabilmesine olanak sağlamaktadır. Bu şekilde, veri sahiplerinin verilerini şifrelemesini ve şifrelenmiş girdileri bir model sahibine ve muhtemelen diğer veri sahiplerine göndermesini sağlamaktadır. Model daha sonra şifrelenmiş girdi örneklerine uygulanmakta ve etiketleme sonucu, şifresini çözebilen ve istenen bilgileri elde edebilen uygun taraflara

> Makine öğrenme algoritmalarının hemen hemen tamamı, çeşitli güvenlik zafiyetleri içermektedir.

iletilmektedir. Microsoft SEAL veya HeLib gibi açık kaynak araçlar ve kütüphaneler kullanarak bu tip homomorfik şifreleme ürünleri geliştirilmesi oldukça kolaylaşmaktadır.

Sonuç

Yapay zekânın günlük hayatımızda kullanımı, önümüzdeki yıllarda da artarak devam edecek edecektir. Makine öğrenme modellerine dayalı geliştirilen uygulamaların çok fazla güvenlik zafiyetine sahip olduğu, saldırganlar tarafından bilinmektedir. Saldırgan makine öğrenmesi koruma konusunda bazı ilerlemeler sağlanmış olsa bile halen istenilen seviyelere ulaşılamamıştır. Özellikle savunma sanayi alanında faaliyet gösteren kuruluşlar tarafından geliştirilen ürünlerin içerisinde yer alacak bu tip algoritmaların ve eğitim verilerinin bu şekilde orijinal halleriyle kullanılması ileride büyük zararlar ortaya çıkarabilecektir. Güvenli yazılım geliştirme faaliyetlerinin tanımlanması gibi, güvenli model oluşturma adımlarının da tanımlanarak ürün geliştirmelerin yapılması bir zorunluluktur.

KAYNAKÇA

1. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331.
2. Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial Attacks and Defenses in Deep Learning. Engineering, 6 (3), 346-360. Defenses in Deep Learning. Engineering, 6 (3), 346-360.

Dipnotlar

1. https://github.com/tensorflow/cleverhans
2. https://github.com/IBM/adversarial-robustness-toolbox

TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

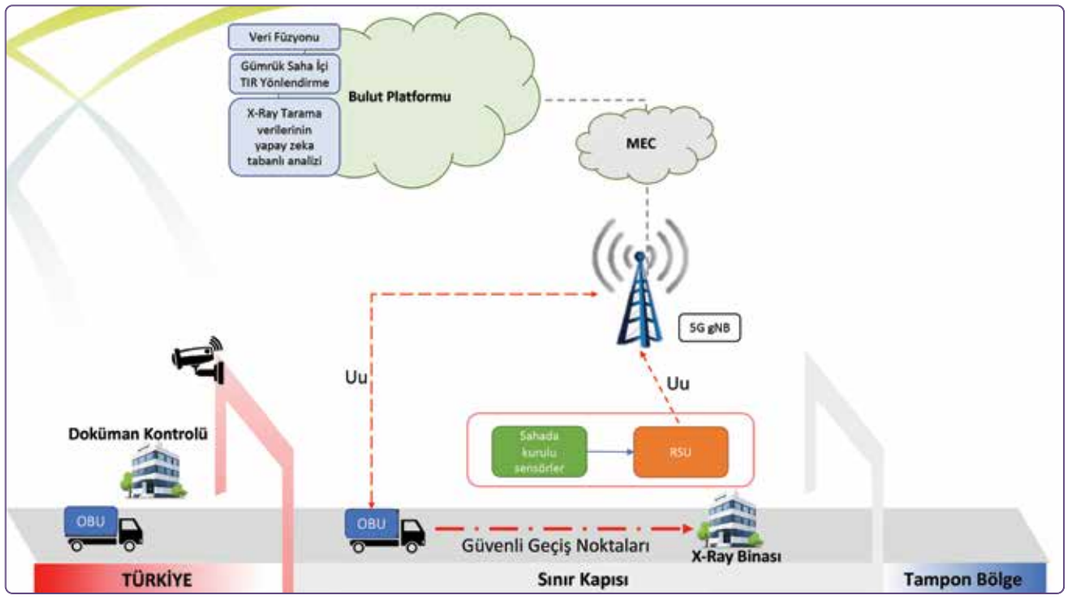
5G-MOBIX Projesi

Bir AB Ufuk 2020 projesi olan 5G-MOBIX (5G for Cooperative & Connected Automated Mobility on X-border corridors), 5G teknolojisinin sağladığı düşük gecikme, yüksek band genişliği gibi temel yeniliklerden ve ileri yapay zekâ tekniklerinden faydalanarak, otomatikleştirilmiş araç fonksiyonları geliştirmeyi hedeflemektedir.

Proje, 10 ülkeden 59 ortakla sürdürülmektedir. Altı farklı ülkede deneme sahaları oluşturularak, geliştirilen teknolojilerin ön gösterimleri gerçekleştirilecektir. İspanya-Portekiz ve Türkiye-Yunanistan sınırları olmak üzere iki farklı sınır geçiş koridorunda ise tüm proje kapsamında geliştirilen teknolojilerin, çeşitli kullanım senaryoları ile gösterimi yapılacaktır.

BİLGEM, Türkiye-Yunanistan sınır geçiş koridorunda gerçekleştirilecek gösterim kapsamında projeye dâhil olmuştur. Kurumumuz dışında yerli ortaklar olarak Ford Otosan, Turkcell, ve Ericcsson TR, Yunanistan tarafında ise Cosmote, WINGS ve Ericcsson GR gibi kuruluşlar yer almaktadır.

Projenin 31 Ekim 2021 tarihinde tamamlanması planlanmaktadır.



"TIR Yönlendirme" Kullanım Senaryosu

Küresel Salgının Bilişim Güvenliğine Etkileri

> Yeni normal dönem olarak adlandırılan küresel salgın sonrası dönem, hiçbir şeyin artık eskisi gibi olmayacağı ve sağlıktan ekonomiye, teknolojiden sosyolojiye her alanı derinden etkileyen, oyunun kurallarının yeniden yazıldığı bir dönem olacaktır.

Ensar Şeker – Uzman Araştırmacı, Muttalip Tulgar – Başuzman Araştırmacı,
Erkut Beydağlı – BS Birim Müdürü / BİLGEM İGBY, Dr. Orhan Muratoğlu – Direktör / ASELSAN

Yeni normal dönem' olarak adlandırılan küresel salgın sonrası dönem, hiçbir şeyin artık eskisi gibi olmayacağı ve sağlıktan ekonomiye, teknolojiden sosyolojiye her alanı derinden etkileyen, oyunun kurallarının yeniden yazıldığı bir dönem olacaktır. Ancak bu sarsıcı değişimin etkisinin ne boyutta ve ne yönde olacağı, tartışma konusu olmaya devam edecektir.

Başta sağlık sistemini derinden etkileyen Yeni Koronavirüs hastalığı (COVID-19) ile mücadele kapsamında, "Sorun Küresel, Mücadelemiz Ulusal"[1] söylemini etkin kriz yönetimi ve koordinasyon becerisiyle hayata geçiren ülkemiz, salgın sonrasındaki değişim sürecini milli seferberlik bilinciyle yürütmektedir. "Yeni bir dünya gerçeğiyle karşı karşıya olduğumuz, bu sebeple salgın sonrası dönem için hazırlık yapılması"[2] zorunluluğu ortaya çıkmış, bunun da bütüncül olarak tüm disiplinleri kapsayacak şekilde yapılması ile ancak başarıya ulaşılacağı anlaşılmıştır.

Yeni Çalışma Düzeni: Uzaktan İş Gücü

2019 yılının son aylarında ortaya çıkan ve salgın ilanına sebep olan COVID-19 ve beraberinde getirdiği felaketler, şirketler ve çalışanlar için günlük normların aniden değişmesine ve iş yaşamı ile birlikte tüm hayatın derinden etkilenmesine yol açtı. Birçok şirketin İş Sürekliliği Planları ya mevcut değildi ya da bu planlanan, tüm işgücü ve operasyonları ile birlikte uygulamaya hazır değildi.

Salgının yayılmasının önüne geçebilmek için tüm dünyada sıkı tedbirler birer birer uygulanmaya başlarken günlük operasyonların ve iş sürekliliğinin devamı ve çalışanların uzaktan çalışabilmesi için yeni yöntem ve metotlar uygulanmaya başladı. Bunlar arasında toplantı ve görüşmelerin çevrimiçi ortamlarda telekonferans çözümleri ile gerçekleştirilmesi, verilere kolay erişim sağlanabilmesi için bulut tabanlı altyapıların kullanılması, gizlilik dereceli verilerin korunabilmesi için VPN tabanlı teknolojilerin adapte edilmesi gibi örnekler sıralanabilir.

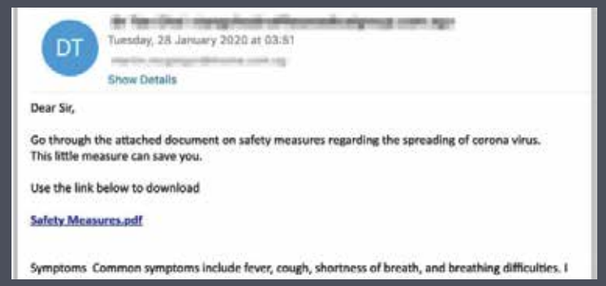
Bu yeni çalışma düzenine belki de en çabuk, siber saldırganlar adapte oldu ve bu süreçte kullanımı artan bu uygulamaların zafiyetlerini sömürmek için yeni stratejiler geliştirdiler. Bu makalede bu saldırı yöntemlerinden ve ulusal bilişim güvenliğine etkilerinden bahsedilmiştir.

Tüm bunların dışında çıkış noktası İnternet olan yeni dijital çağ[3] Coronavirus'ün katalizör etkisiyle bambaşka bir ivme kazandı. Bu noktada, Türkiye'nin pozisyonunu değerlendirmek, kişisel mahremiyet ve ulusal güvenlik eksenlerinde ortaya çıkan bilişim kavramlarını tartışmaya açmak ve geleceğe dönük teknolojilerin uygulanabilirliklerini sorgulamak anlamlı olacaktır.

Salgın ve Bilgi Güvenliği

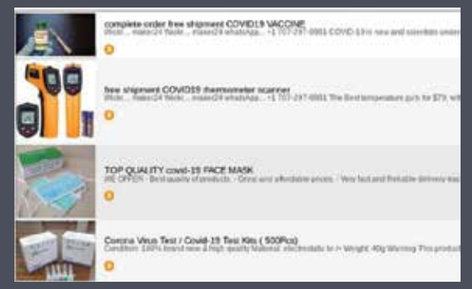
Bilgi güvenliği uzmanları, bir kişi, kurum ya da kuruluşun kişisel olarak tanımlanabilir bilgileri ile hassas bilgi ve verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini güvence altına almak için çalışır[4]. Bilgisayar korsanları, basit komut dosyala-

Şekil 1. COVID-19 Tedavisinde Kullanıldığı İddia Edilen hydroxy-chloroquine Maddesi ile İlgili Yapılmış Sahte Bir Web Sayfasının Ekran Görüntüsü [8]

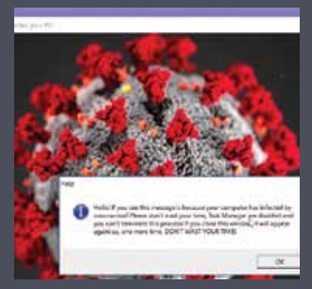


Şekil 2. COVID-19 ile İlgili Gönderilmiş Bir Oltalama Saldırısı Ekran Görüntüsü[9]

Şekil 3. Bir Hastaneye Yapılmış DDoS Saldırısı ile İlgili Ekran Görüntüsü[12]



Şekil 4. DarkWeb'de Satışı Yapılan COVID-19 Tanı Kitleri ve İlaçlar ile İlgili Ekran Görüntüsü[13]



Şekil 5. Bir Bilgisayara Bulaşmış COVID-19 Kötücül Yazılımı Ekran Görüntüsü[15]

rı çalıştıran alt seviyeden, gelişmiş kalıcı tehdit (APT) ve siber silahlar geliştiren üst seviye gruplara kadar beceri, finansman ve nihai hedef olarak çeşitlilik gösterir[5]. Açık kaynak araçlarını indirebilen ve temel komut dosyası saldırılarını kolayca gerçekleştirebilen, genelde kişisel tatmin ya da politik amaçlı saldırılar yapan saldırganlardan, ekonomik gelir elde etmek ve daha da ileri seviyede genellikle ulus-devlet destekli çok fazla finansman desteği olan, onlarca yıllık deneyimi ve ileri seviye ekipmanlara sahip imkânlarını uluslararası casusluk ve siber savaş için kullanan APT gruplarının ulaşmak istedikleri hedefler, birbirinden oldukça farklıdır.

Bununla birlikte kriz anları, genellikle siber saldırılarda ve güvenlik ihlallerinde bir artışa neden olur. Siber suçluların dolandırıcılık, kimlik hırsızlığı ve sosyal mühendislik yoluyla kredi kartı verileri de dahil olmak üzere birçok özel ve gizli bilgileri çalmak için krizden faydalandığı COVID-19 salgını döneminde de gözlenmiştir.

Bilgi güvenliği politikalarının sacayaklarını CIA olarak bilinen gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) oluşturmaktadır[6]. Risk yönetimi olası tehdit ve zafiyetlerin, bu üçleme üzerinde ne tür etkiler bırakabileceği değerlendirilerek yapılır. Geleneksel olarak gizlilik ve bütünlük için süper sofistike çözümler geliştirilip (kimlik doğrulama, şifreleme, imzalama, vb.) tedbirler alınırken, erişilebilirlik konusu sanki daha az önemliymiş gibi ikinci planda kalır. Ta ki istenmeyen bir hataya veya beklenmeyen bir felakete kadar.

Gerek kurumlar açısından çalışanlarına gerek çalışanlar açısından kurumsal kaynaklara erişim konusunda kaçınılmaz bir algı ve kurgu değişikliğinin, bilişim güvenliği gerekleri karşılanarak gerçekleşmesi beklenmektedir.

> **Türkiye'nin pozisyonunu değerlendirip kişisel mahremiyet ve ulusal güvenlik eksenlerinde ortaya çıkan bilişim kavramlarını tartışmak ve geleceğe dönük teknolojilerin uygulanabilirliklerini sorgulamak anlamlı olacaktır.**

Çalışanların performans göstergeleri, işyerine giriş/çıkış saatleri olmaktan çıkıp, kendilerine atanan görevleri hangi kalite ve zamanlama ile yerine getirdikleri olacaktır. Telefon, e-posta ve video konferans gibi kanallardan 7/24 erişilebilir olan çalışanların iş güçleri, kimi zaman çileye dönen ulaşım veya çay/kahve molalarıyla ziyan edilmeyecektir.

Özellikle sınıflandırılmış verilerin işlendiği veya gizlilik dereceli projelerin yürütüldüğü kuruluşlar, kurumsal kaynaklarını nasıl yönettiklerini gözden geçirmek ve uzak erişim ihtiyaçlarını gerekli güvenlik önlemleri ile karşılar şekilde yeniden yapılandırmak zorundalar. Bu bağlamda, KVKK (Kişisel Verileri Koruma Kanunu) ve MSB (Milli Savunma Bakanlığı) yönergelerinin de uzaktan çalışma modellerinde verimliliği artıracak şekilde, gizlilik ve bütünlük gereklerini karşılayacak güvenlik önlemleri ile güncellenmeleri gerekecektir.

COVID-19 Salgınında Siber Tehditler

Koronavirüsün yayılmasına, uzaktan çalışanlar, devlet kurumları ile ulusal ve uluslararası tıbbi tesislere karşı siber saldırılar da normalden fazla bir artışla eşlik etti. Tehditlerin sayısı ve etkisinin artmasıyla birlikte istihbarat, ulusal güvenlik ve kolluk kuvvetleri tarafından daha fazla uyarılar yapıldı ve bu kapsamda önlemler alınmaya başlandı.

ABD ve İngiltere'nin ilgili siber güvenlik birimleri tarafından yayınlanan ortak bir bildirgede, kriz ortamını fırsata çevirmek isteyen bilgisayar korsanlarının faaliyetlerine dikkat çekilmiştir. Bu faaliyetler arasında sahte video konferans ve uzaktan erişim uygulamaları aracılığıyla kötü amaçlı yazılımları dağıtmanın yanı sıra, dijital kimlik avı ve fidye yazılımı saldırılarının salgın sürecindeki artışına özellikle vurgu yapılmıştır. FBI ve Interpol, devlet destekli bilgisayar korsanları ve COVID-19 ile ilgili araştırmalara açıkça katıldıklarını belirten tıbbi kurumları hedef alan fidye yazılımı saldırıları ile siber casusluk operasyonlarına karşı uyarıcı tavsiyeler yayınlamışlardır. NASA tarafından çalışanlarına bu süreçteki saldırılarla ilgili bilgiler aktarılarak dâhili uyarılar yapıldığı bildirilmiştir. FBI ve Hindistan'ın ulusal siber olaylara müdahale ekibine göre kötü niyetli aktörler çevrimiçi okul derslerini kesintiye uğratmış ve bu kayıtlardaki kişisel verileri toplamışlardır. Uyarılara yanıt olarak, birçok devlet kurumu ve küresel şirket Google, SpaceX, ABD Senatosu, Tayvan hükümeti, Alman Dışişleri Bakanlığı ve Avustralya Savunma Bakanlığı dahil olmak üzere birçok güvenlik sınırlamalarını faaliyete geçirmiş ve bu kapsamda birçok uygulamanın kullanımını da yasaklamıştır.

Bu süreçte siber casusluk operasyonları da artış gösterdi. Çin, devlet kurumlarını COVID-19 ile ilgili bilgiler arayışında hedefleyen Vietnam kaynaklı bir siber casusluk kampanyası tespit ettiğini duyurdu. Google'ın Tehdit Analizi Grubu, sağlık kuruluşlarını hedef alan bir düzineden fazla devlet destekli bilgisayar korsanı grubu hakkında bulguları olduğunu bildirdi. Aynı zamanda, bazı devlet destekli bilgisayar korsanı grupları, sosyal medya üzerinden dezenformasyon kampanyaları başlattı.

Sahte Alan Adları ve Web Sayfaları

ABD Başkanı Donald Trump'ın 19 Mart 2020 tarihinde, bir brifingde COVID-19 tedavisinde kullanılabilecek bazı ilaç isimlerini telaffuz etmesinin[7] hemen akabinde, bu ilaç adlarını içeren sahte alan adları ve bu alan adları kullanılarak oluşturulmuş sahte web siteleri sayısında inanılmaz bir artış oldu[8]. Her ne kadar bu sahte web sayfaları Ulusal Siber Olaylara Müdahale Merkezleri (USOM) tarafından tespit edildikleri anda erişimleri engellense de, benzer başka alan adları da alan saldırganlar, faaliyetlerini sürdürmeye devam etmeye çalışmaktadır.

Oltalama Saldırıları

Dünya COVID-19 salgınına karşı büyük bir mücadele verirken ve henüz herhangi bir tedavi tam manada geliştirilememişken, bilgisayar korsanları insanlara hastalığa çözüm bulduklarını iddia ettikleri e-postaları göndererek zararlı yazılımları bulaştırmaya çalışmaktadır[9].

Uç-nokta Saldırıları

Uç-noktalar, bir organizasyonun verilerine, kimlik bilgilerine ve ortamına erişim noktalarıdır[10]. Salgın dolayısıyla uzaktan çalışmaya bağlı olarak uzaktan erişim için uç noktalar artmış, dolayısı ile siber suçlular için hedeflenen yüzey alanları da artmıştır. Uç nokta güvenliği oldukça kritik bir konudur, zira veri ihlallerinin ve kötücül yazılım bulaşmasının çoğu son kullanıcı cihazlarında gerçekleşmektedir.

Uzaktan Eğitim Sistemlerine Saldırılar

Salgın sürecinde birçok okul ve eğitim merkezi de uzaktan öğrenme sistemine geçip bu konu ile ilgili teknolojik altyapıları kullanmaya başladı. Bu sistemler de siber korsanların saldırılarına maruz kalmış ve eğitim seansları kayıtlarını içeren birçok data internette paylaşılmaya başlanmıştır[11]. Videoların çoğu, katılımcıların seslerini, yüzlerini ve iletişim numaralarını ve başka kişisel verileri içermektedir. Ayrıca eğitimle ilgili notların da çevrimiçi tutulmak

durumunda olduğu bu dönemde bazı siber korsanlar belli bir ücret mukabilinde sistemlere sızarak ders notlarını yükseltmeye başlamıştır.

Sağlık Bakanlıkları, Araştırma Laboratuvarları ve Hastanelere DDoS ve Ransomware Saldırıları

Tüm dünya genelinde güvenlik birimleri; sağlık bakanlıkları, araştırma laboratuvarları ve hastanelere gerçekleştirilen siber saldırıların önemli ölçüde arttığına dikkat çekerek, bilgisayar korsanlarının ulusal ve uluslararası sağlık politikası konusunda istihbarat elde etmeye veya COVID-19 ile ilgili araştırmalar hakkında hassas verileri ele geçirmeye çalıştıklarını bildirerek ilgili tıbbi kurum ve kuruluşları uyardı[12].

Bazı saldırganlar, sağlık çalışanlarının insan hayatını kurtarabilmek için saniyelerle yarıştığı böyle bir ortamda, finansal gelir elde edebilmek için ya bu tıbbi kurum ve kuruluşların web sayfalarına DDoS saldırısı yaparak erişimi engelledi ya da ransomware saldırıları ile hassas hasta/hastane verilerini şifreleyerek tekrar erişim için para talep etti.

Çek Cumhuriyeti'ndeki hastaneler, sistemlerine yapılan siber saldırıları önlediğini duyururken, İtalya'nın sosyal güvenlik sitesine erişim bir süreliğine engellendi. Dünya Sağlık Örgütü, ağlarına gerçekleştirilen siber saldırıların geçen yılın aynı dönemine kıyasla beş kat artış gösterdiğini bildirdi.

DarkWeb'de Sahte Kit, Sahte İlaç ve Plazma Satışları

Siber güvenlik araştırmacıları, DarkWeb'de sahte COVID-19 aşıları, tanı kitleri ve daha önce hastalığı atlatmış kişilerden alındığı öne sürülen plazmaların satışa sunulduğu birkaç sanal pazar yeri tespit etti[13]. Satıcıların listelerini yüz maskeleri, el dezenfektanı içerecek şekilde çeşitlendirdiği gözlendi.

Telekonferans Uygulamalarına Yapılan Saldırılar

Son zamanlarda, binlerce çevrimiçi toplantı kaydının hiçbir koruma olmadan internette erişime açık olduğu tespit edildi[14]. Bu kayıtlarda birçok hassas bilgi paylaşıldığı ve bu bilgilerin siber korsanlarca kullanıldığı da bilinmektedir. Kullanıcı bilgilerinin (kullanıcı adı ve şifre) ele geçirildiği saldırılar sonrası bu bilgiler, hem internet üzerinden satışa çıkarılmış hem de bilgileri çalınan kişinin başka hesaplarına da saldırılar düzenlenmiştir.

COVID-19 Kötücül Yazılımı

Siber güvenlik uzmanları yakın bir zamanda, bir sistemin ana önyükleme kaydını (MBR) geçersiz kılan ve önyüklenemez hale getiren bir korona virüs temalı kötü amaçlı yazılımı analiz etti[15]. Bu kötücül amaçlı yazılım çalıştırıldığında, makineyi otomatik olarak yeniden başlatır ve ardından kapatılamayan virüs temalı bir pencere görüntüler. Pencerenin sağ üst tarafındaki normal çıkış düğmesi ise çalışmamaktadır.

VPN Saldırıları

Mevcut VPN şifreleme protokolleri sağlam olabilir ve önemli koruma sağlar. Ancak, hiçbir şey saldırıya karşı %100 bağışık değildir. Geleneksel olarak, VPN'lerde kullanılan Internet Anahtar Değişimi (IKE) [16] saldırganların hedefleri arasındadır. Çoğu VPN servis sağlayıcısı, müşterileri için kullanıcı adları ve şifreler gibi önemli bilgileri içeren güvenlik riskleri oluşturabilecek kimlik doğrulama verilerini depolamayı önerir. Bu durum, bilgi güvenliği açısından oldukça kritik ve istenmeyen bir durumdur. Ayrıca, hata mesajları ve paket başlıkları, çalışmakta olan VPN'nin türü ve sürümü hakkında saldırganlara oldukça önemli bilgiler verebilmektedir.

Saldırılara Karşı Tedbirler

Devletler, salgın sürecindeki siber tehditleri azaltmak için daha proaktif bir yaklaşım benimsemeye başladı. Avustralya Sinyaller Müdürlüğü (ASD) Koronavirüs ile ilgili saldırıları ve kötü niyetli faaliyetleri engellemek için saldırgan siber yeteneklerini seferber ettiğini açıkladı. Amerikan Senatosu, ABD Siber Komutanlığı'na sağlık sektöründeki eylemleri değerlendirme, siber tehditleri tespit etme ve caydırmaya hususunda tam yetki verdi. ABD Adalet Bakanlığı yüzlerce kötü amaçlı COVID-19 web sitesini kaldırmak için teknoloji şirketleri ile işbirliğini artırdı.

Önde gelen teknoloji şirketleri tarafından bu konuda girişimler başlatıldı. Whatsapp ve Facebook, kendi platformlarında yanlış bilgilerin yayılmasını sınırlamak için adımlar attı. Facebook, 50'den fazla dilde yapılan paylaşımların bilgi kontrol ve içerik derecelendirmesi için dış denetçi, bağımsız bir kuruluşla işbirliğini duyurdu.

Kullanıcı Sorumlulukları

Herhangi bir siber güvenlik zincirinde en güçlü ve en zayıf halka insanlardır. Bir kurum ya da kuruluş, aktif ağ taraması ile en gelişmiş tehdit istihbarat programına sahip olsa da zararlı bir yazılımı önce kendi bilgisayarına daha sonra organizasyon ağına bulaştıracak bir bağlantıyı tıklatmak, yalnızca bir çalışan yeterlidir. Kuruluş ne kadar güvenli olursa olsun, ne kadar karmaşık çözüm ve politikalar uygulanmış olursa olsun personel, belirlenen yönetim süreçleri altında faaliyet göstermiyorsa, derinlemesine savunma güvenlik katmanları, kuruluşun korunmasında daha az etkili hale gelir.

Bu sebeple, BT departmanlarının aldığı güvenlik tedbirlerinin ötesinde bireysel kullanıcılara da oldukça önemli sorumluluklar düşmekte ve bu kullanıcılar, gerek kendi kişisel verilerini gerekse parçası oldukları organizasyona ait hassas verileri korumakla yükümlüdürler.

Organizasyon Sorumlulukları

İster büyük ister küçük bir organizasyonda güçlü politikalar belirlemek, mevcut kontrolleri geliştirmek ve son kullanıcılara eğitim sağlamak, durumsal farkındalığı artırmaya yardımcı olacak en iyi uygulamalardır. Hassas işler yapan kuruluşlar, faaliyetlerinin doğası gereği her zaman hedef olacaklardır. Örneğin, çevrimiçi bankacılık, bir şirketin finansal suçlar için tanımlanması ve hedeflenmesi riskini artırır. Büyük holding / Fortune 500 şirketleri için tehdit yüzeyi geniştir. Bahsi geçen organizasyonlar bu çok çeşitli siber olayları tanımlayabilmeli ve bu saldırılara hazırlıklı olarak yanıt verebilmelidir.

Siber Operasyon ve Siber Olaylara Müdahale Merkezleri

Cephede savaş veren SOM analistleri, güvenlik tehditlerini analiz etmek ve bunlara müdahale etmekten sorumludur. Uzaktan erişim ve uzaktan bağlantı gerektiren bu yeni dönemde SOM analistlerinin günlük karşılaştığı rutin network trafiği ve bu trafiğe yönelen tehditler de değişti. Böylesi kaotik zamanlarda, saldırganlar inanılmaz derecede kısa sürede çeşitli teknikler, taktikler ve prosedürlerle seferber olabilmektedir. SOM analistleri, açık kaynak siber tehdit istihbaratı (OSINT) ile saldırılar gerçekleşmeden önce, olası siber saldırı analizleri yaparak bu doğrultuda adımlar atmaktadır.

Ulusal çapta ise Siber Olaylara Müdahale Merkezleri Ulusal Bilişim Güvenliğine tehdit gördükleri hususlarla ilgili önemli çalışmalar yapmakta, gerçekleştirilen ya da gerçekleştirilecek siber saldırıların engellenmesi ya da en az zararla önüne geçilmesi adına faaliyetlerini sürdürmektedir.

KAYNAKÇA

[1] T.C. Sağlık Bakanlığı, n.d. "Sorun Küresel, Mücadelemiz Ulusal." May 26, 2020 (/TR,64342/sorun-kuresel-mucadelemiz-ulusal.html).
[2] Anadolu Ajansı. "Cumhurbaşkanı Erdoğan'dan Türk Konseyi'ne Salgın Sonrası İçin Hazırlık Mesajı." Retrieved May 26, 2020 (https://www.aa.com.tr/tr/turkiye/cumhurbaskani-erdogandan-turk-konseyine-salgın-sonrasi-icin-hazirlik-mesaji/1800568).
[3] Schmidt, Eric, and Jared Cohen. 2014. The New Digital Age: Transforming Nations, Businesses, and Our Lives. Reprint edition. New York: Vintage.
[4] Tipton, H. F., and M. Krause. 2003. Information Security Management Handbook. 5th ed. CRC Press.
[5] Campbell, T. 2016. "Chapter 1: Evolution of a Profession." PP. 1–14 in Practical Information Security Management: A Complete Guide to Planning and Implementation. APress.
[6] Samonas, S., and D. Coss. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." Journal of Information System Security 10(3):21–45.
[7] Reuters. 2020. "Special Report: Doctors Embrace Drug Touted by Trump for COVID-19, without Hard Evidence It Works."
[8] SentinelLabs. "Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Salgınc." Retrieved May 14, 2020 (https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-salgınc/).
[9] Google. "Protecting against Cyber Threats during COVID-19 and Beyond." Google Cloud Blog. Retrieved May 14, 2020 (https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond/).
[10] McAfee. "COVID-19 - Malware Makes Hay During a Salgınc." McAfee Blogs. Retrieved May 14, 2020 (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-salgınc/).
[11] Cosn. "COVID-19 & Cybersecurity - Member Exclusive. Pdf." Retrieved May 14, 2020 (https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf).
[12] Healthcare IT News. "Cyber-Attacks on Healthcare Facilities 'growing Threat' during Coronavirus Salgınc." Retrieved May 14, 2020 (https://www.healthcareitnews.com/news/europe/cyber-attacks-healthcare-facilities-growing-threat-during-coronavirus-salgınc).
[13] Majumdar, Romita. 2020. "Coronavirus: Fake COVID-19 Drugs, Vaccines Thrive on Dark Web." Livemint. Retrieved May 14, 2020 (https://www.livemint.com/news/india/dark-web-criminals-peddle-fake-covid-19-vaccines-as-a-front-for-malware-attacks-11587390740238.html).
[14] Norton. "Video Conferencing Risks When Working at Home: 16 Ways to Avoid Them." Retrieved May 14, 2020 (https://us.norton.com/internetsecurity-emerging-threats-zoom-bombing-video-conference-threats.html).
[15] Trend Micro. "Developing Story: COVID-19 Used in Malicious Campaigns - Новости о Безопасности - Trend Micro TR." Retrieved May 14, 2020 (https://www.trendmicro.com/vinfo/tr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains).
[16] Threat Post. "Government VPN Servers Targeted in Zero-Day Attack." Retrieved May 14, 2020 (https://threatpost.com/government-vpn-servers-zero-day-attack/154472/).

'YENİ NORMAL DÖNEM'DE ULUSAL BİLİŞİM GÜVENLİĞİ

Fatih Düzgün - Başuzman Araştırmacı, Aziz Gökhan Narin - Uzman Araştırmacı, Aykut Şensoy - Başuzman Araştırmacı, Cem Koral - Başuzman Araştırmacı /BİLGEM İGBY

> Ulusal bilgi güvenliği, ulusal kalkınma hedefleri ile doğrudan ilintili olup ekonomik ve sosyal fayda üreten bilgi sistemleri ile kritik altyapıları korumak adına ayrı bir önem arz etmektedir.

Küresel salgınla mücadelede ön plana çıkan sosyal mesafe kavramı ile çalışma şartları yeni bir boyut kazanmış, mekân bağımlılığı ortadan kalkarak uzaktan veya evden çalışma modeli öne çıkmıştır. Salgın adeta hızlı bir şekilde dijital dönüşümü de zorunlu hale getirmiştir. Bu dijital dönüşüm de, siber uzayın taşıdığı tehdit ve riskleri de beraberin getirmektedir.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında siber güvenlik şu şekilde tanımlanmıştır: siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu olaylara karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder[1].

Yine aynı belgede ulusal siber güvenlik kavramı; "ulusal siber uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenliğini ifade eder" olarak açıklanmaktadır. Bu iki tanımdan yola çıkıldığında siber güvenliğin ulusal güvenliğimizin bir parçası olduğunu söylemek yanlış olmayacaktır.

Risk ve Tekditler

Ulusal bilişim güvenliği, siber güvenlik stratejilerimizi de yeniden gözden geçirmeyi gerektiriyor. "Yeni normal dönem" de bizleri bekleyen risk ve tehditleri şöyle sıralayabiliriz:

- Küresel salgın sonrası IoT temelli akıllı şehirler, dijital vatandaşlık servisleri, yapay zekâ ve büyük veriye dayalı hizmetlerin artması ve bu hizmetlerin güvenliğine yönelik yaklaşımların önem kazanması.
- Uzaktan çalışma modelinin, siber tehdit yüzeylerini artırarak kurumların yoğun bir şekilde siber saldırılara maruz kalmasına neden olması.
- Hâlihazırda güvenlik nedeniyle İnternete açık olmayan kapalı ağların, uzaktan çalışma gerekliliği kapsamında yeterli risk değerlendirmesi yapılmadan İnternet'e kontrolsüz olarak açılarak veri sızıntısına neden olması.
- Dışa bağımlı bilişim teknolojileri yatırımlarında tedarik zincirlerinden kaynaklanan sorunlar yüzünden, siber saldırılara karşı kritik altyapıların dayanıklılığının ve sürekliliğinin sağlanmasının zorlaşması.
- Koronavirüs verilerini toplamak gibi biyomedikal güvenlik ve "medikal istihbarat" [2] kaynaklı bilgi toplama çalışmalarının, endüstriyel casusluk kapsamında hükümetler tarafından daha yoğun olarak yapılması.
- Vatandaşların e-devlet uygulamalarındaki kullanım sebebiyle, kişisel bilgisayarların güvenliğinin de önem kazanması.
- Yerli ve milli bulut altyapılarının azlığı ile ulusal bilgi güvenliği farkındalığının eksikliğinden kaynaklı nüfus, sağlık ve iletişim bilgileri gibi kritik verilerin kontrolsüz olarak yurt dışı kaynaklı bulut servislerinde işlenme ihtimalinin artması.
- Covid-19 ile mücadele sürecinde de görüldüğü gibi, önemli sosyo-ekonomik olaylar sırasında, sosyal medya ve internet aracılığı ile kasıtlı olarak oluşturulan yanlış haber ve bilgi kirliliğinin kamu düzenini olumsuz olarak etkilemesi.
- Siber olaylara karşı, kurumlar arası koordinasyon eksikliğinden kaynaklı olarak, hızlı ve etkin müdahalenin yapılamaması.
- Her türlü kurum ve kuruluşta oltama postaları, zararlı yazılım ve benzeri saldırılar sonucunda, dolandırıcılıkla yoğun bir şekilde karşı karşıya kalınması.
- Hastalığın gidişatı ile ilgili daha fazla veri toplamak için kullanılan mobil uygulamaların, kişisel verileri ifşa ettiği ve gizlilik kaygılarının ön plana çıkmasına neden olması [3].
- BT altyapı ve hizmetlerinde kritik rolde olan personelin, küresel salgın nedeniyle seyahat edememesi veya hasta olması gibi durumlarda alternatif önlemlerin belli olmaması.
- Uzaktan çalışma modelinde mobil cihazların ve iletişim kanallarının şifreli olmaması veya şifrelemenin milli kripto çözümleri ile sağlanmaması.
- Video/telekonferans iletişiminin küresel BT firmaların bulut çözümleri ile yapılmasının ulusal bilgi

> **Herhangi bir siber güvenlik zincirinde en güçlü ve en zayıf halka insandır.**

güvenliği zafiyetine yol açması.

- Salgın nedeniyle devletlerarası kamu diplomasisinin, dijital diplomasi [4] ile birlikte yürütülmesiyle, istihbarat örgütlerinin ülkeler arası iletişim ağına sızma isteğinin artması.
- Uzaktan çalışma esaslarına yönelik yasal mevzuat boşluğunun, bilgi güvenliği süreçlerini etkin ve doğru olarak yönetmeyi zorlaştırması.
- Ofisten ve uzaktan çalışma modellerinin kullanıldığı dağıtık BT mimari yapısına sahip kurumlarda, siber güvenliğe yönelik izlenebilirlik ve olay müdahale süreçlerinin zorlaşması.
- Siber risk yüzeyinin artması ile IoT, yapay zekâ, kritik altyapılar, bulut teknolojileri, büyük veri gibi alanlarda siber taarruz yöntemlerinin tam olarak bilinmemesi ve ilgili güvenlik yaklaşımlarına hâkim, nitelikli personel eksikliğinin ortaya çıkması.
- Uzaktan çalışma nedeniyle, BT hizmetlerinde artan kapasite ihtiyaçlarına hızlı cevap vermek adına, plansız ve kontrolsüz olarak sağlanan servisler ile güvenlik gereksinimlerinden taviz verilmeye başlanması.

Ulusal Bilgi Güvenliği Yol Haritası

Ulusal bilgi güvenliği, ulusal kalkınma hedefleri ile doğrudan ilintili olup ekonomik ve sosyal fayda üreten bilgi sistemleri ile kritik altyapıları korumak adına ayrı bir önem arz etmektedir. Bu noktada ulusal bilgi güvenliği stratejileri belirlenirken hem kamu hem de özel sektörün eşgüdüm içerisinde çalışacakları kurumsal bir yapı hazırlanmalıdır. Küresel salgın sonrası, ulusal bilgi güvenliğine dair yol haritasında şu noktalar daha çok önem kazanacaktır:

- Hızlı değişen dijital dönüşüm talepleri nedeniyle, Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının 3 yılda bir yerine, yıllık olarak güncellenmesi gerekmektedir.
- Uç nokta güvenliği, ağ güvenliği ve iletişim güvenliği için kamu ve özel kurumlar, Millî Açık Anahtar Altyapısı (MA3) [5] gibi tamamıyla yerli ve milli kriptografik çözümler kullanmalıdır.
- Kurumlara ait gizlilik dereceli haberleşmenin yerli ve milli kripto sistemleri ile geliştirilen güvenli ağ cihazları (AGC)[6] üzerinden gerçekleştirilmesi sağlanmalıdır.
- Güvenli kamu internet ağı (KAMUNET) yaygınlaştırılmalıdır.
- Yurt içinde oluşturulan nüfus, sağlık, iletişim gibi kritik verilerin, BİLGEM tarafından geliştirilen Safir Depo [7] gibi yerli ve milli bulut alt yapılarında güvenli olarak saklanması ve bu tür çözümlerin yaygınlaştırılması sağlanmalıdır. [8]
- Siber güvenlik çözümlerinde makine öğrenmesi ve derin öğrenmeye dayalı tehdit algılama, saldırı önleme ve davranışsal analiz yaklaşımları kullanılarak otomatik yanıt veren SOAR sistemler kullanılmalıdır. Bu kapsamda siber tehdit analizinde kullanılmak üzere ulusal veri setleri hazırlanmalıdır.
- Tüm kamu kurum/kuruluşları, özel sektör ve akademi temsilcilerinin katkılarıyla temelleri atılan Türkiye Siber Güvenlik Kümelenmesi'nde [9] yer alan yerli/milli çözümlerin, markalaşıp global pazarda rekabetçi ve söz sahibi olması için başta kamu kurumlarında kullanılmasını sağlayacak yasal düzenlemelerin yapılması gerekmektedir.
- Bilgi güvenliğine yönelik ulusal risklerin belirlenip merkezi olarak risk yönetiminin tek bir otorite tarafından yürütülmesi sağlanmalıdır.
- Siber güvenlik kurumları arasında var olan koordinasyon zaaflarının giderilmesi için yaptırım gücüne sahip, yetkilerin tek bir elde tutulduğu kurumsal bir yapının oluşturulması gerekmektedir.
- Ulusal bilgi güvenliği alanlarında Ar-Ge faaliyetlerinin desteklenmesi için üniversitelerle iş birliği yapılarak bilgi güvenliği alanında yüksek lisans ve doktora programlarının sayısının nitelik ve nicelik olarak artırılması sağlanmalıdır.
- "Hattı müdafaa yoktur, sathı müdafaa vardır, o satıh da bütün vatandır" [10] ilkesi esas alınarak siber güvenliğin tüm vatandaşları ilgilendiren bir konu olduğu bilinciyle, eğitim ve farkındalık faaliyetlerinin ülke çapında yaygınlaştırılması sağlanmalıdır.
- Ülkenin siber saldırı kapasitesinin geliştirilmesine yönelik yerli ve milli çözümler kullanılmalıdır.
- Başta enerji, finans ve iletişim sektörleri olmak üzere Türkiye'nin kritik altyapılarına yatırım yapan şirketlerin yabancı ortaklı özel girişimler olduğu düşünüldüğünde, bu girişimlerin uyması gereken

zorunlu siber güvenlik tedbirleri sıkıca denetlenmelidir.

- Sosyal medya ve haberleşme uygulamalarının yurt dışı kaynaklı olması, bu ortamların hükümetlerini, amaçları doğrultusunda toplumsal hareketliliği yönetme konusunda güçlü kılmaktadır. Sosyal medyaya ait yerli uygulamaların kullanımı ve çeşitliliği artırılmalıdır.
- Gelişen teknoloji ile eş zamanlı olarak siber güvenlik ihtiyaçlarını karşılayacak hukuki düzenlemelerin hızlıca hayata geçirilmesi gerekmektedir. Yasal düzenlemelerin, bilişim alanındaki uluslararası hukuki düzenlemeler ile uyum içinde olması sağlanmalıdır.
- Kurumsal bilgi güvenliği yönetişim süreçleri, kamu kurumlarında zorunlu hale getirilmelidir.
- Global pazarda rekabet edebilmek için yerli ve milli siber güvenlik ürünlerinin test ve sertifikasyonuna yönelik uzman personel ve laboratuvar sayılarının artırılması gerekmektedir.
- Siber güvenlik alanında başta kamu kurum ve kuruluşları ile özel sektör girişimleri ve tüm bireylerin ihtiyaçlarını pratikte karşılayacak güvenlik yapılandırma kılavuzlarının, sistemlere yönelik sıkılaştırma rehberlerinin, en iyi uygulama tecrübelerinin belirtildiği dokümanların ele alındığı portal yapılarının hazırlanarak güncelliğinin sağlanması ve bunların herkese açık internet ortamında yayınlanması gerekmektedir.

> **Bilgi sistemleri alanında CIA (confidentiality-gizlilik, integrity-bütünlük ve availability-erişilebilirlik) ve mahremiyet için kullanılan yazılım ve donanımın bütünüyle yerli/milli çözümler ile geliştirilmesi artık kaçınılmazdır.**

- Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) [11], siber istihbarat ve bilgi paylaşımı konusunda çeşitli ülkelerle ikili iş birliği anlaşmaları yaparak ortak siber güvenlik tatbikat sayılarını artırması gerekmektedir.

Avrupa Birliği ve Dünya Sağlık Örgütü gibi uluslarüstü örgütlerin küresel salgındaki yetersiz ve güçsüz kalmaları, kendi mücadelesini tek başına veren güçlü devlet kavramını ön plana çıkarmıştır[12]. Görünen o ki salgın, ülkelerin kendi stratejik sektörlerini özel korumaya alacağı, yerli ve milli kavramının güçleneceği, uluslararası iş birliği beklentisinin zayıflayacağı yeni bir dünya düzenini tetiklemiştir. Bu bağlamda, bilişim güvenliği de kritik altyapıların dayanıklılığının ve sürekliliğinin sağlanması açısından ulusal güvenliğin önemli bir boyutu olarak ele alınmalı, 'yeni normal dö-

nem' içerisinde ulusal siber güvenlik ekosistemini yaygınlaştırarak yerli ve milli çözümleri üreten ve etkin kullanan bir anlayış egemen kılınmalıdır.

COVID-19 Sonrası Dönem

Ulusal ve uluslararası arenada, pek çok yeni normalin şekilleneceği ve daha önce ihtiyatla yaklaşılan yöntemlerin gerekirse mutasyona uğrayarak hızla yaygınlaşacağı, "post-Korona" olarak da nitelendirilebilecek bir döneme girilmiştir.

COVID-19 sonrası bu dönemde Türkiye her zamankinden daha önemli bir aktör olmaya adaydır. Yetişmiş insan gücü, binlerce yılda olgunlaşan kültürel zenginliği ve jeopolitik avantajları harmanlandığında ciddi bir potansiyel ortaya çıkmaktadır.

Salgın ile birlikte internet ulaştırma alanındaki seçeneklere yeni alternatifler sunmakla birlikte, post-Korona döneminde bilişim alanında mecburi olabilecek böylesine hızlı bir dönüşümün, ulusal bilişim güvenliği alanında oluşturabileceği riskin minimize edilebilmesi için çözüm üretilmesi birincil gündem maddesidir.

Salgın sebebi ile değişen dijital alışkanlıklar göz önüne alındığında, dijital alanda işlenecek olan çok büyük oranda hassas veri için 'bilmesi gereken' prensibine uygun erişim ve bütünlük gereklerinin tümüyle yerli/milli yazılım ve donanım çözümleri (İşletim Sistemi/Operating System, Firewall/Güvenlik Duvarı, Sanal Özel Ağ/VPN, Güvenli İnternet Erişim Sistemi, Security Information & Event Management / SIEM, Intrusion Detection System/IDS, Intrusion Prevention System/IPS, Network Access Control NAC, Siber Saldırı Erken Uyarı Sistemi / HoneyPot, Data Leakage Prevention / DLP) ile karşılanması, ulusal bilişim güvenliği stratejisi kapsamında, birincil hedef olarak ön planda olmalıdır.

Salgın nedeniyle bilişim kullanıcısı sayısındaki ve bilişim kullanıcılarının çevrimiçi ortamlarda işledikleri verilerin çeşitliliğindeki yoğun artış, sosyal mühendislik kaynaklı saldırıları da ön plana çıkardığından, bu alanda farkındalık eğitimleri ve kamu-spotu faaliyetlerinin planlanması önemlidir. Çünkü herhangi bir siber güvenlik zincirinde en güçlü ve en zayıf halka insandır.

Hızlandırılmış dijitalleşme olarak da nitelendirilebilecek post-Korona döneminde aşağıdaki örnek gelişmelerin çok hızlı bir şekilde hayata geçmesi muhtemeldir:

- e-Devlet olarak lanse edilen dijital dönüşüm programının mikro-servis mimarisiyle tüm kamu kurum ve kuruluşlarını kapsayacak şekilde yaygınlaştırılması
- Gerek vatandaşa yansıyan gerek arka planda yürüyen süreçlerin alabildiğine hızlandırıldığı bir otomasyon sistemine geçilmesi
- Kaynakların daha etkin kullanılabilmesi adına veri merkezlerinin konsolide edilerek her türlü felaket/saldırı senaryosuna karşı gerekli tedbirlerin alındığı bir bulut altyapısının kurulması
- Cüzdanlardaki kimlik kartlarının yerini mobil cihazlardaki yapay zekâ ile desteklenen uygulamaların almasıyla izlenebilirlik ve uyumluluğun en üst seviyelere taşınması
- Çok faktörlü kimlik doğrulama ve blokzincir teknolojilerinden yararlanılarak tüm genel/yerel seçimlerin çevrimiçi yöntemlerle yapılması

Bu oranda hızlı bir dijital dönüşümün etkileri gereği; Ulusal bilişim güvenliğinde oluşabilecek riskin asgari seviyeye çekilebilmesi ortak hedef olup, bilgi sistemleri alanında CIA ve mahremiyet (privacy) için kullanılan yazılım ve donanımın bütünüyle yerli/milli çözümler ile geliştirilmesi artık kaçınılmazdır.

Bilişimin sosyal yaşamdaki kullanımından kaynaklanan güvenlik risklerinin de asgari seviyeye çekilebilmesi için, kullanılmakta olan sosyal medya platformları ve iletişim araçları için de alternatif ve yaygın kullanımı sağlanabilecek yerli/milli çözümlerin üretilmesi gerekmektedir.

KAYNAKÇA

[1] T.C. Ulaştırma ve Altyapı Bakanlığı. n.d. Retrieved May 27, 2020 (https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf).

[2] Stratejik Araştırmalar Merkezi. "COVID-19 Sonrası Küresel Sistem: Eski Sorunlar, Yeni Trendler" Retrieved May 27, 2020 (http://sam.gov.tr/tr/covid-19-sonrasi-kuresel-sistem-eski-sorunlar-yeni-trendler/).

[3] Romm, Tony, "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus." Washington Post. Retrieved May 27, 2020 (https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/).

[4] Corneliu Bjola, Marcus Holmes, "Digital Diplomacy: Theory and Practice." CRC Press. ISBN 9781138843820. March 19, 2015.

[5] TUBITAK BİLGEM, "Milli Açık Anahtar Altyapısı.| MA3." BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ. Retrieved May 27, 2020. (https://ma3.bilgem.tubitak.gov.tr/).

[6] TUBITAK BİLGEM. "AGC-G - Gigabit Ağ Güvenlik Cihazı." BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ. Retrieved May 27, 2020 (https://bilgem.tubitak.gov.tr/tr/icerik/agc-g-gigabit-ag-guvenlik-cihazi).

[7] TUBITAK BİLGEM. "Safir Depo." BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ. Retrieved May 27, 2020 (https://safirdepo.b3lab.org/welcome).

[8] Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. "2019/12 Sayılı Bilgi Güvenliği Tedbirleri Cumhurbaşkanlığı Genelgesi." Retrieved May 27, 2020 (https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/).

[9] Türkiye Siber Güvenlik Kümelenmesi. Retrieved May 27, 2020 (https://portal.siberkume.org.tr/).

[10] Atatürk Araştırma Merkezi Başkanlığı. "Savunma hattı yoktur savunma sathı (175)." Retrieved May 27, 2020 (https://www.atam.gov.tr/nutuk/savunma-hatti-yoktur-savunma-sathi-175-vardir).

[11] Bilgi Teknolojileri ve İletişim Kurumu. "2020-2023 Siber Güvenlik Stratejileri BTK'da Belirlendi." Retrieved May 27, 2020 (https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi).

[12] Stratejik Araştırmalar Merkezi. "Covid-19 Sonrası Küresel Sistem." Retrieved May 27, 2020 (http://sam.gov.tr/tr/wp-content/uploads/2020/04/sam-covid-kitap.pdf).

Salgın Döneminde
İş Sağlığı ve Güvenliği Faaliyetleri

> Çalışma hayatında, salgın gibi afet dönemlerinde belki de en etkin ve herkesin gözünü açıp kulak kabarttığı organizasyonlar, İşyeri Sağlık ve Güvenlik Birimleri (İSGB) olmaktadır.

Orhan Demir – İSG Birim Müdürü / BİLGEM

Dünya Sağlık Örgütü (DSÖ) tarafından COVID-19'un "salgın" olarak ilan edilmesi ve vaka sayılarının tüm dünyada ve ülkemizde hızla artması sonrasında, dünyada ve ülkemizde kamu ve özel sektörde birçok işveren, işyeri faaliyetlerini tamamen durdurmuş veya sınırlandırmış ya da personelinin uzaktan/evden çalışma usulüne geçmesi için çalışmalara başlamıştır. İlgili teknolojik altyapıya sahip işyerlerinde uzaktan çalışma yapılması mümkün olmakla birlikte, işin niteliği gereği uzaktan çalışma modelinin uygulanamayacağı üretim ve hizmet sektörlerinde faaliyet gösteren işverenlerin, işyerlerinde iş sağlığı ve güvenliğini korumak amacıyla gerekli her türlü önlemi almaları daha da bir önemli hal almıştır. Gerek uzaktan çalışmalarda gerekse salgın dönemlerinde, çalışanların sağlığını ve güvenliğini korumak ve bu kapsamda gerekli tedbirleri yürütmede iş sağlığı ve güvenliği faaliyetlerinin ne kadar önemli olduğu bu süreçte bir kez daha görülmüştür.

> Maske gibi tüm atıkların sıfır atık kapsamında, ayrı olarak belirlenen noktalarda toplanmasının ve imha edilmesinin sağlanması, sağlığımızın ve çevremizin korunması için yüksek önem arz etmektedir.

Salgın döneminde iş sağlığı ve güvenliği açısından işyerlerinde alınması gereken tedbirlere kısaca değinirsek, bu dönemde belki de en etkin ve herkesin gözünü açıp kulak kabarttığı organizasyonlar, İşyeri Sağlık ve Güvenlik Birimleri (İSGB) olmaktadır. Çok sık rastlanmayan, belki de elli yüz yılda bir yaşanabilecek bu salgın döneminde pek çok organizasyon hazır olmadığı gibi, İSGB'ler de bazı sıkıntılar yaşadı. Temel odak noktası insan sağlığı ve risk yönetimi olan İSGB'lerin, bu dönemin kurumlarda en hazır organizasyonu olması gerekir. Bu dönemde İSGB profesyonellerinin yapması gereken, kanun ve yönetmelik bazında ilgili kurumların talimatlarını hızlıca devreye sokmak ve denetleyerek gerekli tedbirlerin alınmasını sağlamaktır.

Üç Aşamada Tedbir; İSGB, İşveren, Çalışan

Salgınla mücadele kapsamında kurum tarafından alınan ve titizlikle uygulanan tüm kararlara, çalışanların uyumunun sağlanması ve denetiminin yapılması, bu dönemde çalışan sağlığı için önceliğin kişisel hijyen olduğunun ve temizliğin en önemli faktör olduğunun bilinmesi gerekmektedir. Çalışanlar arasında, maske kullanımı ile fiziki mesafenin korunması ve bu kurala riayetin sağlanması, maskesiz dolaşımın denetimlerle engellenmesi ile farkındalık çalışmalarının artırılması, olmazsa olmaz önlemler kapsamındadır. Ayrıca, maske gibi

tüm atıkların sıfır atık kapsamında ayrı olarak belirlenen noktalarda toplanmasının ve imha edilmesinin sağlanması, sağlımızın ve çevremizin korunması için yüksek önem arz etmektedir.

Çalışanlara sunulan servis, yemek hizmetlerinde ve dinlenme noktalarında gerekli fiziki düzenlemelerin yapılması, bu kapsamda fiziki mesafenin korunarak hijyenin üst düzeyde tutulması, umuma açık alanlarda sıra, oturma düzeni için oluşturulan kuralların uygulanması ve denetlenmesi, yine İşyeri Sağlık ve Güvenlik Birimlerince kontrol altında tutulmalıdır.

Çalışanların, COVID-19 belirtileri göstermeleri halinde (Ateş, Öksürük, Nefes Darlığı vb. hususlarda) nasıl davranacağı ile ilgili bilgilendirmelerin yapılması, salgın dönemine ait acil eylem planının oluşturulması ve eylemlerin belirlenmesi hususları da personeli bilinçlendirme noktasında önem arz etmektedir. Çalışanlara yapılacak el hijyenine dair bilgilendirmeler hususunda, talimatların afiş broşür gibi görsellerle desteklenmeli, ortak kullanım alanlarındaki sık dokunulan yüzeyler için (kapı kolları, telefon ahizeleri, masa yüzeyleri gibi) kullanım talimatlarının oluşturulması, uygulanması ve denetlenmesi, hem İşyeri Sağlık ve Güvenlik Birimi hem de Kurum/Şirket yönetimi işbirliğinde, tüm personele gerekli duyuru kanalları ile ilan edilmeli ve kurallara uyulması sağlanmalıdır.

İşyerinde ortak kullanılan tüm ekipmanların tek kullanımlık hale getirilmesine yönelik tedbirlerin geliştirilmesi, çoklu kullanımı olan parmak izi ve şifreli okuyucuların olduğu alanların gerekli güvenlik tedbirlerinin alınarak devre dışı bırakılması ve alternatif yöntemlerle girişlerin yapılmasının

> **Tüm kurum ve kuruluşların, iş sağlığı ve güvenliği hususlarında gerekli altyapıya sahip olmaları ve zafiyet göstermeden süreci yönetmeleri, ilgili birimlerle etkin bir koordinasyon sağlamaları gerekmektedir.**

sağlanması, ilgili alanların temizliğine yönelik talimatların oluşturulması ve kullanım öncesinde bu alanlarda hijyen sağlanması, kapalı ofislerin sık sık havalandırılması ve temiz hava sirkülasyonun sağlanması, dezenfeksiyon işlemlerinin periyodik olarak yapılması ve sürekliliğinin sağlanması, çalışanlara yönelik olarak ilgili görsellerle farkındalığın oluşturulması ve giriş noktalarında temassız ateş ölçümünün yapılması, işyerinde virüsten koruyucu önlem ve faaliyetlerin temel maddelerini oluşturmaktadır.

İçinde bulunduğumuz dönem içerisinde, uyulması gereken hijyen kurallarının, alternatif yöntemlerle de desteklenerek en etkili şekilde yürütülmesi, virüsün panzehiri niteliğinde olan su ve sabunun birincil temizlik aracı olması, ulaşılamadığı noktalara dezenfektanların konulması ve kullanımı hususundaki talimatlara uyum da, yine işveren, çalışan ve İSGB işbirliğince uygulanan tedbirleri kapsamaktadır.

Ek olarak, salgın döneminde mümkün mertebe toplantıların tele/video konferans yoluyla yapılmasının sağlanması ve bu kapsamda gerekli alt yapının düzenlenmesi, gerçekleşmesinin mümkün olmadığı durumlarda en az katılımcı ile gerekli fiziki mesafe ve kurallar oluşturularak toplantıların düzenlenmesi gibi tedbirlerin alınması,

salgın döneminin en az hasarla atlatılması için İSGB'ler tarafından yapılması gereken faaliyetlerin başında gelmektedir.

Bu dönemde kritik teknoloji alanlarında faaliyet yürüten kuruluşların, tesis güvenlik özel şartlarının yerine getirildiğini ispatlayabilmeleri, gerek faaliyetlerinin riske atılmaması, gerekse çalışanların sağlığının korunması yönünden önem arz etmektedir.

Kritik Savunma Sanayi Hizmeti faaliyetleri yürüten kuruluşların da iş sağlığı ve güvenliği hususlarında gerekli altyapıya sahip olmaları ve zafiyet göstermeden süreci yönetmeleri ve Tesis Güvenlik Koordinatörünün ilgili birimlerle etkin bir koordinasyon sürdürmesi gerekmektedir. Tesis Güvenlik ile ilgili tüm alanlarda, kontrollü bölgelere girişlerde, yetkilendirmelerde gerekli güvenlik tedbirlerinin alınarak yürütülmesi için acil eylem planları oluşturulmalı, bir taraftan insan sağlığı gözetilirken bir taraftan da tesis güvenlik özel şartları ihlal edilmeden gizlilik dereceli projelerin mahremiyeti korunmalıdır.

Yeni Normal: Uzaktan Çalışma

Salgın dönemi ile çalışma hayatında yeni kavramlar ortaya çıkmaya başlamıştır. Uzaktan/evden ve dönüşümlü çalışma gibi çalışma programları, çalışma hayatı kavramlarının üst sıralarında yerini almaya başlarken, belirli altyapıya sahip olan kurumlar, çalışanlarına evlerinden çalışabilme olanağı sundu.

Öte yandan bu kavramlarla birlikte İş sağlığı ve güvenliği faaliyetleri durmamalı. Evden çalışmalarda iş sağlığı ve güvenliği faaliyetlerinin de yürütülmesi gerekli talimatların hazırlanarak çalışanların bilgilendirilmesi gerekmektedir. Bu kapsamda; çalışanların evlerinde temizlik ve hijyen kurallarına uymaları, COVID -19 ile ilgili kendilerinde veya temaslı oldukları birinde belirti olması durumunda hareket tarzının belirlenmesi ve işveren ile koordinasyon içinde olmaları ile ilgili bilgilendirmeler yapılmalıdır. Bununla birlikte, çalışanların ev kazalarına karşı tedbirli olmaları, tehlikeleri bilmeleri ve ilgili aksiyonların neler olacağı ile ilgili farkındalıkların oluşturulması da gerekmektedir.

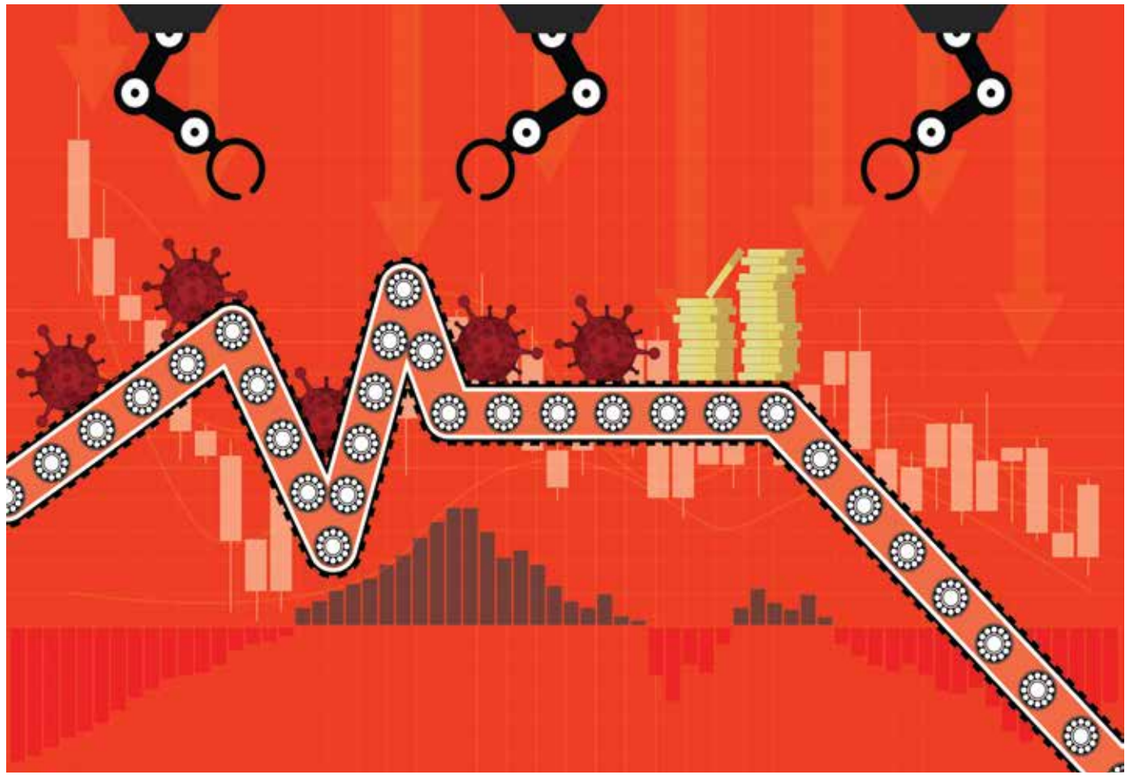
Evde de olsa iş ortamı yaratarak, çalışan personelin ekranlı araçlarla çalışmaları noktasında ergonomi kuralları ile ilgili bilinçleri, kas iskelet rahatsızlıklarının önüne geçebilmek için işyerinde uydukları kurallara aynen uzaktan çalışırken de uymaları hususu ile ilgili talimatlar tekrarlanmalıdır. Tüm bu durumlara mahal vermemek amaçlı, her türlü acil durum ve kazalarda işyerindeki uygulamalara benzer basit yönergeler oluşturulmalıdır.

Normalleşme dönemine geçerken iş sağlığı ve güvenliği ile ilgili faaliyetlerin günün şartlarına göre güncellenmesi ve tedbiri elden bırakmadan yürütülmesi, salgın dönemini en az hasarla atlatmak ve mevcut faaliyetleri etkin ve verimli sürdürmek için bu dönemde biraz daha fazla tedbir ve daha etkin İş sağlığı ve güvenliği Uygulamaları ile hazır olunmalıdır.

Salgın dönemi, hayatımızın her alanını etkilediği gibi çalışma hayatımızı da önemli ölçüde etkilemiş ve farklı bir bakış açısı ile beraberinde farklı bir çalışma düzeni getirmiştir. İSG profesyonellerinin bu ve benzeri acil durumlara hazır olmaları görevlerini etkin bir şekilde yürütmeleri, riskleri göz önünde bulundurarak, yaygın, etkin ve katma değeri yüksek bir çalışma bilinci ile faaliyetlerini sürdürmeleri gerekmektedir. Unutmayalım ki hayatın her alanında iş sağlığı ve güvenliği bizler içindir.

COVID-19'un Ekonomimize Etkileri

> Salgın; öncesinde benzer düzeyde insan, mal ve hizmet izolasyonunun olmaması, dünya genelinde olduğu gibi Türkiye'de de bazı sektörler hariç genel olarak ticaretin yavaşlamasına neden olmuştur.



Dr. Abdullah Altun – Başuzman / BİLGEM KKYBY

Uzakdoğu ülkelerinden yayılarak dünya genelinde etkili olabilecek bir virüs salgını öncesinde, bazı çevrelerce öngörülmekteydi. Az gelişmiş ve gelişmekte olan ülkelerin bu salgından daha fazla etkileneceği düşünülse de, salgının tüm ülke ekonomileri üzerinde beklenenin ötesinde bir etkisi olmuştur. Bazı veriler yıllık bazda yayınlandığı için, şimdilik ancak aylık bazda yayınlanan veriler ışığında değerlendirme yapabiliyoruz.

Bu küresel salgınla mücadelede Türkiye, en başından beri sorumlu ve ciddi bir yaklaşım ortaya koymuştur. Toplum sağlığını korumada gereken önlemlerin hızlıca alınması ve Bilim Kurulu'nun oluşturulması, başarılı uygulamalardandır. Bununla birlikte, toplumun her kesiminin bu süreci en az etkiyle atlatabilmesi için önemli ekonomik destekler sağlandı. Ayrıca gelişmiş ülkeler, serbest dolaşımdaki tıbbi malzemelere el koyarak kötü sınavlar vermişken Türkiye, bu süreçte dünyada en fazla yardım yapan ülke unvanına sahip olmuştur.

Ekonomik Göstergeler

Daha önce benzer düzeyde, insan, mal ve hizmet izolasyonunun olmaması, dünya genelinde olduğu gibi Türkiye'de de bazı sektörler hariç genel planda ticaretin yavaşlamasına neden olmuştur. Türkiye açısından bu zorlu sürecin ekonomik göstergelerdeki etkilerini inceleyelim. Figür 1' deki yeni kurulan şirket sayılarına baktığımızda, Nisan ve Mayıs aylarında koronavirüs etkisiyle düşüş görülmekteyken Haziran ayı istatistiklerinde, Nisan ve Mayıs aylarını telafi eden toparlanmalar dikkat çekmektedir.

> Küreselleşmenin bugüne kadar iki büyük çözülme ile gerçekleştiği ve üçüncü büyük çözülmenin arifesinde olduğumuz kabul görmektedir. Birincisi Sanayi Devrimi ile ikincisi, üretimin farklı coğrafyalara yayılmasıyla sağlanmıştır. Üçüncüsü ise, insan gücü ve makinelerin gitgide birbirinden ayrışmasını ifade etmektedir.

Tablo 1'de yeni kurulan yabancı ortaklı şirketlerin istatistikleri incelendiğinde; Nisan ayında belirgin bir azalış, Mayıs ayındaysa, yeni kurulan şirket adedindeki artış ve 1 milyar TL üzerindeki yabancı sermaye miktarı görülmektedir.

Figür 1. Kurulan Şirket Sayısı (Aylık)

	2019		2020	
	Sayı	Ortak Olunan Şirketlerdeki Yabancı Sermaye Toplamı (TL)	Sayı	Ortak Olunan Şirketlerdeki Yabancı Sermaye Toplamı (TL)
Ocak	1.213	256.779.545	1.076	268.864.262
Şubat	1.035	277.033.165	1.142	272.556.125
Mart	1.082	289.249.425	942	310.530.179
Nisan	1.098	219.377.938	196	244.650.626
Mayıs	1.055	451.234.328	3.578	1.166.450.109
Haziran	696	207.055.898	619	197.890.225

Tablo 1. Yabancı Ortaklı Yeni Kurulan Şirketler (Aylık)

Tablo 2'de ciro endeksleri incelendiğinde; Mart ayı ile başlayan ve Nisan ayında bir önceki aya göre %24'lere varan ciddi bir düşüş bulunuyorken, Mayıs ayı ile toparlanmanın başladığı görülmektedir.

Ay	İndeks (2015=100)	Aylık Değişim (%)
Oca.20	217,5	1,0
Şub.20	221,8	2,0
Mar.20	203,6	-8,2
Nis.20	153,4	-24,7
May.20	172,6	12,5

Tablo 2. Ciro Endeksleri ve Değişim Oranları
(Sanayi, İnşaat, Ticaret ve Hizmetler)

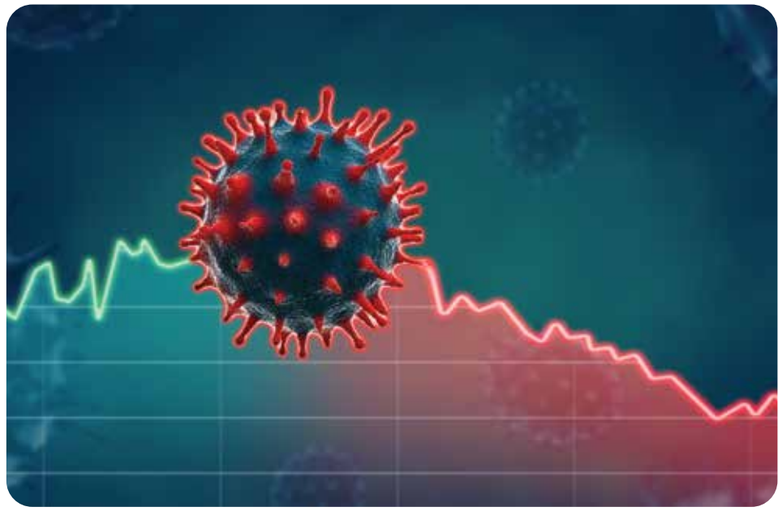
Tablo 3'te görüldüğü üzere, Nisan ayında ciddi şekilde düşmüş olan ihracatımız, Mayıs ayı itibariyle toparlanma sinyalleri vermektedir. Haziran ayı rakamlarının geçen yılın aynı ayına göre %15,77 artış göstermesi, ilgili bütün kurum ve kuruluşların ihracatçılarımız ile koordineli hareket ettiğine güzel bir örnektir.

Bu verilerle birlikte iç piyasanın canlılığını anlamamız açısından bakmamız gereken istatistiklerden biri de perakende ciro istatistikleridir. Tablo 4'e göre; dikkat çeken en belirgin düşüş, tekstil sektöründedir. Azalışlar sonrasındaki artışlar, sağlık tedbirleriyle birlikte ekonomik hayatın canlılığını muhafaza etmenin önemini göstermektedir. Posta yolu ve internet üzerinden yapılan alışverişlerdeki inanılmaz artış, pandemi döneminin acaba teknolojik dönüşümde bir katalizör etkisi mi olacak sorusunu tekrar hatıra getiriyor.

Turizm bu süreçte en çok etkilenen sektörlerin başında gelmektedir. Nisan ve Mayıs aylarını kıyaslarsak, geçen yılın aynı ayına göre %99 üzerinde bir azalma görülmektedir. Sağlanan desteklerle Haziran ayında yerli ve yabancı turist sayısında artış başlamıştır.
Bu noktada sağlık turizminin önemi gittikçe artmaktadır. Türkiye'nin sağlık sisteminin kalitesi, sadece sağlık sistemi zayıf olan çevre ülkeleri açısından değil, sağlık sisteminde uzun bekleme süreleri olan batılı ülkeler tarafından da Türkiyenin cazip bir destinasyon olarak görülmesini sağlamaktadır. Sağlık teknolojilerindeki yerlileşme, yakın zamanda Türkiye'nin sadece sağlık hizmetleri sunumunda değil, aynı zamanda tıbbi teçhizat üretim ve ihracatında da ciddi bir hamle yapacağını göstermektedir.

Küresel Ekonomik Dönüşüm Süreçleri

Bu yaşadığımız süreç globalleşmeden geriye dönüş müdür, yoksa farklı bir algoritmayla yeni bir globalleşme dalgasının arifesinde miyiz? Bir görüş, ulus ekonomilerinin ortaya çıkması ve öz yeterliliklerin öneminin artması şeklindedir. Bu bir noktaya kadar doğru bir söylem olsa da resmin



	Ocak	Şubat	Mart	Nisan	Mayıs	Haziran
İhracat	14 692 322	14 596 878	13 348 618	8 980 750	9 967 161	13 469 000
İthalat	19 206 817	17 633 489	18 810 699	13 553 172	13 386 913	16 305 000

Tablo 3. Türkiye Aylık Dış Ticaret Verileri (Bin ABD $)

bütünü farklı motifler içermektedir.
Küreselleşmenin bugüne kadar iki büyük çözülme ile gerçekleştiği ve üçüncü büyük çözülmenin arifesinde olduğumuz kabul gören önemli yaklaşımlardan biridir[1]. Birinci büyük çözülme, Sanayi Devrimi ile üretim ve tüketimin bilhassa buharlı gemiler ve trenlerle birbirinden gitgide ayrışması.

İkinci büyük çözülme, küresel değer zincirleri devrimi olarak ifade edilmekte olan üretimin alt safhalarının başka coğrafyalarda gerçekleştirilmesidir. Daha önce gelişmiş ülkeler diye sınıflandırılan ülkelerde yoğunlaşmış olan üretim süreçleri, maliyetlerin düşürülmesi amacıyla yavaş yavaş gelişmekte olan ülkelere doğru kaydı. Tabi bu noktada sermaye, fikri-sınai (royalti) ve lisans hakları, sermaye malları ve ara malları gibi stratejik öneme sahip bileşenler, gelişmiş ülkelerin ellerindeydi. Bu sürecin ciddi bir şekilde sekteye uğraması 2008 yılındaki küresel ekonomik krizle olmuş, korumacı politikalar yavaş yavaş ortaya çıkmaya başlamıştır. Sonrasında ticaret savaşları diye nitelendirilen, ABD'nin Çin ile olan mücadelesi, korumacı ekonomik politikaların hepten artmasıyla sonuçlanmıştır.

Çin, ikinci büyük çözülme dediğimiz 1990'larla başlayan bu dönemin son zamanlarına doğru artık hem royalti ve lisans hakkı üretiminde liderliğe yükselirken, yurtdışı sermaye yatırımları ile de yayılmacı politikalar izlemektedir. Tabi bu da farklı bir rekabet alanı anlamına gelir. Bu noktada bir örnek vermek gerekirse; 2018 yılında dünya genelinde gerçekleşen 3.236.300 patent başvurusunun %46,4'ü olan 1.542.002 başvuru Çin tarafından gerçekleştirilmiştir[2]. Buna ek olarak, WIPO (Dünya Fikri Mülkiyet Göstergeleri) 2019 Raporu'na göre; tüm dünyadaki faydalı model başvurularının %96'sı, marka tescil başvurularının %51,4'ü ve endüstriyel dizayn tescil başvurularının %54'ü Çin tarafından gerçekleştirilmiştir. Bu değişen rekabet koşulları, rekabet gücünü kaybeden ülkelerin bu durumu tersine çevirmeye yönelik neler yapacağı ile ilgili soru işaretlerini de birlikte getiriyordu.

Üçüncü büyük çözülme ise, insan gücü ve makinelerin gitgide birbirinden ayrışmasını ifade etmektedir. Yani yanında operatörü olmadan otonom çalışan makineler, bu makinelere gereken müdahalelerin çok uzak mesafelerden yapılabilmesi, servis hizmetlerinin uzaktan verilmesi ve hatta uzaktan 3D[3] yazıcılara yedek parçaların yazdırılarak yerinde işin çözülmesi gibi durumlar bu bağlamda değerlendirilmek-

Ekonomik Faaliyet	Ocak	Şubat	Mart	Nisan	Mayıs
Perakende ticaret	169,4	171,0	182,0	144,3	154,2
Gıda, içecek ve tütün	177,5	181,9	228,5	214,9	208,3
Gıda dışı (otomotiv yakıtı hariç)	166,7	172,1	166,7	118,6	138,6
Bilgisayar, bilgisayar donanım ve yazılımları, kitap, iletişim aygıtları v.b.	157,7	169,5	163,1	116,4	128,1
Ses ve görüntü cihazları, hırdavat, boya ve cam, elektrikli ev aletleri, mobilya v.b.	114,0	127,7	144,0	109,8	131,0
Tekstil, giyim ve ayakkabı	193,1	182,2	130,9	43,3	91,7
Eczacılık ürünleri, tıbbi ve ortopedik ürünler, kozmetik ve kişisel bakım malzemeleri	248,2	245,6	272,6	235,3	203,7
Posta yoluyla veya internet üzerinden	322,8	365,4	411,4	535,7	622,2
Otomotiv yakıtı	164,2	151,4	152,3	105,5	113,9

Tablo 4. Perakende Ciro Endeksi (2015=100)

	YILLAR			% DEĞİŞİM ORANI	
AYLAR	2018	2019	2020*	2019/2018	2020/2019
OCAK	1 461 570	1 539 496	1 787 435	5,33	16,11
ŞUBAT	1 527 070	1 670 238	1 733 112	9,38	3,76
MART	2 139 766	2 232 358	718 097	4,33	-67,83
NİSAN	2 655 561	3 293 176	24 238	24,01	-99,26
MAYIS	3 678 440	4 022 254	29 829	9,35	-99,26

Tablo 5. Türkiye'ye Gelen Yabancı Ziyaretçilerin Yıllara ve Aylara Göre Dağılımı

tedir. Bununla birlikte 5G, nesnelerin interneti (IoT), büyük veri (big data), makine öğrenmesi ve yapay zekâ alanlarında ortaya çıkan gelişmeler, makinelerin robotlaşmasına yönelik ciddi dönüşümler ortaya koymaktadır. Bütün bunlar yeniden tanımlanmaya çalışılan ürünler veya hizmetler olarak karşımıza çıkabilecektir.

İkinci büyük çözülmedeki küresel ekonominin algoritmasını dikkate alırsak üçüncü büyük çözülmede nasıl bir algoritma ile karşılaşabiliriz? Bu noktada gelişmiş ülkeler royalti ve lisanslarıyla yine önde olmak isteyecektir. Üretimin alt safhalarının farklı coğrafyalarda gerçekleştirilmesinden yerel olarak üretilmesine dönüş süreci yaşanması durumunda dahi, daha önceden sermaye malları satan ülkelerin yine sermaye malları satarak başka ülkelerin üretim altyapılarının kurulmasından kazanmaya devam etmek isteyecekleri açıktır. Aynı durum ara mal ihracatı açısından da geçerlidir. Yani ikinci büyük çözülmede royalti ve lisanstan, sermaye mallarından ve ara maldan kazananlar, üçüncü büyük çözülmede aynı şekilde kazanmaya devam etmek isteyecektir. Bu noktada ürünleri ve üretim hatlarını yeniden tanımlayabilecekleri bir tarzda hareket etmek isteyecekleri, ikinci büyük çözülmede değişen rekabet koşullarını tersine çevirmeye zorlayacakları da gözden kaçmamalarıdır.

Değerlendirme

Türkiye, bu noktada önemli sorumluluklara ve fırsatlara sahiptir. Türkiye, dünyadaki değişim ve dönüşüm süreçlerinin bir sömürge düzeninden diğer bir türüne dönüşmemesi ve insani bir şekilde gerçekleştirilmesinde insani kalkınma diye adlandırılan önemli bir role sahiptir. Türk Dış Siyasetinde bunu son yıllarda açıkça görmekteyiz.

Türkiye, yerlilik ve millilik bağlamında da savunma sanayi başta olmak üzere önemli atılımlar yapmaktadır. Bu çalışmaları makro düzeyde küresel ve bölgesel değer zincirleriyle haritalandırmak ve olası dönüşümleri senaryo bazlı simüle etmek

daha etkin sonuçlar kazandırabilir. Bununla birlikte sermaye malı ve ara malı üretiminde de Türkiye'yi ileriye taşıyacak stratejiler özel önem arz etmektedir.

Yukarıda bahsettiklerimiz çerçevesinde ülkeler ve firmalar düzeyinde değer zincirleri oluşturmak veya dönüştürmeye yönelik çalışmalar, koronavirüs sonrasında ortaya çıkabilecek durumdan rekabet avantajı elde etmek açısından önemlidir.

KAYNAKÇA

1. Türkiye Ticaret Sicili Gazetesi Verileri; TOBB Aylık Kurulan/Kapanan Şirket İstatistikleri: https://www.tobb.org.tr/BilgiErisimMudurlugu/Sayfalar/KurulanKapananSirketistatistikleri.php
2. www.tuik.gov.tr
3. Turizm İstatistikleri; https://yigm.ktb.gov.tr/
4. T.C. Ticaret Bakanlığı 2020 Yılı Haziran Ayı Veri Bülteni: https://ticaret.gov.tr/data/5efd885513b876a83c6f2bcc/2020%20Y%C4%B1l%C4%B1%20Haziran%20Ay%C4%B1%20Veri%20Bu%CC%88lteni-4.pdf

Dipnotlar

[1]Daha detaylı okuma için Richard Baldwin' in makalesi: Büyük Ayrışma; https://www.economist.com/finance-and-economics/2007/01/18/the-great-unbundling

[2] WIPO Dünya Fikri Mülkiyet Göstergeleri 2019 Raporu; https://www.wipo.int/publications/en/details.jsp?id=4464&plang=EN

[3] 3 Boyutlu Baskının Ticaret Etkileri; https://voxeu.org/article/trade-effects-3d-printing

Kızılötesi Füze İkaz Sistemleri

"Füze ikaz sistemi, bir elektronik harp süitinin kritik bir parçası olup platforma doğru atılan/gelen füzelere karşı tedbir uygulamak ve ikaz üretmek maksadıyla kullanılmaktadır."

Halil İbrahim Cüce - Başuzman Araştırmacı, Muhammet Özbay - Uzman Araştırmacı / BİLGEM İLTAREN

Savunma stratejileri, gelişen teknoloji ile beraber sürekli bir değişim geçirmektedir. Geçen yüzyılın başında karasal uzun savunma hatları oluşturmak ve olası düşman hatlarına karşı mevzi kazanmak öncelikli iken, II. Dünya Savaşı'nda tank ve hava platformları ön plana çıkmıştır. Körfez savaşında ise her biri sensör ve akıllı algoritmalarla donatılmış taktik ve balistik füzelerin oldukça etkili olduğu görülmüştür. Bu durum ve özellikle omuzdan atılan füzelerin nispeten kolay edinilmesi, bu tür füzelere karşı platformların korunma ihtiyacını beraberinde getirmiş ve çeşitli yöntemlerin geliştirilmesine neden olmuştur. Herhangi bir tehditten korunmanın öncül şartı, tehdidin olabildiğince erken algılanmasından geçmektedir. Benzer durum, özellikle hava platformlarına atılan füzeler için de son derece kritiktir.

Füze tehditlerine karşı ikaz ve korunma, 1960'lı yıllarda Radar İkaz Alıcı (RWR) geliştirme çalışmaları ile başlamıştır. Bu çalışmalar, günümüzde elektronik harp olarak adlandırılan sisteme evirilmiş ve altında birçok alt sistemi barındıran hava platformlarının önemli bir aviyonik paketi haline gelmiştir. Bir hava platformu elektronik harp suiti şu alt sistemlerden oluşmaktadır:

- Elektronik Harp Yönetim Sistemi (EWMS)
- Radar İkaz Alıcı (RWR),
- RF Karıştırıcı/Aldatıcı (Jammer)
- Karşı Tedbir Salım Sistemi (CMDS)
- Lazer İkaz Alıcı (LWR)
- Füze İkaz Sistemi (MWS)

Füze İkaz Sistemleri

Füze İkaz Sistemleri (FİS), sabit ve döner kanatlı hava platformlarını, güdümlü füzelere karşı korumak için kullanılan elektronik harp destek sistemleri arasında yer almaktadır. Bu sistemlerin temel görevi, platforma yöneltilmiş olan güdümlü füzeleri en kısa zamanda tespit edip karşı tedbir sistemine ve/veya elektronik harp suit merkezine bildirmektir.

II. Dünya savaşı zamanlarında savaş meydanlarında belirmeye başlayan hareketli hava platformlarının (uçak, helikopter vb.) bertaraf edilebilmesi maksadıyla kızılötesi (KÖ) güdümlü füze teknolojisi ortaya çıkmıştır. 1950 yıllarında hava-hava füzelerinin de ortaya çıkmaya başlaması, bir askerin taşıyabileceği ebatlarda ve omuzdan atılabilen füzelerin de üretilebilmesinin yolunu açmıştır. Bu sayede 1960 yıllarında kısaltması MANPADS (Man Portable Air Defence) olan alçak irtifa hava savunma sistemleri konsepti ortaya çıkmıştır. Radar özellikli füzelerin yaygın olarak üretilmesine rağmen 1960 yılından sonra hedef alınan hava araçlarının yaklaşık olarak %70'inin MANPADS saldırılarıyla düştüğü belirtilmektedir. Sovyet Rusya'nın, Afganistan'a müdahalesi sırasında yaklaşık olarak 260 adet hava aracını MANPADS saldırılarında kaybettiği bilinmektedir.

Hava araçlarının MANPADS saldırılarına bu denli maruz kalmasının elbette birçok farklı sebebi vardır, fakat 3 ana sebepten bahsetmek mümkündür. Bunlardan birincisi; bazı KÖ füzelerin kısa menzillerden (500 m – 6 km) atılabilmesi, yüksek hızlara ulaşabilmesi (1.5-2 Mach) ve bu nedenle de pilotun füzeyi farkedip kurtulmasına fazla zaman kalmamasıdır. İkinci sebep olarak, KÖ füzelerin ortama bir yayın yapmadan pasif bir şekilde hedefini tespit etmesi sebebiyle, hava aracının herhangi bir sistem ile füzenin fırlatılacağını algılama imkânı olmaması gösterilebilir. Üçüncü sebep, hava aracının füzeyi fark edebilmesine rağmen füzeyi yanıltmak için uyguladığı karşı tedbir uygulamalarına, füzelerin giderek artan oranlarda sahip oldukları yeni teknolojiler ile aldanmamasıdır.

Hava platformlarını füzelerden korumak için başvurulan ilk yöntemler arasında, sürekli açık tutulan çok yönlü KÖ karıştırıcıları ve tehlike hissedildiği durumlarda herhangi bir tespit sistemi kullanılmadan sadece insan faktörüyle platformdan atılan ateş topları (flare, ısı fişeği) gösterilebilir. Füze teknolojisinin ilerlemesi ile çok yönlü KÖ karıştırıcıların etkisi hızla azalmıştır. Herhangi bir tespit sistemi kullanılmadan atılan ateş topları bir miktar önleme sağlasa da, platformlara çok sayıda ateş topları konulamaması, füzelerin insan faktörüyle tespit edilip aksiyon alınmasının çok zor olması ve hava araçlarını kullanan personelin işlerini de artırması gibi sebeplerden dolayı bu yöntemler etkisini yitirmiştir. Bu nedenle, hava araçlarına tehlike oluşturan füzeleri otomatik olarak tespit edebilen ve karşı tedbir sistemlerine ya da elektronik harp suit merkezine haber verebilen sistemlere ihtiyaç duyulmuştur.

Güdümsüz ya da KÖ, RF, Lazer gibi farklı güdümlere sahip füzeler, hava araçlarına tehdit oluşturabilmektedirler. Bu nedenle FİS'lerin bu tarz füzelerin hepsini tespit edebilecek kabiliyette tasarlanması gerekmektedir. FİS'lerin tasarımı her füzede ortak olan iki ana temele dayanmaktadır. Bunlardan birincisi; her füzenin hareketlenmek için kullandığı ve yüksek ışıma yayan bir motorunun olması, ikincisi de füzelerin hedeflerine yüksek hızlarda yaklaşıyor olmasıdır.

Tip	Özellikler	
SD-DD	Avantajları	Uzun menzil, her hava koşulunda çalışabilme, füze ışımasından bağımsız tespit kabiliyeti, füze menzili ve çarpmaya kalan süre hesaplayabilme kabiliyeti.
	Dezavantajları	Aktif yayın, düşük irtifalarda güçlü yer yansıması riski, helikopter platformlarında pal enterferansı, taktik füzelerin düşen radar kesit alanı sorunu.
KÖ	Avantajları	Yakıt bitimi sonrası da dahil hem egzoz ışıması hem de sıcak motor tespiti, düşük atmosferik zayıflatma (Ultraviyole banda göre daha uzak mesafelerden tespit yapabilme yeteneği).
	Dezavantajları	Güçlü arkaplan gürültüsü, uzun menzilde algılama sağlayan hassas detektörün kısa menzildeki yüksek ışımalarda doyuma uğrama riski, soğutma gereksinimi durumunda sistemin karmaşıklaşması riski.
UV	Avantajları	Minimal arkaplan gürültüsü ve bu sayede sinyal işleme kolaylığı ve sistem karmaşıklığının düşmesi, soğutma gereksiniminin olmaması, düşük maliyet, olgunlaşmış teknoloji.
	Dezavantajları	Füze yakıtının bitmesinden sonra tespit yapılamaması, ozon zayıflatması sebebiyle kısıtlı menzil, arkaplan gürültüsünün insan yapımı (şehir ışıkları, endüstriyel bölgeler vb.) ve ateş gibi doğal kaynaklarla artması.

Tablo 1. FİS Tipleri-Avantaj ve Dezavantajlar

Füze İkaz Sistemi Tipleri

Bahsi geçen iki temel üzerinden tasarlanan FİS'ler üç farklı tipte ortaya çıkmaktadır. Bunlardan birincisi radar tabanlı (Sürekli Dalga, Darbe Doppler) tespit gerçekleştirirken diğer iki tanesi optik/görüntüleme (Kızılötesi, Ultraviyole) tabanlı sistemlerdir.

Sürekli Dalga ya da Darbe Doppler (SD - DD)

Temel olarak platform etrafına radyo dalgaları yayıp sahnede füze varsa, geri yansıyan radyo dalgalarındaki frekans kaymalarının (füzenin yüksek hızından dolayı) tespitine dayanmaktadır. RWR sistemleri ile çakışmamaları için, genel olarak elektro manyetik spektrumun L bandında (1 ila 2 gigahertz arasındaki radyo spektrumu frekans aralığı) çalışmaktadır.

Kızılötesi Görüntülemeli (KÖ)

Füze egzozundan yayılan yüksek ışımaların, kızılötesi bandının orta dalga boyu olarak adlandırılan kısmında (3-5 µm) tespit edilmesine dayanmaktadır. Mekanik taramalı ya da FPA (bir bakan dizi) şeklinde tasarlanabilmektedirler.

Ultraviyole Görüntülemeli (UV)

Füze egzozundan yayılan yüksek ışımaların, ultraviyole bandının güneş körü olarak adlandırılan kısmında (0.2-0.3 µm) tespit edilmesine dayanmaktadır. Farklı tiplerdeki FİS'lerin avantaj ve dezavantajları Tablo 1'de özetlenmiştir.

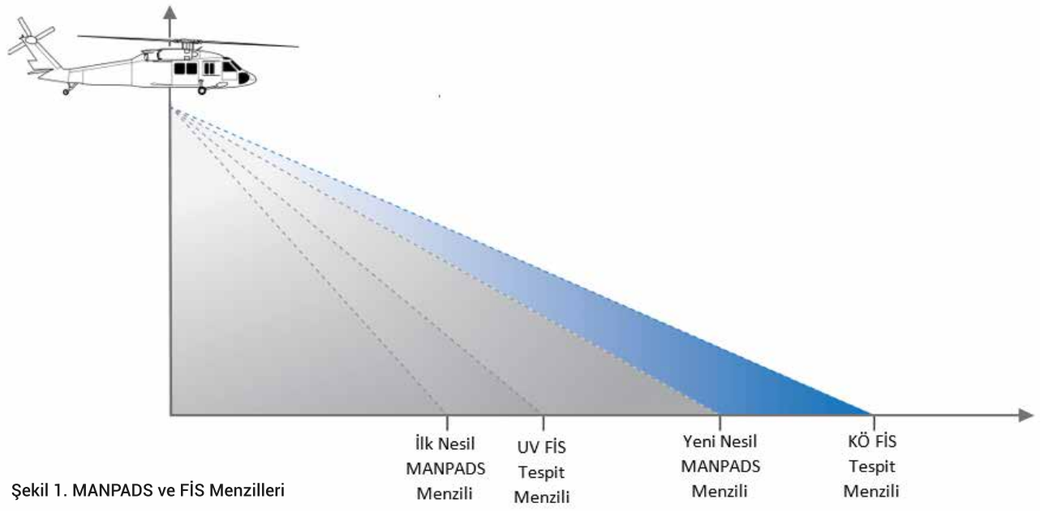
Bahsedilen özelliklere göre bir FİS farklı konseptlerde kendine yer bulabilmektedir. Örneğin UV detektörler kısa menzilde düşük arkaplan gürültüsüne sahip olması sebebiyle, genelde helikopterler ve kargo uçakları gibi göreceli düşük hızlarda seyreden hava araçlarında tercih edilmektedir. KÖ FİS'ler, orta/uzun menzilden tespit kabiliyetine sahip olmaları hasebiyle genelde savaş jetleri gibi yüksek hızlarda seyreden hava araçlarında tercih edilmektedir. Çünkü bu tarz hava araçlarına yoğunlukla, orta/uzun menzillerden atılabilen füzeler tehdit oluşturmaktadır.

Gelişen teknoloji ile beraber FİS'lerin de performansları artırılmakta ve yeni kabiliyetler eklenerek herhangi bir tehlike anında hava araçlarının bekası sağlanmaktadır. Füze fırlatma noktası tespiti, durumsal farkındalık, tehdit önceliklendirme gibi ilave kabiliyetleri ile KÖ füze ikaz sistemini karşılamak mümkündür.

Kızılötesi Füze İkaz Sistemleri

Teknolojinin gelişmesi ile beraber aktif radar yapısı kullanan füze ikaz sistemleri, yerini UV bant sensör kullanan sistemlere terk etmiştir. Günümüzde ise kızılötesi görüntülemedeki gelişmeler, bu sensörlerin füze ikaz sistemlerinde de kullanılabilirliğinin önünü açmıştır.

Kızılötesi füze ikaz sistemi, genellikle MWIR (Orta Dalga Kızılötesi) bandında algılama yapan sezimciler ile platforma doğru atılan veya gelen füze tehditlerini algılar. İçinde barındırdığı algoritmaları ile tespit ve teşhis işlemi yaparak pilota görsel ve sesli ikaz üretmektedir. Aynı zamanda otomatik modda, karşı tedbir salım sistemini aktive ederek saman veya ısı fişeği atılmasını sağlamaktadır.



Şekil 1. MANPADS ve FİS Menzilleri

Kızılötesi füze ikaz sisteminin etkinliğini gösteren kritik parametreler şunlardır:

- Uzun mesafeden tespit
- Yüksek tespit oranı
- Hızlı reaksiyon
- Çarpışma anına kalan süre
- Tam kapsama alanı
- Çoklu tehdit tespit ve izleme
- Yüksek açısal çözünürlük hassasiyeti
- Düşük yanlış ikaz oranı
- Farklı hava ve görünürlük koşullarında güvenirlik ve yüksek performans
- Otomatik karşı tedbir salım sisteminin aktive edilmesi
- Olay tabanlı veri kayıt
- Yüksek güvenirlik
- Otomatik/yarı otomatik çalışma modları

Kızılötesi Füze İkaz Sistemi Bileşenleri

Kızılötesi tabanlı füze ikaz sistemi; KÖ sensör, işlemci ile kontrol ve gösterge birimlerinden oluşmaktadır.

KÖ Sensör

Füze ikaz sistemlerinde kullanılan sensörler, günümüzde çoğunlukla spektrumun ultraviyole bandını kullanmaktadır. Bu dalgaboylarında, düşük yanlış alarm oranında doğal veya insan kaynaklı UV yayınlarının algılanabilmesi için arkaplan etkilerinin oldukça düşük veya hiç olması önem arz etmektedir. Bu da otomatik kendini koruma sistemleri için olmazsa olmaz bir koşul olarak çokça değerlendirilmektedir.

UV dalga boyunda atmosfer, UV yayınlarını güç bir şekilde soğurduğu için tehdit algılama mesafesi, birkaç kilometre olabilmektedir. Bu tip sensörler, UV yayını güçlü eski tip füzeler için gerekli reaksiyon zamanı sağlamakta ancak modern, yeni nesil ve uzun mesafeli füzeler için bahse konu karşı tedbir üretmek için reaksiyon süresi yeterli olmayabilmektedir. Kızılötesi bant çalışan sensörleri, uzak mesafelerden yeni nesil yakıt sistemi olan füzelerin kızılötesi dalgaboyunda yaptıkları yayınları algılayabilme kabiliyetine sahip olduğundan, geleceğin başarılı füze ikaz sistemlerin ayrılmaz bir parçası olacaktır.

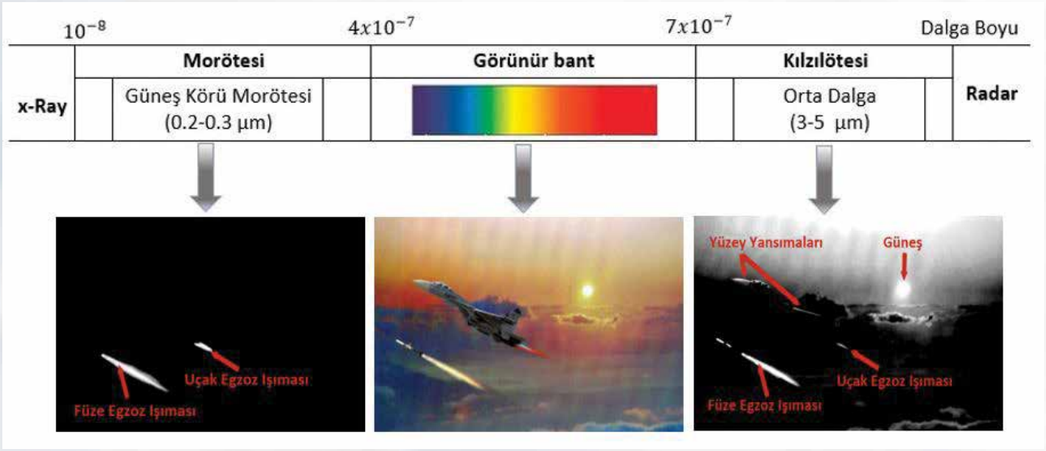
Diğer taraftan, karmaşık arkaplanlı ortamlarda füze egzozundan yayılan ışımaların kızılötesi bantta algılanmasıyla oluşturulan görüntülerden düşük yanlış alarm oranında ikaz üretmek, karmaşık görüntü işleme algoritmaları gerektirmektedir. Günümüz teknolojisinde 3-5μ bandında veya bu bant içinde farklı iki alt bant algılama yapan sensörlerin kullanımına yönelik çalışmalar canlılığını korumaktadır.

KÖ Sensörler; KÖ detektör, soğutucu, okuma devresi, opto-mekanik aksamlar ve koruyucu mekanik yapıdan oluşmaktadır. Ancak detektör, soğutucu ve okuma devresi, KÖ sensörün en kritik parçaları olup tasarım ve üretilmesi yüksek teknolojik alt yapı gerektirmektedir. Diğer yandan KÖ sensörün görüş açısı, gürültü oranı, çözünürlük derecesi, bit derinliği ve çerçeve hızı, KÖ füze ikaz sisteminin operasyonel performansında etkin olan parametrelerdir.

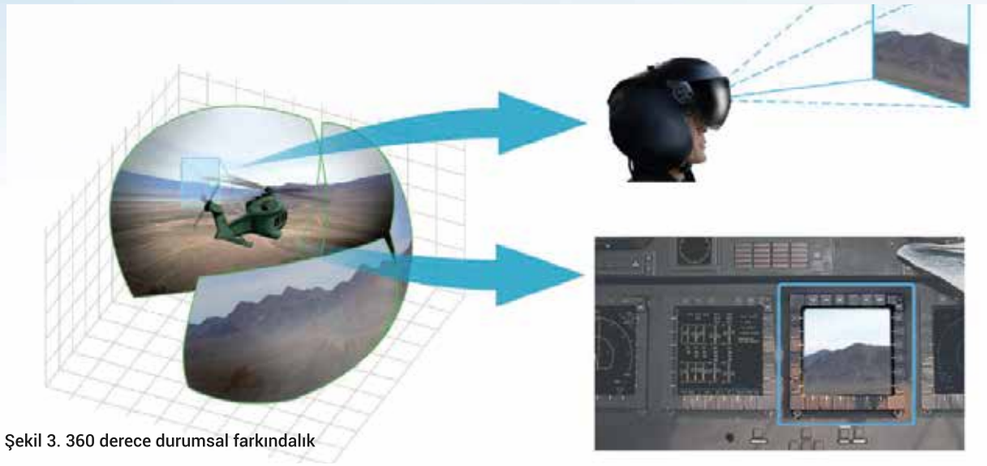
İşlemci

KÖ sensörlerden okunan görüntü ya da verilerin işlenip KÖ Füze İkaz Sisteminden beklenen kararların üretildiği birimdir. İşlemciyi sistemin beyni olarak nitelemek yanlış olmayacaktır. Aynı zamanda platform ve platform üzerindeki diğer Elektronik Harp(EH) bileşenleri ile koordinasyon, bu birim üzerinden yürütülmektedir.

İşlemci, üzerinde füze ikaz sisteminin olmazsa olmaz görevlerini yerine getiren karmaşık görüntü işleme ve karar destek algoritmaları koşmaktadır:



Şekil 2. Dalgaboyları ve örnek görüntüler



Şekil 3. 360 derece durumsal farkındalık

- **Ön işlemler:** Süzgeçler ve veri en iyileme işlemleri
- **Tespit:** Muhtemel ve aday tehditlerin tespit edilmesi
- **Teşhis:** Aday tehditlerin tehdit olarak etiketlenmesi
- **İzleme:** Teşhis edilen tehdidin izlemeye alınması
- **İkaz:** Sesli/görsel ikaz üretilmesi
- **Karşı tedbir:** Karşı tedbir salım sisteminin aktive edilmesi
- **Koordinasyon:** Platform ve EH Suit ile koordinasyon

Kontrol ve Göstergeler

KÖ Füze İkaz Sistemlerinin insan-makine arayüz işlevlerini yerine getiren buton ve ekrandan oluşan bileşenidir. Sistemin kapatılıp açılması, çalışma modlarının seçilmesi, işlemci tarafından üretilen görsel ve sesli ikazların sergilenmesi kontrol ve gösterge tarafından yerine getirilmektedir. Kontrol ve gösterge bileşeni, KÖ Füze İkaz Sistemlerinin bir parçası olabileceği gibi hava platformlarında yer alan halihazırdaki çok fonksiyonlu kontrol ve göstergelere de entegre edilebilmektedir.

360° Durumsal Farkındalık

Teknolojinin her alanda baş döndürücü hızla ilerlemesi, KÖ Sensörlerin ve işlem gücünün kabiliyetlerini sürekli artırmaktadır. KÖ sensörlerin yüksek çözünürlükte ve daha fazla bilgi içeren veriler sağlaması ve bu verileri düşük güç tüketimi ile işlemeye imkân veren yeni işlemci mimarileri, platformların yeni harekât kabiliyetlerine sahip olmasının önünü açmaktadır.

Platforma yerleştirilen KÖ sensörler, aslında platformun 360° her yönünü gören birer göz olarak düşünülebilir. Bu gözlerden alınan verilerin son nesil işlemci mimarisi üzerinde işlemesi yapılarak platforma, 360° farkındalık özelliği kazandırılmaktadır.

360° Derece farkındalık, tehdit füzelerinin tespit edilmesinin yanında;

- Platformun 360° etrafını gösteren siferik ve panaromik görüntü
- Tehdit platform tespiti ve atış kontrol radarı veya IRST yönlendirme
- Kalkış, iniş ve parklar desteği
- İstihbarat tabanlı görüntü alma

gibi ilave özellikler, platformun kullanım amaçlarının çeşitlendirilmesine, kaza ve kırımların minimize edilmesine ve harekât kabiliyetlerinin artırılmasına katkı sağlamaktadır.

Sonuç

1990 yıllardan sonra yapılan askeri harekâtlarda insanlı veya insansız uçar platformların ve akıllı füzelerin kullanımı, harekâtların başarısını artırmaktadır. Uçar platformların bu denli yoğun kullanılması ve özellikle omuzdan atılan füzelerin değişik gruplarca kolay edinilmesi, platformların bir füze saldırısına uğrama ihtimalini de aynı oranda artırmaktadır. Bir platformun düşürülmesi ve pilot kaybı bir ülke için maddi ve manevi kayıpların yanında önemli bir prestij kaybına da neden olmaktadır.

Bahse konu olumsuz etkilerin en aza indirilmesinde ve platformların bekasının artırılmasında askeri ve kritik sivil platformların, KÖ Füze İkaz Sistemine haiz olması önemini giderek artırmaktadır. Sonuç itibariyle sistemin veya kritik bileşenlerinin temin edilecek devletin iznine tabi olması; bu tür sistemlerin milli imkanlarla geliştirilmesi, üretilmesi ve platformlara entegre edilmesinin gerekliliğini ayrıca göstermektedir.

Askeri Stratejinin Büyük Ustası

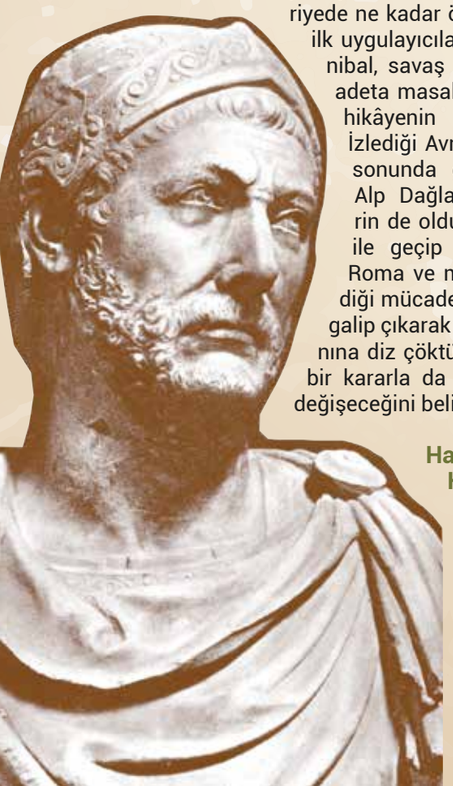
HANNİBAL BARCA

Anıtmezarı TÜBİTAK Gebze Yerleşkesi'nde bulunan Hannibal'in, tarihte gizem dolu sıra dışı bir hikâyesi var.

Bertuğ Kayhan – Uzman Yardımcısı / BİLGEM İGBY

İsimler nasıl efsaneleşir? Bu sorunun muhataplarından birisi de tarihin en ünlü komutanlarından olan Kartacalı Hannibal Barca'dır. Babasıyla birlikte daha çocuk yaşlarda savaş meydanlarında yer alan Hannibal, daha sonra Kartaca Ordusunun başına geçince tarihin en ünlü askeri hareketlerinden birine imza atmıştır. Kartaca'dan başlayıp İspanya ve İtalya topraklarında sürdürdüğü zaferler zinciri yine Kartaca'da sona ermiş ve aldığı tek bir yenilgi ülkesinin de kaderini belirlemiştir.

'Askeri stratejinin babası kimdir' sorusunun yanıtı kimilerine göre Kartacalı General Hannibal Barca'dır. M.Ö. 247-183 yılları arasında yaşayan ve dönemin emperyal gücü Roma'yı yok olmanın eşiğine kadar getiren Hannibal Barca, günümüzde askeri okullarda hala stratejileri incelenen ve analiz edilen tarihi bir şahsiyettir. Planlı bir zekânın askeriyede ne kadar önemli olduğunun ilk uygulayıcılarından olan Hannibal, savaş maceraları ile de adeta masal gibi anlatılan bir hikâyenin başkahramanıdır. İzlediği Avrupa kıyı şeridinin sonunda geçilmez denilen Alp Dağları'nı, içinde fillerin de olduğu koca bir ordu ile geçip İtalya'ya gelerek Roma ve müttefikleriyle girdiği mücadelelerin hepsinden galip çıkarak en büyük düşmanına diz çöktüren Hannibal, tek bir kararla da tarihin ne yönde değişeceğini belirlemiş bir isimdir.



Hannibal Barca Kimdir?

Hannibal, Kartaca ile Roma arasında devam eden savaşlar sırasında M.Ö. 247 yılında

doğdu. Kartaca'da o zaman Baal isminde bir bereket tanrısına inanılıyordu ve babası yeni doğan oğluna "Baal, bana karşı cömert ol" anlamına gelen "Hannibal" ismini vermişti. Hannibal'in babası Hamilcar Barca, Kartaca Ordu Komutanı olarak uzun zamandır Roma ile savaşıyordu ve bu sebeple Hamilcar'ın çocukları adeta savaş meydanlarında büyüdü.

Romalı tarihçi Valerius Maximus, Hannibal'in çocukluğu ile ilgili bir hikâye anlatır. Kartaca Ordusu Komutanı Hamilcar Barca, içlerinde Hannibal'in de bulunduğu oğullarını birbirleri ile sık sık güreştirir ve karşılarına geçerek onları izlermiş. Oğlanlar birbirine üstün geldiklerinde de "Evlatlarım, Roma'nın sonunu getirecek olan aslan parçalarıdır" diye övünürmüş. İşte Hannibal böyle bir babanın terbiyesinde, bu psikolojik ortamda büyümüştü. Hamilcar'ın Roma'ya karşı hırsı öyle büyüktü ki, küçük bir çocuk olan Hannibal'i Baal'in tapınağına götürmüş ve ellerini kan dolu bir kâseye sokarak hayatı boyunca Roma'ya düşman olacağına dair yemin ettirmişti.

Tarih Sahnesine Çıkışı

Hamilcar Barca, dağınık bir halde yaşayan vahşi Vettoni Kabilesi tarafından bir müzakere sırasında öldürüldüğünde, Hannibal 19 yaşında genç bir delikanlıydı. Babasından ayrılması erken olsa da, Hannibal ondan bir orduyu yönetmek konusunda çok şey öğrenmişti. Belki de bu sebeple, ani ölümlere karşı soğukkanlı ve hayatı boyunca da sert mizaçlı bir komutan oldu.

Babasının ölümünden sonra, ülkesinin yönetimi tarafından kendisine İspanya Ordu Komutanlığı görevi verilen Hannibal, ordusu ile birlikte Kartaca'dan İspanya üzerine yürüdü ve burada Roma ile müttefik olan yerleşimleri Kartaca'ya bağladı. Zaman içinde İspanya'daki konumunu sağlamlaştıran Hannibal, M.Ö.219 yılında Roma'nın önemli müttefiki Saguntum'u kuşattı ve sekiz ayda ele geçirdi. Saguntum Kuşatması, II.Pön Savaşı'nı başlatan hamle olarak Hannibal'in yıldızını parlatmasının yanında, tarihin önemli savaşlarından biri olarak kabul edilir. Ayrıca Hannibal artık Avrupa'daydı ve Roma'nın da savaş ilanıyla beraber hiçbir şey eskisi gibi olmayacaktı.

Efsanevi Roma Yürüyüşü

Antikçağ tarihinde net olarak yanıtlanamayan sorulardan birisi de toplumların sahaya sürdüğü savaşçılara dair sayılardır. Hannibal'in İspanya'dan çıkarak Roma üzerine yürüyüşü sırasında daha Galya'ya gelişinde ordusu %40 oranında azalmıştı. Ancak gerek Keltler'den oluşturduğu paralı askerler, gerekse müzakerelerle yanına kattığı yerel kolonilerle birlikte ordusunu güçlü tutuyordu. İstihbarat ağını etkin şekilde kullanıyor ve casusluk faaliyetleriyle topladığı önemli bilgiler sayesinde, Roma'ya karşı etkili bir algı operasyonu yürütüyordu.

Galya'dan sonra İtalya yolunda, Alplere gelmeden önce ordusunun Rhone Nehri'ni geçmesi gerekiyordu. Hannibal, ordusunu karşıya geçirmek için sert güç kullandı. Yerel kolonilerin mevcut kayıklarına el koydu ve kaynaklarıyla büyük sandallar yaptırdı. Bu sırada ordusunda 37 savaş fili olan Hannibal'in, bu hayvanları karşıya geçirmek için mühendislik harikası kayıklar yaptırdığı söylenir. Kelt kabileleri ile Roma saldırılarının üstesinden gelen Kartaca Ordusu, Rhone Nehri'ni geçmeyi başardı ve Hannibal, Roma'yı yok etmek için yanında getirdiği 30.00 asker, 15.000 süvari ve 37 filden oluşan ordusuyla Alp Dağları'nın eteklerine dayandı.

Alpleri Geçişi

Hannibal'in Roma'ya varmak için buzla kaplı Alp Dağları'nı geçmesi, tarihte pek de eşi olmayan muazzam bir olaydır. Zorlu hava şartlarına rağmen Roma'ya bu şekilde karadan ulaşmak isteyişinin sebebi, babasından edindiği tecrübe tecrübedir. Çünkü Roma denizlere hükmediyordu ve babasının komutasındaki Kartaca Ordusu, daha Roma'ya varamadan denizlerde büyük bir yenilgi almıştı.

Hannibal, Alp Dağları geçidine geldiği zaman Roma müttefiki yerel kabilelerin saldırılarına uğrasa da bunları başarıyla püskürttü. Bu arada yakınlık kurduğu kabilelerden de Alp Dağları üzerinden Roma'ya en uygun yoldan nasıl gidilebileceğini öğreniyordu.

Ordunun Alp Dağları'nda ilerledikçe karşılaştığı tek manzara soğuk hava, sarp kayalıklar ve buzullar oldu. Buzlarla kaplı dağ yollarında ilerledikçe ordunun nefesi tükeniyordu. Bindikleri hayvanları kesip yemek zorunda kalıyorlar ve günde ortalama 100 asker zatürreden ölüyordu. Günde en az 37 kilo yem yemesi gereken filler açlık ve soğuktan ölüyordu. Ölen askerler ise gömülmüyor, kendilerini takip eden dağ kurtlarına yem oluyordu. Hannibal, ordunun bu koşullara uzun süre dayanamayacağının farkındaydı. Bu yüzden orduyu dağdan en kısa sürede çıkarmak için karla kaplı zirvelere sevk etti ve dokuz günde soğuk ve fırtınadan başka hiçbir şey görülmeyen Alplerin zirvelerine ulaştı.

Zirveye ulaşan Hannibal hem ordusunu dinlendirmek, hem de geride kalan insan ve hayvanları toparlamak için dondurucu soğukta üç gün bekledi. Ordu zirveden inerken bu kez başka bir zorlukla karşılaştı. Alplerin Roma'ya giden tarafı çok dikti ve buzla kaplı yol hem kayıyor, hem de yer yer çöküyordu. Dağlara tırmanırken insan yokuşa doğru eğilir ama inerken yerçekimi düşmanınız olur. Hannibal'in yorgun askerleri de ya uçurumlardan düşüyordu, ya da küçük çaplı çığların altında kalıyordu.

Antik zamanların ünlü tarihçisi Polybios, Hannibal'in ordusundaki askerlerin Alplerden indiği zaman adeta birer hayvan gibi göründüğünü, büyük çoğunluğu ölen filleriyle beraber ordusunun yarısının da yok olduğunu söyler. Hannibal'in Alpleri geçmesi 15 gün kadar sürmüştü ama ordusu büyük bir savaş atlatmış gibi hasar almıştı. Bu noktada askerlerine şu konuşmayı yaptı: "Kuzey ve güneyden deniz sizleri kuşatıyor. Hayatınızı kurtarmanız için tek bir geminiz bile yok. Önünüzde Po Nehri, arkanızda bir daha

Hannibal Tepesi - TÜBİTAK Gebze Yerleşkesi

geçemeyeceğiniz Alp bloku duruyor. Bundan sonra ya muzaffer olacaksınız ya da öleceksiniz..."

Roma İçin Kâbus

Aşılamaz denilen Alp Dağları'nı geride bırakan Hannibal, önündeki Po Bölgesi'ni de hızlıca geçti. Bu arada Keltler ile de bir anlaşma yaptı ve 15 bin kişilik Kelt Süvarisini ordusuna kattı.

Roma, yaklaşan tehlikenin farkındaydı ve Hannibal üzerine bir ordu gönderdi. Hannibal ile Roma orduları arasındaki ilk büyük çarpışma Trebia'da yaşandı. Kartaca'nın 30 bin askerine karşılık Roma 42 bin kişilik bir güçle gelmişti. Savaş sonunda Hannibal'in 4000 ile 5000 arası kaybına karşılık, Roma 30.000 askerini kaybetmişti. Hannibal'in yenilikçi savaş taktikleri ile kazanılan Trebia Savaşı, Roma'ya indirdiği ilk büyük darbe oldu.

Trebia'dan sonra Hannibal, yerel kabilelerin desteğini de alarak ordusunu gittikçe güçlendirmeye başladı. Roma'ya ilerleyişini sürdüren Kartaca Ordusu, Apenin Dağları'nı geçmişti ki Roma Konsülü'nden Gaius Flaminus komutasında bir ordunun kendisine doğru gelmekte olduğunu öğrendi. Trasimene Gölü Bölgesi'nde Hannibal bir kışkırtma operasyonu yaptı ve 2.000 asker kaybına karşılık 15.000 Romalıyı yok etti. Hannibal'in Tresimene'de uyguladığı taktik, askeri muharebe tarihinin en geniş ve en başarılı pusularından biri olarak kabul edilir.

Roma'nın Tresimene'den hemen sonra gönderdiği bölge yöneticisi Gaius Centenius'un komutasındaki 4000 kişilik ordusu da Hannibal tarafından yok edildi.

Cannae: Roma Ordusunun Tamamen Yok Edildiği Savaş

Trebia ve Tresimene'de büyük yenilgiler alan Roma'da işler tamamiyle değişmişti. Diktatörleri devriliyor, konsülleri çekiliyordu. Savaş yanlısı olan Gaius Terentius Varro, Roma yönetimini Hannibal'e karşı zafer kazanacağına ikna etti ve Roma'nın 86.400 kişilik ordusuyla Hannibal'in üzerine yürüdü.

Hannibal, 54.000 kişilik ordusuyla 86.400 kişilik Roma Ordusu'nu Cannae'de yok etti. Sadece 5000 kayıp vermişti. 75.000 Romalı ise öldürülmüştü. Bu savaş, antik tarihin en kanlı savaşı olarak kabul edilir. Roma'nın artık bir ordusu yoktu. Kapıları ise açık bir şekilde, Hannibal'in işgalini bekliyordu.

Cannae Savaşı'nda Roma'ya karşı uygulanan strateji, günümüzde ilgili derslerde örnek olarak verilmektedir.

Roma'yı Geri Döndüren Adam: Scipio Africanus

Ancak Hannibal savunmasız Roma'yı almadı. Kartaca karşısında zayıf kalacağını düşünerek kendi haline bıraktı. Bu kararıyla ülkesinin yok olmasına zemin hazırlarken, dünya düzeninin Roma tarafından yürütülmesinin devamına sebep oldu.

Cannae'de ölümcül bir yara alan Roma, geçen zamanda boş durmadı. Romalı General Scipio, Hannibal'i yıllarca ders çalışır gibi çalıştı. Onunla ilgili her şeyi öğrendi. Küllerinden doğan Roma Ordusu ile önce İspanya'yı aldı, ardından Kartaca'nın tam kalbine saldırdı. Kartaca, Hannibal'i İtalya'dan geri çağırdı. Kendi topraklarına dönen Hannibal ilk önce bir ordu topladı. Ancak elinde büyük ölçüde tecrübesiz gençler ile eğitimsiz filler vardı. Scipio, Hannibal'in savaşmama teklifini reddetti ve Zama Bölgesi'nde Hannibal'i kendi taktikleri ile büyük bir bozguna uğrattı.

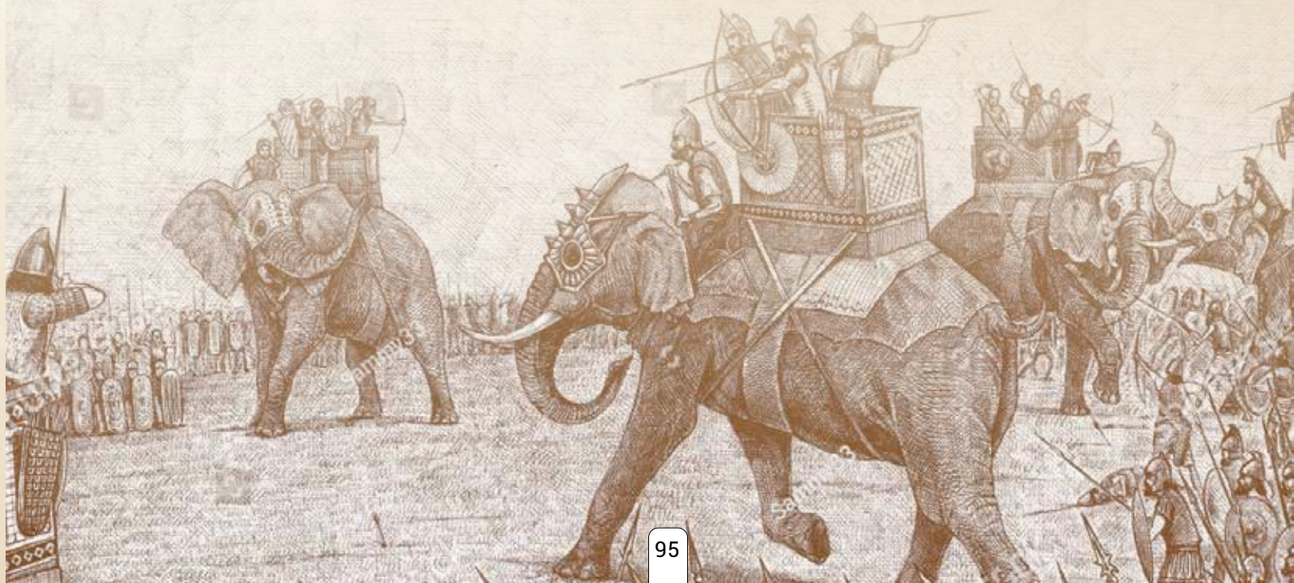
Hannibal yenilmişti. Scipio da bunun sonucunda Scipio Africanus oldu. Roma, Kartaca'yı vergiye bağladı. Ancak hayatta olan Hannibal, Roma için her zaman bir tehditti. Kartaca'dan Hannibal istendi. Hannibal ülkesinden kaçarak önce Ermenistan'ın olduğu bölgeye geldi. Sonrasında da şu anda Bursa, Kocaeli, Gebze, Körfez bölgesini kapsayan Bitinya Krallığı'na sığındı. Burada askeri danışmanlık yapan Hannibal, bir gece penceresinden kendisini almaya gelen Romalı askerleri görünce yüzüğünde sakladığı zehri içerek hayatına son verdi. Roma, Hannibal'i kendisi öldürememişti ama ondan çok şey öğrenmişti. Hannibal'den öğrendikleri ile kendisini geliştiren Roma, muazzam bir imparatorluğa dönüştü ve 3 büyük kıtada 1480 yıl boyunca varlığını sürdürdü.

Hannibal'in mezarı kesin olarak belli değildir. Ancak TÜBİTAK Gebze Yerleşkesi'nde kendisine adanmış Hannibal Tepesi'nde anıtmezarı vardır. Anıtın burada yapılmasını bizzat Gazi Mustafa Kemal Atatürk vasiyet etmiştir.


Hannibal Anıtmezarı - TÜBİTAK Gebze Yerleşkesi

Kendisi hakkında onlarca belgesel, sinema filmi ve bilgisayar oyunu yapılan Kartacalı Hannibal Barca, askeri bir deha olarak Dünya tarihinde yerini aldı. Ardında hala yaşayan ve saygı duyulan bir isim bırakarak...

KAYNAKÇA
1. Hunt, P. N. (2019). Hannibal: Roma'nın En Büyük Düşmanı. İstanbul: Kronik Kitap Yayınları.
2. Bazalgette, E. (Yönetmen). (2006). Roma'nın Korkulu Rüyası [Sinema Filmi].
3. Günday, O. Hannibal'in Anadolu'daki Faaliyetleri ve Lbyssa Üzerine Bir İnceleme. https://www.academia.edu/33110072/Hannibalin_Anadoludaki_Faaliyetleri_ve_Libyssa_Gebze_%C3%9Czerine_Bir_%C4%B0nceleme?auto=download
4. Hannibal Barca. (2012). Vikipedi, Özgür Ansiklopedi: https://tr.wikipedia.org/wiki/Hannibal
5. Scullard, H. H. Scipio Africanus. Encyclopaedia Britannica: https://www.britannica.com/biography/Scipio-Africanus



“Sanat İnsana Değer Katar Dünyayı Güzelleştirir”

Taş boyama; nesnelerin kullanımı, fikir üretme ve el becerisini geliştirme açısından oldukça değerli, sanatsal bir uğraştır.

Röportaj: Mehmet S.Ekinci – Uzman / BİLGEM KKYBY

Her sayımızda bilim ve teknolojinin yanında az da olsa sanat ve kültür alanına yer vermeye çalışıyoruz. Bunlar, aynı zamanda hayatta da insanların temel uğraş alanları… Bu sayımızda BİLGEM KKYBY'de Başuzman olarak çalışan Sayın Remzi Salihoğlu ile bir röportaj gerçekleştirdik. Remzi Hocamızın söyledikleri, hangi türü olursa olsun sanatın, insana değer ve güzellik kattığı fikrini pekiştiriyor…

Taş boyama nedir? Nasıl yapılır?

Aslında bunu taş sanatının bir parçası olarak değerlendirebiliriz. Taş sanatında iki temel uygulama söz konusudur. Birincisi, birbiriyle uyumlu farklı biçimlerdeki taşların birleştirilmesi ve çeşitli motiflerin çıkarılmasıdır. (stone art). Bununla uğraşanlar, gerek taşları bütün olarak gerekse kırık taş kullanarak farklı eserler ortaya çıkarırlar. Burada boya kullanımı söz konusu değildir.

Taş sanatının ikincisi ise taşların boyanması ile yapılır. Uygun ebatta seçilen taşların yüzeyleri temizlenerek boyanır ve çeşitli motifler çıkartılır. Bu sanatın yaygın adı ise taş boyamadır (stone painting). Taş boyamada taşlar iki şekilde değerlendirilir. İlkinde, yaklaşık 8-10 cm boyutunda tek bir taş üzerine insan veya hayvan figürleri, daha büyük boyutta yassı taşlar üzerine ise tabiat resimleri veya soyut çalışmalar uygulanır. Diğer uygulamada ise küçük boyutta taşlar (2-3 cm) boyanarak tablo üzerinde birleştirilip farklı resimler oluşturulur.

Taş boyama çalışmaları için su bazlı akrilik boya kullanımı yaygındır. Bu boyanın özelliği, çabuk kuruması ve temiz çalışma olanağı sağlamasıdır. Akrilik boyanın yanı sıra yağlı boya veya guaj boya ile yapılan çalışmalar da vardır. Boya ile birlikte fırça ve boya kalemleri kullanılır. Özellikle küçük boyuttaki taşlar üzerinde ince hatları çizmek için boya kalemleri kullanımı yaygındır. Akrilik boya ve porselen kalemler de kullanılabilir. Bu kalemlerin özelliği, hiçbir şekilde akma ve bulaşma yapmamasıdır. Asetatlı kalemler ise akma ve bulaşma nedeniyle tercih edilmemektedir.

Taş boyamada elverişli bir sonuca ulaşabilmek için son işlemler esnasında koruyucu vernik kullanılır. Bu nedenle yüzeydeki boyaların bozulmaması için, doğru malzemelerin kullanılması elzemdir. Taş yüzeyinin sert veya pürüzlü olması nedeniyle

Remzi Salihoğlu

Sanat insana değer katmakla birlikte insanın varlık olarak diğer canlılardan ayrılmasını sağlar. İnsanın dünyayı daha güzel kılmak için bunu kullanması gerekir.

kullanılacak fırçaların seçimi de önemlidir. İpek uçlu ve çeşitli kalınlıkta fırça kullanımı gerekmektedir. Boyama işlemi tamamlandıktan sonra parlak veya mat vernik ile koruma sağlanması, resimlerin hem uzun ömürlü olmasını hem de güzel bir görünüm elde edilmesini sağlayacaktır.

Taş boyama yaygın bir uğraş mıdır?

Oldukça yaygın olduğunu söyleyebiliriz. Özellikle sosyal medyanın etkili bir şekilde kullanılmasının sonucunda belirli yaş, cinsiyet ve sosyal gruplardaki insanların hobileri arasında yer aldığını gözlemliyorum. Hatta gelişmesinde sosyal medyanın önemli bir katkısı var. Yapılan çalışmaların çoğu, herkesin görmesi için kişisel hesaplar üzerinden paylaşılıyor. Bu durum sonucunda birbiriyle benzer eserler üretildiği gibi farklı eserlerin üretilmesinin de önü açılıyor.

Okullarda çocukların sanatsal etkinliklerinin de bir parçası olarak son yıllarda sıklıkla kullanıldığını görüyorum. Bazı özel okullardan eğitim talepleri geliyor. Katıldığım etkinliklerde gözlemlediğim kadarıyla taş boyamanın, yeni neslin ilgisini çeken bir sanat boyutuna ulaştığını rahatlıkla söyleyebilirim.

Tabiattaki Her Canlı Muhteşem Bir Görünüme Sahip!

Ne zamandır taş boyamayla ilgileniyorsunuz?

2016 yılı sonunda ilk taşı boyadığımı hatırlıyorum. Tamamen tesadüf eseri evde bulunan çakıl taşlarından biri üzerine bir kirpi figürü çizdim. Tabiattaki her bir canlının aslında muhteşem bir görünüme sahip olduğunu bilen biriyim, ama çizmeye çalıştığım kirpiyi daha dikkatlice inceleme fırsatı buldum. Bende hayranlık uyandırması nedeniyle başlangıç eserimi, aynı zamanda logom olarak seçtim. Sosyal medyada yayınladığım çalışmalarda da kirpi logosu yer alıyor.

İlk çizimden sonra taş boyamayı hiç bırakmadım. Geçen yıllar içerisinde binin üzerinde tablo, bunun üçte biri kadar tek taş ve kütük üzerinde çalışma gerçekleştirdim. Zaman içerisinde malzeme kullanımı konusunda, gerek deneme yanılma gerekse araştırarak tecrübe kazandım. Özgün figürler ortaya çıkarmaya da çalıştım. Bazı çalışmalarım, dünyanın farklı yerlerinde farklı kişiler tarafından yeniden üretildi. İlk tasarlayan olarak bundan büyük mutluluk duyduğumu belirtebilirim.

Bu uğraşı size neler katıyor?
Asıl mesleğim kütüphaneciliktir. Şu anda ise farklı bir alanda çalışıyorum. İnsanın yaptığı her iş, kendisine farklı bir değer katar inancındayım. Sanat ise bambaşka bir değer. Bence sanat, insana değer katmakla birlikte insanın varlık olarak diğer canlılardan ayrılmasını sağlar. İnsanın dünyayı daha güzel kılmak için bunu kullanması gerekir. Sanatla uğraşanlar genellikle bu amaca doğrudan veya dolaylı olarak katkı sunuyorlar. Benim uğraşım, bütünüyle amatör olarak bu konunun bir parçası olmaktan ibaret.

Genel olarak resim çizmenin kişilere rahatlama hissi verdiğini ve iyi vakit geçirmesini sağladığını duyuyordum. Ama hiç deneme fırsatı veya ihtiyacı duymamıştım. Taş boyamaya başladığım ilk günlerden itibaren, duygu durumumda gerçek anlamda bir değişim hissetmeye başladım. Adını daha önce hiç duymadığım renklerin (fuşya, oxford yeşili, magenta) aslında insan ruhuna etki eden semboller içerdiğini öğrenmiş oldum. En az bir kötü alışkanlığım (sigara) sona erdi. Çünkü bağımlılık, gerçekte ruhsal bir yönelim ile şekilleniyor ve zaman harcarken sizi mutlu kılan bir uğraşınız varsa bu tür eğilimlerden uzaklaşabiliyorsunuz. En büyük kazanımım ise sabır oldu. Bir tablo ile saatlerce uğraşmak sabır gerektiriyor. Ben bu uğraşının her anından zevk almayı öğrendim sanıyorum.

Taş boyamaya başladığım ilk zamanlar yaptığım çalışmaları evde biriktiriyordum. Zamanla tamamladığım her tabloyu instagram hesabımdan paylaşmaya başladım. Bu, eserlerin bilinirliğini artırdı ve çeşitli tasarım fuarları, kermesler, okul ve belediye faaliyetlerine davetler almaya başladım. Bu süre içerisinde farklı kesimlerle ilişkilerim gelişti. Benzer çalışmalar yapan kişilerle tanışarak fikirlerimizi paylaştık.

Evde ürettiğim eserlerin sayısı arttıkça alıcılar da çıkmaya başladı. Böylece hobi olarak başladığım çalışma, aynı zamanda ekonomik bir anlam da kazanmış oldu. Buradan gelen gelirlerin bir kısmıyla, örneğin salgın sürecinde işsiz kalan ihtiyaç sahiplerine yardım faaliyetleri yürütebildik. Diğer tasarımcı arkadaşlarımızla gruplar oluşturarak kendi aramızda bir dayanışma planı yaptık. İnsanların zor zamanlarında yanlarında olabilmenin verdiği manevi hazzı bu sanat sayesinde tattım.

Bugün için basit veya zor en az bir hobi edinmenin, sanatın herhangi bir alanıyla ilgilenmenin her yaş grubu için çok gerekli olduğuna inanıyorum. Çocuklara mutlaka kazandırılması gereken bir özellik olduğunu düşünüyorum. Sanatın her türünün, hem bireysel gelişimi destekleyen hem de çocuğun ileriki yaşamında bağımsız bir birey olarak ayakta kalmasını sağlayabilecek önemli araçlardan biri olduğu fikrindeyim. Taş boyama ise nesnelerin kullanımı, fikir üretme ve el becerisini geliştirme açısından oldukça değerli sanatsal bir uğraş.

Bir eser için gerekli malzemeler nelerdir?
Nasıl bir eser çıkarmanız gerektiğiyle bağlantılı olarak açıklamaya çalışacağım. Örneğin 13*18 cm'lik fotoğraf çerçevesi boyutunda bir eser planlıyorsanız ve bunlardan yaklaşık 100 adet yapacaksanız, ihtiyacınız olan malzemeler ve yaklaşık fiyatları şunlardır:

Boyalar: Farklı renkler seçilebilir. 250 ml fiyatı yaklaşık 7-8 TL/adet. 8-10 adet renk boya yeterlidir.

Kalemler: Akrilik boya kalemleri (0,7 mm uçlu, 15 TL/adet), porselen kalemleri (sıcak, soğuk ve standart renkler, 35-45 TL/paket-altılı)

Çerçeve: 13*18 cm MDF, 25 tl/adet

Taşlar: Nehir veya deniz taşları. Taş yüzeyleri öncelikle beyaza boyanmalıdır.

Koruyucular: Şeffaf parlak vernik, 15-25 TL/adet.

Fırçalar: Piyasada bulunan taş boyamaya elverişli çeşitli numaralarda fırçalar kullanılabilir. Fiyatlar değişkendir.

İsimsiz Sınav Kağıdı*

Yeterince
Çalışmıyorum, çalışmıyorsun, çalışmıyor
Ve
Çalışmıyoruz, çalışmıyorsunuz, çalışmıyorlar
Gel problemi itiraf et de
Başlayabilelim onu çözmeye
Bak daha sınav kağıdına ismimizi yazamadık
Çevredekiler yarılarken çözümleri azimle ...

Yaş Söğüte Öğüt*

Genç kardeşim bir öğüt sana
Düşündüklerini uygula
Uyguladıklarını düşün mutlaka

Bu sayede ilerleyebilirsin ancak hayatta
Uyguladıklarını düşünmezsen tanışırsın yanlışlarla
Ve düşündüklerini uygulamazsan kıvranırsın pişmanlıklarla!

Dr. Umut Uludağ – Başuzman Araştırmacı / BİLGEM UEKAE

*Şiir, Umut Uludağ'ın Kayıp Hattat 26 adlı şiir kitapçığında yer almaktadır.

TÜBİTAK
BİLGEM

Milli Bulut Depolama Çözümü

SAFİR DEPO

TÜBİTAK BİLGEM Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı tarafından geliştirilen Safir Depo, bir milli bulut nesne depolama uygulamasıdır. Safir Depo üzerinde depolanan nesnelere internet üzerinden; akıllı telefonlar, tabletler veya bilgisayarlar aracılığıyla her an her yerden ulaşılabilmektedir.

Safir Depo'ya yüklenen doküman, ses, fotoğraf, video gibi her tür dosya üzerinde klasörleme, taşıma, yeniden adlandırma gibi dosya işlemleri gerçekleştirilebilmesinin yanı sıra; ofis dokümanlarında çevrimiçi görüntüleme, düzenleme ve versiyonlama yapılabilmekte, paylaşım özelliği sayesinde Safir Depo'da bulunan dosya / klasörler, istenilen herkes ile kolayca paylaşılabilmektedir.

Safir Depo Beta sürümü, 2017 Ağustos ayından bu yana internete açık canlı ortamda hizmet vermektedir.

https://safirdepo.b3lab.org
www.bilgem.tubitak.gov.tr