BİLGİ GÜVENLİĞİ ALTYAPISI TEDARİKİ REHBERİ

1. KAPSAM VE AMAÇ

1.1. Bilgi Güvenliği Altyapısı Tedariki nedir?

Güvenlik duvarı, e-posta güvenlik, ağ erişimi kontrolü (NAC), saldırı önleme sistemi (Network IPS), uygulama güvenliği ve yük dengeleme (WAF), web güvenliği - vekil sunucu, VPN cihazı, veri sızıntısı önleme sistemi (DLP), içerik filtreleme sistemi, saldırı tespit sistemi (IDS) vb. bilgi güvenliği altyapısına ilişkin donanımların tedarikini kapsamaktadır.

1.2. İhtiyaç analizi çalışması yapıldı mı?

İhtiyaç analizi, kurumun ihtiyaç duyduğu güvenlik donanım ürünlerinin/çözümlerinin tam ve doğru olarak belirlenmesini sağlar. İhtiyaç analizi yapılırken aşağıda belirtilen adımlar göz önünde bulundurulmalıdır:

- Sahip olunan güvenlik donanımı envanterlerinin listesinin çıkartılması
- Mevcut güvenlik donanım sistemlerinde geriye dönük problem kayıtlarının incelenmesi, kullanıcı şikâyetlerinin ve beklentilerinin dikkate alınması
- Oluşturulan güvenlik donanım envanterinde bulunan güvenlik donanımlarının bu ihtiyaç kapsamında kullanıp kullanılmayacağının değerlendirilmesi
- Varsa diğer lokasyonlardaki ihtiyaçlarının göz önünde bulundurulması
- Gelecek 5 yıl içerisindeki büyüme planları dikkate alınarak kapasite planlamasının yapılması
- Çözüm bileşenlerinde yedeklilik ihtiyacının olup olmayacağının değerlendirilmesi

İhtiyaç duyulan doğru güvenlik donanımını, doğru ölçekte ve doğru lisanslama ile konumlandırabilmek için aşağıdaki hususların dikkate alınması önemlidir.

1.2.1. Güvenlik duvarı donanımı

Güvenlik duvarı (Firewall), farklı ağlar üzerinde hizmet veren kaynakları diğer ağlardan gelecek izinsiz erişimlere karşı koruyup, farklı ağlar arası trafiği önceden belirlenmiş kurallara göre denetleyen ürünlerdir. Güvenlik duvarının asıl görevi ağ üzerinde kendisine gelen paketlerin gitmeleri gereken hedef sunucu ve servislere (önceden belirlenmiş kurallara göre) gidip gidemeyeceğine karar vermektir. Güvenlik duvarı teknolojinin gelişmesine paralel olarak ana fonksiyonu dışında IPS, URL filtreleme, uygulama güvenliği, e-posta güvenliği, SSL VPN (uzak erişim), veri güvenliği gibi ek güvenlik yeteneklerine sahiptir. Ek güvenlik özellikleri ürün lisanslamasında ve ürünün çalışacağı donanımı ölçeklendirmesinde de önemli bir rol oynar.

Kurumun ihtiyaçlarına uygun güvenlik duvarı seçimi için aşağıdaki maddeler göz önüne alınmalıdır;

- Kaç adet ağ segmenti oluşturulması gerektiği tespit edilerek, güvenlik duvarı üzerinde ihtiyaç duyulan i nterface sayısı ve tipi belirlenmeli,
- Güvenlik duvarı üzerinde DMZ ağ segmenti olacak mı belirlenmeli,
- İlerde ihtiyaç duyulabilecek ağ arabirimlerinin planlaması yapılarak alınacak donanımda ilerde kullanılmak üzere boş interface modül ihtiyacı belirlenmeli,
- Güvenlik duvarı donanımı üzerinde yoğun işlem ihtiyacı duyan servisler için (VPN gibi) özel üretilmiş donanım parçalarına ihtiyaç olup olmayacağına karar verilmelidir,
- Güvenlik duvarının konumlandırılacağı noktadaki yedek donanım ihtiyacı değerlendirilmeli,
- Hangi ek güvenlik özelliklerine (IPS, URL filtering, Application Control vb.) ihtiyaç olduğuna karar verilmeli,
- Dış kurumlarla veri transferi için özel güvenli iletişim kanalı (IPSec VPN/site-to-site VPN) ihtiyacı ve bağlantı kurulacak kurum sayısı belirlenmeli,
- Kurum içinde kaç adet kullanıcı olduğu belirlenmeli,
- Güvenlik duvarı donanımın kurulacağı lokasyon (yerleşim yeri, bölüm, başkanlık vb.) sayısı belirlenmeli,
- Güvenlik duvarı merkezi yönetim yazılımı ihtiyacı değerlendirilmeli (Her bir güvenlik duvarının ayrı ayrı yönetilmesi yerine merkezi olarak yönetilmesi operasyonel kolaylık sağlar. Bazı güvenlik duvarları merkezi yönetim özelliği sunarken bazıları sadece kurulu olduğu güvenlik duvarı yazılımını yönetebilmektedir.)
- Güvenlik duvarı üzerinden geçen trafiğin log kayıtlarının nerede ve ne kadar süre ile tutulacağı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim ara yüzü ihtiyacı belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli

1.2.2. E-posta güvenlik donanımı

E-posta güvenlik donanımları, dış dünyadan kurum e-posta adreslerine gelen ve kurum e-posta adreslerinden dış dünyaya giden elektronik postaların kontrol edilip varsa zararlı yazılımlardan arındırılmasını sağlar. E-posta güvenlik donanımlarının ana fonksiyonu gelen ve giden elektronik postaları virüs ve spam kontrolünden geçirmektir. Gelişen güvenlik ihtiyaçları ile birlikte e-posta güvenlik sistemleri şifreli e-posta iletimi, kötü amaçlı yazılım (malware) analizi, veri sızıntısı kontrolü gibi ek güvenlik modülleri içermektedir.

E-posta güvenlik donanımı ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- Koruma yapılacak e-posta adresi sayısı,
- Antivirüs ve antispam kontrolü ile birlikte veri sızıntısı önleme, e-posta şifreleme ve malware önleme çözümlerinden hangilerine ihtiyaç olduğu belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,
- Yedekli yapı ihtiyacı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim ara yüzü ihtiyacı belirlenmeli,

1.2.3. Ağ erişim kontrolü (NAC) donanımı

Ağ erişim kontrolü sistemleri, son kullanıcı cihazlarının (PC, notebook, tablet, akıllı telefon vb.) kontrollü ve güvenli bir şekilde kurum ağına dahil olmasını ve belirlenen politikalara göre ağ kaynaklarına erişimini kontrol eder. NAC çözümü ile yetkisiz kullanıcıların, yetkilendirilmiş olsa bile önceden belirlenmiş güvenlik isterlerini (İşletim sistemi versiyonu, service pack seviyesi, antivirüs yazılımı varlığı vb.) karşılayıp

karşılamadığını kontrol ederek ağa dâhil eder. NAC çözümleri ajanlı ve ajansız olarak 2'ye ayrılır. Ajanlı çözüm daha derinlemesine bir güvenlik kontrolü yapılmasını sağlar. Ağ erişim kontrolü yazılımı ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- Kullanıcı sayısı belirlenmeli,
- Ağa dahil olacak kullanıcı cihazları (PC, notebook, tablet, akıllı telefon vb) ve sayısı belirlenmeli,
- Kablosuz ağ ile entegrasyon desteği dikkate alınmalı,
- Kullanıcı cihazları işletim sistemleri ve versiyonları belirlenmeli,
- Kurum ağında kullanılan ağ anahtarlarının (switch) marka ve modelleri belirlenmeli,
- Hub kullanılıp kullanılmadığı belirlenmeli,
- Çözümün ajanlı olup olmayacağı belirlenmeli,
- Kimlik doğrulamasından geçen kullanıcılarda ne gibi kontrollerin (İşletim sistemi versiyonu, service pack seviyesi, antivirüs yazılımı varlığı vb.) yapılacağı belirlenmeli,
- Kimlik doğrulamasından geçemeyen kullanıcıların izole bir ağa alınıp alınmayacağı belirlenmeli,
- Misafir kullanıcılar, bilinmeyen cihazlar, VOIP cihazları için ne tür politikaların uygulanacağı belirlenmeli,
- Çözümün kurum ağında çalışan diğer ağ cihazlarıyla uyumlu çalışıp çalışmadığı test edilmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,
- Yedekli yapı ihtiyacı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim ara yüzü ihtiyacı belirlenmeli,

1.2.4. Saldırı önleme sistemi (Network IPS) donanımı

Saldırı önleme sistemlerinin temel amacı ağa yapılan saldırıları veri tabanında bulunan imzalar yardımı ile önceden belirlenmiş güvenlik politikalarına bağlı olarak engellemektir. Saldırının tespit edilmesi, kayıt altına alınması ve sistem yöneticisine gerekli uyarılarda bulunulması saldırıya karşı zamanında gerekli önlemlerin alınmasını sağlar.

Saldırı önleme sistemi kullanım ihtiyacına göre ağda konumlandırılmalıdırlar. Yönlendirici (Router) ile güvenlik duvarı arasına konumlandırılacak bir saldırı önleme sistemi güvenlik duvarının maruz kaldığı ve engelleyebildiği saldırıları da (saldırıların veri tabanında var olduğu varsayılmıştır) engelleyecektir. Bu noktada saldırı önleme sistemi ve güvenlik duvarı performansı karşılaştırılmalıdır. Aynı saldırıyı her iki cihazda engelleyebiliyorsa ve ağın performansı iyileştirilmek amacıyla hızlı çalışan cihaz daha dışa konumlandırılabilir. Donanım tabanlı saldırı önleme sistemi ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır:

- Kaç adet ağ segmenti oluşturulması gerektiği tespit edilerek, cihaz üzerinde ihtiyaç duyulan interface sayısı ve tipi belirlenmeli,
- Bypass özelliğine (IPS de sorun yaşandığında trafik akmaya devam etmesi) ihtiyaç olup olmadığı belirlenmeli. Bypass özelliği gerekiyorsa bunun cihaz içinde mi yoksa harici bypass ünitesiyle mi yapılacağı belirlenmeli,

- SSL decryption ihtiyacı belirlenmeli,
- Manuel imza yazılması ihtiyacı belirlenmeli,
- Ses trafiğinin incelenip incelenmeyeceği belirlenmeli,
- Davranışsal analiz ihtiyacı belirlenmeli,
- DDos özelliğinin istenip istenmediği belirlenmelidir,
- Yedekli yapı ihtiyacı belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim ara yüzü ihtiyacı belirlenmeli,

1.2.5. Uygulama güvenliği ve yük dengeleme (WAF) donanımı

Yük dengeleme sistemleri, kullanıcılardan gelen trafiği aynı hizmeti veren birden fazla sunucu arasında akıllı yük paylaşım algoritmalarına göre dağıtan bir teknolojidir. Bu teknolojiyi kullanarak en iyi kaynak kullanımı, en yüksek işlem hacmi, en düşük cevap süresi sağlanabilir; sunuculara yapılan bağlantılar optimize edilerek oluşabilecek aşırı yük (overload) engellenebilir. Bazı çözümlerde, uygulama güvenliği ve yük dengeleme özellikleri birlikte bulunabilir. Bu durumda, uygulama güvenliği çözümünü kullanmak için ek bir lisans alımı ihtiyacı doğar. Kurum ihtiyaçlarına uygun bir uygulama güvenliği ve yük dengeleme donanımı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- SSL sonlandırma kullanılıp kullanılmayacağı belirlenmeli,
- Web uygulamalar üzerinde sıkıştırma yapılıp yapılmayacağı belirlenmeli,
- Hangi servisler için yük dengelemesi yapılacağı belirlenmeli,
- Hangi sistem ve servisler için uygulama güvenliği istendiği belirlenmeli,
- Yük dengelemesi yapılacak sunucular üzerindeki toplam bağlantı sayısı belirlenmeli,
- Hangi kurumsal uygulamalar için uygulama güvenliği kullanılacak belirlenmeli,
- Donanımın ağ içinde nasıl konumlandırılacağı belirlenerek üzerinde bulunması gereken interface özellikleri ve sayıları belirlenmeli,
- Uygulama güvenliğinde "öğrenme" özelliği istenip istenmediği belirlenmeli,
- Uygulama güvenliğinde uygulanacak güvenlik modeli belirlenmeli (pozitif güvenlik modelinde izin verilenler dışında her şey engellenirken, negatif güvenlik modelinde yasaklananlar dışında her şeye izin verilir),
- Yedekli yapı ihtiyacı belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim ara yüzü ihtiyacı belirlenmeli,

1.2.6. Web güvenliği – Vekil sunucu

Web güvenliği sistemleri URL filtreleme ve içerik filtreleme olarak iki kısma ayrılır. URL filtreleme çözümünde tüm internet siteleri farklı kategorilere dahil edilir ve kullanıcının eriştiği internet siteleri yasaklı bir kategori

içinde ise erişim engellenir. İçerik filtreleme çözümlerinde ise URL filtrelemeye ek olarak internet üzerinden indirilen veri analiz edilir ve zararlı içerikler tespit edilip engellenir. Web güvenliği çözümü ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- Web güvenliği sistemleri kurum ağına aşağıdaki yöntemlerden hangisi ile uygulanacağı belirlenmeli,
  - Yönlendirme mod: Kullanıcı gateway'leri üzerinde http/https trafiği web güvenliği sistemine yönlendirilir
  - Inline Mod: Web güvenliği sistemleri çalıştığı donanım ağa tüm trafik üzerinden geçecek şekilde (inline) olarak dahil edilir.
  - Proxy (Vekil sunucu) mod: Web güvenliği sistemi ağ içinde herhangi bir yerde olabilir. Son kullanıcı web tarayıcılarına vekil sunucu olarak web güvenliği sistemi adresi girilir.
- Https trafiğinin incelenip incelenmeyeceği belirlenmeli,
- Kullanıcı sayısı belirlenmeli,
- Ürün sadece URL filtreleme yanında içerik kontrolü de yapacak mı belirlenmeli,
- Sıkıştırılmış dosyaların incelenip incelenmeyeceği belirlenmeli,
- Ürünün ana fonksiyonu dışında malware analizi, veri sızıntısı kontrolü, e-posta güvenliği yapıp yapmayacağı belirlenmeli,
- İhtiyaç duyulan internet bant genişliği belirlenmeli,
- Internet erişimlerini önbellekleyecek mi (cache) belirlenmeli,
- Kullanıcı makinalarında kullanılan işletim sistemleri ve tarayıcı tipleri belirlenmeli,
- Yedekli yapı ihtiyacı belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,
- Power supply yedeklilik ihtiyacı belirlenmeli,
- Out of band yönetim arayüzü ihtiyacı belirlenmeli,

2. YAPILACAK İŞİN TANIMI

2.1. Mevcut güvenlik sistemlerine ilave bir alım mı yoksa yeni bir alım mı planlandı?

Mevcut sistemde kullanılmakta olan güvenlik donanım ve lisansları; yeni sistemde de kullanılmaya devam edilebilir. Mevcut güvenlik sistemleri, yeni güvenlik donanımlarıyla ile beraber kullanılmaya devam edilecekse sistemlerin uyumluluğu kontrol edilmelidir. Örneğin; yeni güvenlik donanımlarının, network ve log yönetim sistemleriyle entegrasyonu isteniyorsa, mevcut sistemlerin kapasite, lisans ve destek açısından değerlendirilerek bu donanımlara ek güvenlik özellikleri, versiyon yükseltme ve lisans artırımı gibi ihtiyaçlar belirlenmelidir.

İlave bir güvenlik donanımı alımı yapılacaksa, mevcut güvenlik sistemlerinin üretici tarafından desteklenen güncel bir ürün olup olmadığı kontrol edilmelidir. Mevcut güvenlik sistemlerinin operasyonel sürekliliği için, alınacak olan bakım ve destek hizmeti (End of Life ve End of Support) gibi konular hesaba katıldığında mevcut ürünlerin bakım maliyeti, ürünleri yenileme maliyetine yaklaşabilir. Bu gibi durumlarda mevcut

sistemle devam edilip edilmeyeceği ya da yenilenmesi kararı alınmadan önce maliyet fayda analizi çalışmaları yapılmalıdır.

Diğer taraftan alımı planlanan güvenlik donanımlarının versiyonları ile mevcut güvenlik sistemleri versiyonları arasındaki farklılıklar dikkate alınmalıdır. Mevcut ve yeni sistemin yazılım versiyonları ve desteklediği protokollerin uyumluluğunun değerlendirilmesi kurulum sonrasında operasyonel verimliliği artıracaktır.

2.2. Ürün ana fonksiyonu dışında farklı ek özelliklerde içerecek mi?

Bu kapsamdaki teknolojik ürünler ana fonksiyonlarına ek olarak farklı fonksiyon ve özelliklerde içerebilir. Örneğin; alımı yapılacak içerik filtreleme çözümü ek lisanslar ile e-posta güvenliği ve malware analizi gibi farklı fonksiyonları yerine getirebilecek yetenekler kazanabilir. Şayet şuanda düşünülmese bile ilerde malware analizi yatırımı yapılacaksa seçilecek içerik filtreleme çözümünün bu özelliğinin olup olmadığına bakılmalıdır. Böylelikle ilerde mevcut üründe bir lisans artırımı ile malware analizi çözümü rahatlıkla devreye alınıp entegrasyonu sağlanır. Yeni bir güvenlik donanımı almadan ihtiyacın mevcut güvenlik donanımlarına ek özellik alımıyla karşılanabiliyor olması, güvenlik donanımı konfigürasyonlarının kolaylıkla yapılmasını, hem de ek yatırım maliyeti oluşmamasını sağlayacaktır.

Seçilecek çözümlerin özellikle kurumların az kullanıcı lokasyonları için (taşra, il müdürlüğü vb.) güvenlik donanımlarının ana fonksiyonları ile beraber ek özellikler (IPS, URL filtering vb.) içermesi hem yönetim kolaylığı hem de maliyet avantajı sağlamaktadır.

Kurumların çok kullanıcılı lokasyonlarında sadece ihtiyaç duyulan güvenlik fonksiyonu için üretilen donanımların kullanılması önerilmektedir. Örneğin; kritik öneme sahip yerlerde URL filtering çözümü ile güvenlik duvarı çözümünün aynı sistem üzerinde olması performans ve iş süreklilik açısından önerilmemektedir.

2.3. Güvenlik donanımını çalışacağı altyapı mevcut bilgi sistemleri altyapısıyla karşılanabilir mi?

Alımı yapılacak güvenlik donanımının fonksiyonlarını yerine getirebilmesi için ek bir ürüne ihtiyaç olup olmadığı değerlendirilmelidir. Örneğin; kurulacak güvenlik donanımı belli büyüklüğe kadar olan kurulumlarda ürüne dâhil olarak gelen bir veri tabanı kullanırken, belirli büyüklüğü geçen kurulumlarda daha büyük ve harici bir veri tabanı ihtiyacı duyabilir. Bu durumda sunucu, veri tabanı yazılımı, işletim sistemi lisansı vb. ek maliyetlerde hesaba katılmalıdır. Alımı yapılacak güvenlik donanımın bu ihtiyaçları önceden belirlenmeli ve bu ihtiyaçların kurumun mevcut bilgi sistemleri kaynaklarıyla sağlanıp sağlanmayacağı araştırılmalıdır. Ayrıca, güvenlik donanımının kurulacağı sistem odasının altyapısı ve fiziki koşullarının yeterli olup olmadığı göz önünde bulundurulmalıdır. Örneğin; sistem ya da sistemlerin çalışacağı ortamın enerji altyapısının (UPS, Jeneratör), ısı, nem, topraklama, havalandırma vb. altyapılarının yeterliliği önceden değerlendirilmelidir.

Bunlara ilave olarak, güvenlik donanımlarının yerleştirileceği kabinlerde yeterli yer olup olmadığı, veri ve enerji kablolaması ihtiyacının olup olmadığı belirlenmelidir. Kabinlerde yer olmaması durumunda ek kabin ihtiyacı hesaba katılmalıdır.

2.4. Güvenlik sisteminin yönetim ara yüzü özellikleri değerlendirildi mi?

Güçlü, kolay ve görsel bir yönetim ilgili güvenlik donanımının en etkin biçimde kullanılmasını sağlar. Bütün güvenlik sistemleri bir kullanıcı arabirimi üzerinden yönetilir. Bazı güvenlik sistemleri web ara yüzünden yönetim imkânı tanırken bazıları da kurulacak bir yazılım üzerinden yönetim imkânı sunar. Her iki yönetim şeklinin de avantaj ve dezavantajları bulunur. Web ara yüzünden yönetilen yazılımlara ağ erişiminin olduğu her noktadan ve her platformdan erişim sağlanırken, sadece işletim sistemine yüklenen bir program ile yönetilen sistemlere programın kurulduğu ve kurulabildiği makinalardan (kurulum Windows desteği sunarken Linux desteği sunmayabilir) erişim sağlanabilir. Güvenlik sistemleri kendi üzerinde yönetim modülü olabildiği gibi ayrı bir yönetim modülü ile de yönetim imkânı sunabilir. Böylece dağıtık olarak çalışan birden fazla aynı tür güvenlik sistemi ayrı ayrı yönetilmektense bir yönetim modülü ile merkezi olarak yönetilebilir. Bu nedenle güvenlik sisteminin nasıl bir yönetim özellikleri sahip olması gerektiği belirlenmelidir.

2.5. Donanımın ihtiyaç duyulan raporlama yetenekleri belirlendi mi?

Seçilecek güvenlik donanımın raporlama yeteneği işlenen verinin en iyi şekilde gözlemlenmesini ve gerekli aksiyonların zamanında alınarak güvenlik ihlallerinin önüne geçilmesine yardımcı olur. Örneğin; otomatik raporlama özelliği ile günlük, haftalık, aylık otomatik olarak oluşturulan ve belirli kişilere e-posta ile gönderilen raporlar incelenerek farklılıklar değerlendirilebilir. Bu nedenle seçilecek güvenlik donanımının raporlama yeteneğinin ihtiyaca yönelik olarak belirlenmesi gerekir. Aşağıdaki gibi örnek raporlama isterleri belirtilebilir;

- Güvenlik donanımı sistem istatistiklerinin raporlanması,
- Güvenlik donanımı üzerindeki aktivitelerin (bloklama, tarafa, trafik) raporlanması,
- Rapor çıktı formatlarının (pdf, html, txt vb.) belirtilmesi,
- Oluşturulan raporların otomatik olarak birden fazla mail adresine belirtilen zamanlarda gönderebilmesi (günlük, aylık, haftalık)
- Standart rapor şablonlarının bulunması,
- Kullanıcıya farklı raporlar oluşturmaya izin verebilmesi,
- Geçmişe dönük raporlar alabilmesi,
- Kullanıcı kullanımına yönelik raporlar verebilmesi,
- Raporlar oluşturulurken filtreler kullanılabilmesi (rapor icmp trafiği içermesin gibi),

2.6. Güvenlik sisteminden log alınması planlanıyor mu?

Güvenlik donanımlarının ana fonksiyonu (firewall, antivirüs vb.) ile birlikte üzerinde çalıştığı sistem ile ilgili (CPU, memory, çalışan servisler) loglar da üretir. Bu loglar güvenlik donanımının kendi üzerinde veya harici bir sistemde tutulur. Loglar harici bir sistemde tutulacaksa toplanacak log ebatı tahmini yapılarak disk alanı

ihtiyacı olup olmadığı değerlendirilmelidir. Disk alanı ihtiyacı varsa maliyete dâhil edilmelidir. Ayrıca üretilen loglar için 5651 sayılı yasaya uyum gereksinimi varsa bu husus planlama safhasında değerlendirilmelidir.

2.7. Güvenlik sistemlerinden beklenen alarm isterleri belirlendi mi?

Birçok güvenlik donanımı, üzerinde oluşan bir problem anında veya ana fonksiyonu gereği bir güvenlik ihlali oluşması durumunda alarm üretme kabiliyetlerine sahiptir. Örneğin; güvenlik donanımının bir fonksiyon devre dışı kaldığında, disk belli bir yüzde oranında dolduğunda veya bu güvenlik donanımı bir e-posta güvenlik donanımı ise virüs içeren bir mail geldiğinde alarm üretmesi sağlanabilir. Bu alarm şekli e-posta gönderme, SMS gönderme veya önceden tanımlı bir script çalıştırma olabilir. Böylece olası sorunlarda etkin bir şekilde müdahale söz konusu olur. Bu nedenle ilgili güvenlik donanımından beklenen alarm üretme ihtiyaçları belirlenmelidir.

2.8. Güncelleme, destek ve bakım süreleri belirlendi mi?

Tehditlerin çok hızlı bir şekilde yayıldığı her geçen gün farklı ve yeni tehditlerin ortaya çıktığı günümüzde tercih edilecek güvenlik donanımdan beklenen güncelleme hakları ve sürelerinin belirlenmesi gerekir. Özellikle içerik kontrolü yapılan güvenlik donanımlarında (Anti virüs, web filtreleme, e-posta güvenliği vb.) güncellemelerin sıkça yapılıyor olması ve güncel tehditleri içeriyor olması gerekir. Lisans süresi boyunca sürüm ve veri tabanı güncellemelerinin ücretsiz yapılıyor olması önemlidir. Bir diğer kritik nokta lisans süreleri bitiminde güvenlik donanımının nasıl davranacağı belirlenmelidir. Bazı ürünler lisans bitiminde otomatik olarak devre dışı kalırlar. Mümkün olduğunca lisans bitimlerinde devre dışı kalmayan, var olan sürüm ve veri tabanı ile çalışmaya devam edecek ürünler tercih edilmelidir. Bu konunun önceden değerlendirilip, üreticiyle yapılacak anlaşma kapsamının ileride doğabilecek ihtiyaçlara göre gözden geçirilmesi gerekmektedir.

Güvenlik donanımlarının periyodik bakım, onarım ve garanti hizmetlerinin tedarikten önce planlanması önemlidir. Bu planlama yapılırken garanti süresi, parça değişim süresi ve koşulları, garanti süresinden sonraki yedek parça taahhüttü ve tedarik süresi gibi kriterler göz önünde bulundurulmalıdır. Güvenlik donanım ihtiyacı yabancı üreticilerden karşılanıyorsa ilgili üreticinin büyük yerleşim yerlerinde yedek ürün bulundurması önemlidir. Her ne kadar üretici ile yapılan bakım sözleşmelerinde arızalı donanım aynı gün içinde gönderilmiş olsa bile ürünün gümrük işlemlerinde dolayı alınması en az bir haftayı bulmaktadır.

2.9. Bu ürünlerin konumlandırılacağı sistemlerle ilgili hizmet seviye gereksinimleri değerlendirildi mi?

Temin edilecek güvenlik donanımı kritik önemdeki hizmetlere altyapı sağlayacaksa, hizmet sürekliliğinin değerlendirilmesi amacıyla yedekliliğinin göz önünde bulundurulması ve yatırımın bu doğrultuda planlanması gerekir. Örneğin; güvenlik duvarı kurumun ağ mimarisinde çok kritik noktada yer alacağı için bu üründe oluşabilecek bir sorun nedeniyle devre dışı kalması tüm kurumun kullanıcılara verdiği ve kurum kullanıcılarının aldığı hizmetlerin durmasına sebebiyet verecektir. Bu nedenle yüksek öneme sahip güvenlik sistemi ürünlerinin yedekli olarak planlanması önemlidir.

2.10. Yedekli güç kaynağı ihtiyacı belirlendi mi?

Güvenlik donanımlarının birçoğu özel üretilmiş donanımlar olduğu için donanım üzerindeki tüm bileşenler özeldir ve başka yerden temin edilmesi çok zordur. Bu bileşenlerden en önemlisi de cihaz üzerindeki güç kaynağıdır. Güvenlik donanımlarının birçoğunda yedek güç kaynağı opsiyonel olarak sunulmaktadır. Bu nedenle güvenlik donanımda yedek güç kaynağı desteği ve ihtiyacı belirlenmelidir.

2.11. Out of band yönetim ihtiyacı belirlendi mi?

Günümüzde birçok ağ ve güvenlik cihazları ve sunucularda cihazın donanımının yönetimini sağlayan bir ağ arabirimi vardır. Bu ara birim (interface), sunucunun bulunduğu ağdan bağımsız başka bir ağ üzerinden donanıma erişilebilecek şekilde konfigüre edilir. Bu yolla sistemi uzaktan kapatmak, açmak, bios'a girmek, donanım üzerine işletim sistemi kurmak gibi işlevler yerine getirilir. Kurum içinde bulunan donanımlar out of band ile yönetiliyor veya yönetilmesi planlanıyorsa alınacak donanımda out of band ihtiyacı belirlenmelidir.

3. İŞ MODELİ

3.1. Farklı üretici çözümleri değerlendirildi mi?

İhtiyaç duyulan güvenlik donanımı ürün/hizmeti farklı üretici ve yüklenici tarafından farklı çözümler sunularak sağlanabilir. Bir üretici web güvenliği çözümünde sadece URL filtering ana fonksiyonunu sunarken farklı bir üretici web güvenliği çözümünde URL filtering ana fonksiyonu dışında içerik analizi, DLP, malware analizi gibi ek özellikler sunabilir. Bu nedenle aynı kategorideki farklı üreticilerin çözümlerin değerlendirilip avantaj ve dezavantajlarına göre en uygun ürün seçilmelidir. Farklı üreticilerin sunduğu çözümler bir test, pilot veya PoC ortamında gözlemlenerek hangi çözümün neler sağlayabileceği detaylı olarak değerlendirilmelidir. Bu çalışmayla önerilen çözümlerin avantajları ve kurumun ihtiyaçlarını ne düzeyde karşıladığı gibi konular gözlemlenebilir. Böylelikle, ihtiyacı tam olarak karşılamadığı düşünülen noktalar varsa bunlar tedarik öncesinde daha detaylı olarak değerlendirilebilir.

Projelerde farklı kriterlerin ağırlığı hesaplanarak bir teknik değerlendirme tablosu hazırlanabilir. Bu değerlendirme tablosunda fiyat, çözümün teknik yeterliliği, ölçeklenebilirlik, yönetilebilirlik, süreklilik, uyumluluk ve ileride duyulacak ek ihtiyaçlar gibi faktörlerin çözüm içinde hangi önem ağırlığında olduğunun netleştirilmesi daha efektif bir karar verilmesini sağlayacaktır.

Çok sayıda çözümün değerlendirilmesi, hem zaman ihtiyacı gerektirdiği, hem de kaynak sayısını arttıracağı için PoC testi yapılacak ürünler, bu ürünleri kullanan diğer kurumların memnuniyet durumlarına göre sayıca kısıtlanabilir. Böylelikle önerilen çözümler tüm özellikleriyle daha detaylı değerlendirilmiş olacaktır. Üretici çözümleri değerlendirilirken bulut, mobil gibi gelişen teknolojilerle uyumluluğu, kurumun mevcut güvenlik ve kalite standartları dikkate alınmalıdır.

Alınacak ürünün ileride ihtiyaç duyulabilecek bir ölçeklenme çalışması sırasında farklı marka ürünlerle olan

uyumluluğu incelenmeli ve mümkün olduğu kadar üretici bağımlılığından kaçınılmalıdır.

Alınması planlanan güvenlik donanımları için bağımsız değerlendirme kuruluşlarının veya organizasyonlarının hazırladığı raporlarının incelenmesi faydalı olur. Bu kuruluş ve organizasyonlar ilgili ürünleri kendi test ortamlarında eşit şartlarda değerlendirmeye tabi tutarlar ve test sonucu teknik rapor oluştururlar. Buna ek olarak, ürünlerle ilgili farklı karşılaştırmalar da (ürünün deployment seçenekleri, desteklediği diller, üreticinin ürünün geleceği hakkındaki planları, güçlü yönleri, zayıf yönleri ve dikkat edilmesi gerekli noktalar vb.) bu incelemede yer alır. Bu değerlendirmeler dikkatli incelenirse doğru ürünü bulmada yol gösterecektir.

3.2. İhtiyaç duyulan güvenlik donanımına alternatif olabilecek açık kaynak kodlu çözümler incelendi mi?

İhtiyaç duyulan güvenlik fonksiyonları için açık kaynak kodlu çözümler özellikle sınırlı bütçeye sahip kurumlarda için alternatif bir çözüm olabilmektedir. Günümüzde ticari olarak satılan birçok güvenlik ürününün alternatifi olan bir açık kaynak kodlu çözüm bulunmaktadır. Açık kaynak kodlu çözümler maliyet avantajı sunarken özellikle yönetim ve destek tarafında eksiklikleri fazlaca hissedilmektedir. Kurum bünyesinde açık kaynak kodlu çözümlere ileri düzeyde destek verecek ve yönetimini yapacak teknik personel varsa veya bu hizmeti alabilecek bir çözüm ortağı bulunabiliyorsa açık kaynak kodlu çözümlerin değerlendirilmesi önerilir.

3.3. Bu ürünleri kullanan diğer kamu kurumları ziyaret edildi mi?

İhtiyaç duyulan güvenlik donanımını kullanan diğer kamu kuruluşları araştırılarak ürün değerlendirmeleri dikkate alınmalıdır. İhtiyaç duyulan güvenlik donanımını kullanan diğer kamu kurumlarının bilgi ve tecrübeleri dinlenerek doğru güvenlik donanımının konumlandırılması sağlanmalıdır. Aynı ürünü kullanan kurumların, kurulum öncesi ve kurulum sonrası varsa yaşadığı sıkıntılar ve öneriler ürün seçiminde yol gösterici olacaktır.

3.4. Bu donanımın yönetimini yapacak yeterli sayı ve yetkinlikte personel var mı?

Proje'nin verimli olarak yönetilebilmesi, işletim sırasında oluşabilecek aksaklıkların hızlı ve kolay çözülebilmesi için devreye alma aşamasında bu sürece refakat edecek kurumun personel ihtiyacı planlanmalıdır. Personel yetkinliğinin arttırılması gerekiyorsa alınacak eğitimler planlanarak anlaşma kapsamına eklenmelidir. Devreye alma ve işletim sürecinde yeterli personel yoksa dışardan bir kaynak alımı planlanması önemli olacaktır.

3.5. Eğitim planlaması yapıldı mı?

Kurum personeli için alınacak ürünlerle ilgili devreye alma öncesinde eğitim planlaması yapılması önemlidir. Alınacak eğitimler ile;

- Personelin kuruluma destek sağlayarak ürün hakkında deneyim elde etmesini sağlayacak,
- Devreye alma süresini kısaltacak,
- Kurulum sonucunda kurum personeli ürünün işletimini yapabilme yeteneği kazanacak,
- Herhangi bir güvenlik riski oluştuğunda ilgili güvenlik sistemi üzerinde hızlı aksiyon alabilecek,

- Personelin sisteme daha fazla hâkim olmasını sağlayacaktır.

3.6. Üreticinin veya destek verecek yüklenici firmanın ülke genelindeki kurumsallığı ve itibarı değerlendirildi mi?

Üretici firmaya karar verilirken aşağıdaki maddeler göz önüne alınarak bir değerlendirme formu hazırlanabilir:

- İlgili alandaki pazar payı,
- İlgili teknolojiler konusunda standardizasyon belirlenmesine yapılan katkıları,
- Sektördeki tanınırlığı,
- Arge'ye yaptığı yatırım oranı,
- İlgili alanlardaki patent ve buluşları,
- Ürün geliştirme aşamalarında üniversitelerle olan ortak çalışmaları,
- Ürünlerinin bilinirlik düzeyleri,
- Üretim merkezlerinin yaygınlığı ve lojistik, bayi, distribütör ve kanal yapısının yeterliliği,
- İlgili çözüm ve projeyi stratejik olarak görüp görmedikleri,
- Kalite belgeleri ve hangi standartlarla uyumlu oldukları,
- Sertifikalı personel sayısı ve personelin nitelikleri,
- Yerleşik ofisi bulunup bulunmadığı ve yakın konumda çalıştırdığı personel sayısı,
- Faaliyete başladığı yıl.

Benzer şekilde yüklenici firmaya karar verilirken aşağıdaki maddeler göz önüne alınarak bir değerlendirme formu hazırlanabilir:

- Daha önce yapılmış benzer projelerdeki referansları,
- Referans projenin büyüklüğü, karmaşıklığı, hangi noktalarda altyüklenici veya dış kaynak kullandığı/kullanacağı,
- Referans listesinde yer alan kurumlardan görüş alınması,
- Servis ağının yaygınlığı,
- Teknik destek elemanlarının yetkinliği ve uzmanlık sertifikaları,
- Çağrı merkezi, yedek parça ve çağrı takip süreçlerinin bulunması,
- İlgili alanlardaki kalite belgeleri

Uzun süreli ve detaylı projelerde üretici ve yüklenici firmanın finansal durumunun proje sürecini ve kapsamını belirlenen süre içinde yürütebilecek yeterlikte olup olmadığı değerlendirilmelidir.

4. ÇIKTILAR

4.1. Teknik şartname hazırlandı mı?

Kurum ihtiyacı belirlendikten sonra, tedarik edilecek ürüne ilişkin bir teknik şartname hazırlanmalıdır.

Teknik şartnamede net ve anlaşılır bir biçimde istenilen ürün özellikleri belirtilmelidir. Belirli bir marka, model, patent veya ürün ismi kullanmaktan kaçınılmalı, tarafsız bir şartname oluşturulmalıdır.

Teknik şartnamede yer alacak hükümler ve talep edilecek özellikler; tereddüde, yanlış anlamaya ve bir isteğin diğeri ile çelişmesine imkân bırakmayacak şekilde, açık ve kesin olmalıdır.

Teknik şartname en az iki, mümkünse daha fazla üretici firmanın ürününü kapsayacak ve böylece rekabet ortamı yaratacak şekilde hazırlanmalıdır.

Teknik şartnamesi hazırlanan üründen beklenen performans, çalışma şartları, kullanım yeri ve amacı açıkça belirtilerek fonksiyonel istekler yazılmalı; varsa ürünün birlikte kullanılacağı diğer cihazlar/elemanlar ile uyumlu çalışması isteğine de yer verilmelidir.

Teknik şartnamede sayılar ile ifade edilen teknik kriterlere tolerans verilebilir. Kullanılan ölçü birimleri uluslararası ölçü birimleri sistemine uygun olmalıdır.

Ürün ile birlikte istenecek yedek parça ve sarf malzemesi, bakım setleri, doküman ile ilgili hususlar teknik şartnameye dâhil edilmeli, bu tür malzeme, cihaz ve dokümanın miktarı belirtilmelidir.

Tedarik edilecek ürünleri yönetecek personele verilmesi gerekli olabilecek teknik içerikli eğitimler ile ilgili hükümler teknik şartnamede belirtilmelidir.

Ürünü sağlayacak firmadan beklenen kalite güvence sistemi belgesi ve ürün kalite belgesi hususları belirtilmelidir.

Donanım ile ilgili garanti şartları ve yedek parça koşulları teknik şartnameye eklenmelidir.

4.2. Sözleşme hazırlandı mı?

Kurum ile bilgi güvenliği altyapısı donanımlarının tedarik edileceği firma arasında, tedarik kapsamının, koşullarının ve tedarik süresi boyunca uyulacak kuralların yer aldığı bir hizmet sözleşmesi yapılmalıdır. Firma tarafından sağlanacak tüm ürünlere ve tedarik sırasında gerçekleştirilecek faaliyetlere ilişkin detaylar bu sözleşmeye eklenmeli ve karşılıklı görev tanımları ve sınırlarını net olarak belirlenmelidir.

Görev ve sorumluluklar belirlenirken, kurum üzerine düşen görevler de değerlendirilmelidir. Örneğin sözleşme maddesinde aşağıdaki gibi bir ekleme olması beklenebilir.

Firma Sorumlulukları:

- Belirlenen özelliklere uygun ürünlerin teslim edilmesi,

- Söz konusu ürünlerin kullanıma hazır hale getirilmesi,
- Donanımların kuruma teslim edilmesi

Kurum Sorumlulukları:

- Donanımların çalışacağı ortamın hazırlanması,
- Bu ortamda gerekli elektrik ve ağ bağlantılarının hazır olarak sağlanması,
- İlgili paydaşlar ile gerekli koordinasyonun gerçekleştirilmesi.

Sözleşme içerisinde servis seviyesi anlaşması (SLA- Service Level Agreement) maddelerinin (ürünün ne kadar sürede sağlanacağı, ne kadar sürede kurulacağı, vb.) sözleşmede olmasına özen gösterilmelidir. SLA sürelerine uyulmaması durumunda gerçekleştirilecek faaliyetler belirlenmeli, sözleşme içerisine cezai madde ekleyip eklememe konusunda karar verilmelidir. Kurumun cezai madde hususunda yüksek oranlar ile şartname hazırlamaması önerilmektedir. Bu durum ihaleye girecek hizmet sağlayıcı sayısını azaltacağı gibi fiyat performans dengesini de bozacaktır.

Bu sözleşme içerisinde bir alt başlık (veya bir ek) olarak gizlilik sözleşmesi yer almalıdır. Gizlilik sözleşmesi hem kurumun hem de hizmet sağlayıcının haklarını belirleyen önemli bir sözleşmedir. Gizli bilgi ifşa eden tarafın kendisi, işçileri, şubeleri ya da çalışanlarınca, diğer tarafın işçileri, şubeleri ya da çalışanlarına açıklanan her türlü fikir, buluş, iş, yöntem, ilerleme ve patent, telif hakkı, marka, ticari sır ya da diğer yasal korumaya konu olan ya da olmayan her türlü yenilik; tarafların arasındaki ticari ilişki esnasında öğrenecekleri yazılı veya sözlü tüm ticari, mali, teknik bilgiler, taraflardan herhangi birinin diğerine verdiği tüm teklif ve/veya talepler ve bunların içerikleri, nihai müşteri bilgileri ve konuşma bilgileri sır olarak kabul edilmelidir. Bu gizli bilgileri tarafların koruması ve kesinlikle 3. şahıslar ile paylaşmaması sağlanmalıdır.

4.3. Ürünlerin devreye alınması için bir geçiş planı yapıldı mı?

Ürünlerin tedariki sırasında, donanımların devreye alınma sürecinin hesaba katılması önemlidir. Gerekli kaynakları ayarlamak ve koordine etmek, ihtiyaç duyulan süre zarfında ürünlerin çalışır hale getirebilmek için mevcut yapıdan öngörülen yapıya geçişle ilgili bir Geçiş Planı hazırlanmalıdır. Geçiş Planı aşağıdaki başlıkları içermelidir:

- Hangi ürünlerin/cihazların devreye alınacağı
- Ürünlerin devre alınması sıraları ve prosedürleri
- Devreye alınma sürecini etkileyebilecek riskler ve bu risklere karşı uygulanacak önlemler
- Farklı ekiplerin rolleri ve görevleri (donanım kurulumu, altyapı hazırlığı, vb.)
- Mevcut ise Değişiklik Yönetimi Prosedürünün takibi

Devreye alınmadan önce, geçiş sırasında ve geçişten sonra aşağıdaki konular göz önünde bulundurulmalıdır:

- Geçişten önce mevcut sistemlerin yedeklerinin alınması ve geri dönüş testlerinin yapılması,
- Geçiş sırasında bir problem olması durumunda sistemin geçişten önceki başlangıç durumuna geri

dönülmesi için izlenecek alternatif prosedürlerin belirlenmesi,

- Sistemler devreye alınmadan önce bir test ortamında yapılan konfigurasyonların öngörülen şekilde çalışıp çalışmadığının test edilmesi.
- Ürünlerin mümkünse, önce bir pilot yerleşimde devreye alınması ve belli bir süre kullanımı sağlanarak yaygınlaştırmadan önce gözden kaçmış olabilecek noktaların belirlenmesi.

Geçiş sırasında yukarıdaki konularla ilgili mevcut durum değerlendirilip belirsiz noktalar ve karar verilmesi gereken konular varsa geçiş süresine etkileri göz önünde bulundurulmalıdır.

4.4. Ürünlerin teknik dokümanları ve kullanıcı kılavuzları alındı mı?

Sistemler tedarik edildiğinde üretici firma tarafından kutuları içinde bulunan kullanım kılavuzları cd, kullanım kitapları vs. saklanmalıdır. Ürünü hazır hale getiren firmadan da kullanıcı kılavuzları ile teknik dokümanlar temin edilebilir.

4.5. Ürünlerin garanti belgeleri ve lisans belgeleri alındı mı?

Her donanımın üreticisi tarafından verilen garanti belgesi mevcuttur. Bu lisanslar üretici veya yüklenici firmadan talep edilmeli, kurum tarafından yetkili kişilerce saklanmalıdır.