GÜVENLİK YAZILIMI TEDARİKİ REHBERİ

1. KAPSAM VE AMAÇ

1.1. Güvenlik Yazılımı Tedariki nedir?

Antivirüs, güvenlik duvarı, e-posta güvenlik, ağ erişim kontrolü (NAC), web güvenliği - vekil sunucu, saldırı tespit ve önleme, veri sızıntısı önleme (DLP) vb. yazılımların tedarikini kapsamaktadır.

1.2. İhtiyaç analizi çalışması yapıldı mı?

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

- Kurumun elinde bulunan lisanslı yazılım envanterinin çıkartılması
- Güvenlik yazılımlarının üzerinde çalışacağı donanımların teknik özelliklerinin belirlenmesi
- Güvenlik yazılım envanterinde bulunan güvenlik yazılımlarının bu ihtiyaç kapsamında kullanıp kullanılmayacağının değerlendirilmesi
- Mevcut güvenlik yazılım sistemlerinde geriye dönük problem kayıtlarının incelenmesi, kullanıcı şikâyetlerinin ve beklentilerinin dikkate alınması
- 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 ürünün, doğru ölçekte ve doğru lisanslama ile konumlandırabilmek için aşağıdaki hususların dikkate alınması önemlidir.

1.2.1. Antivirüs yazılımı

Antivirüs yazılımları, kurumun son kullanıcı cihazları (PC, laptop, tablet) ve sunucularının zararlı yazılımlardan korunmasını sağlar. Antivirüs yazılımları gelişen özellikleri ile birlikte Endpoint Security olarak adlandırılır. Bunun sebebi bu ürünlerin artık sadece antivirüs korumasına değil farklı güvenlik yeteneklerine sahip olmasıdır. Bunlar IPS, firewall, disk şifreleme, veri koruması vb. dir. Doğru antivirüs yazılımını seçerken aşağıdaki maddelere dikkat edilmelidir;

- Antivirüs yazılımı kurulacak son kullanıcı cihaz sayısı belirlenmeli,
- Antivirüs yazılımı kurulacak sunucu sayısı belirlenmeli,
- Antivirüs yazılımının kullanıcı makinalarındaki işletim sistemlerine desteği kontrol edilmeli,
- Kurum bünyesinde kullanılan mobil cihazların antivirüs koruması sağlanacak mı belirlenmeli,
- Antivirüs özelliğine ek olarak hangi güvenlik fonksiyonlarına (IPS, firewall, disk şifreleme, veri koruması vb.) sahip olması gerektiği belirlenmeli,
- Aktif dizin entegrasyonu desteği kontrol edilmeli,
- Antivirüs yazılımı lisanslama modeli belirlenmeli.

1.2.2. Güvenlik duvarı yazılımı

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 interface sayısı ve tipi belirlenmeli,
- Güvenlik duvarı üzerinde DMZ ağ segmenti olacak mı belirlenmeli,
- Firewall yazılımının üzerinde çalışacağı donanımın teknik özelliklerinin uygunluğu ve üretici tarafından desteklenip desteklenmediği kontrol edilmeli,
- Güvenlik duvarının konumlandırılacağı noktadaki yedeklilik 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 yazılımının 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,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli

1.2.3. E-posta güvenlik yazılımı

E-posta güvenlik yazılımları, 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 yazılımlarının ana fonksiyonu gelen ve giden elektronik postaları virüs ve spam kontrolünden geçirmektir. Gelişen güvenlik ihtiyaçları ile birlikte e-posta güvenlik yazılımları şifreli e-posta iletimi, kötü amaçlı yazılım (malware) analizi, veri sızıntısı kontrolü gibi ek güvenlik modülleri içermektedir. E-posta güvenlik yazılımı ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- Çözümün e-posta sunucusu üzerinde mi yoksa ayrı bir sunucu üzerinde mi çalışacağı dikkate alınarak sunucu ihtiyacı hesaba katılmalı,
- Koruma yapılacak e-posta adresi sayısı,
- Antivirüs ve antispam kontrolü ile birlikte veri sızıntısı önleme, e-posta şifreleme ve kötü amaçlı yazılım

önleme çözümlerinden hangilerine ihtiyaç olduğu belirlenmeli,
- Aktif dizin entegrasyonu ihtiyacı belirlenmeli,

1.2.4. Ağ erişim kontrolü (NAC) yazılımı

Ağ erişim kontrolü yazılımları, 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,

1.2.5. Web güvenliği - Vekil sunucu

Web güvenliği yazılımları 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 yazılımı ihtiyacı belirlerken aşağıdaki maddeler dikkate alınmalıdır;

- Web güvenliği yazılımlarının kurum ağına aşağıdaki yöntemlerden hangisi ile uygulanacağı belirlenmeli,
  - Yönlendirme mod: Kullanıcı gateway'leri üzerinde http/https trafiği web güvenliği yazılımına yönlendirilir
  - Inline Mod: Web güvenliği yazılımının çalıştığı donanım ağa tüm trafik üzerinden geçecek şekilde (inline) olarak dahil edilir.
  - Proxy (Vekil sunucu) mod: Web güvenliği yazılımı ağ içinde herhangi bir yerde olabilir. Son kullanıcı web tarayıcılarına vekil sunucu olarak web güvenliği yazılımının 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,
- Aktif dizin entegrasyonu 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 yazılım ve lisansları; yeni sistemde de kullanılmaya devam edilebilir. Mevcut güvenlik yazılımları, yeni güvenlik yazılımları ile beraber kullanılmaya devam edilecekse sistemlerin uyumluluğu kontrol edilmelidir. Örneğin; yeni güvenlik yazılımlarının, network ve log yönetim yazılımlarıyla entegrasyonu isteniyorsa, mevcut yazılımlar kapasite, lisans ve destek açısından değerlendirilerek bu yazılımlara ek güvenlik özellikleri, versiyon yükseltme ve lisans artırımı gibi ihtiyaçlar belirlenmelidir.

İlave bir güvenlik yazılım alımı yapılacaksa, mevcut güvenlik yazılımı sistemlerinin üretici tarafından desteklenen güncel bir ürün olup olmadığı kontrol edilmelidir. Mevcut güvenlik yazılımlarının 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 yazılımlarının versiyonları ile mevcut güvenlik yazılımlarının 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 email güvenliği, 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 yazılımı almadan ihtiyacın mevcut güvenlik yazılımına ek özellik alımıyla karşılanabiliyor olması, güvenlik yazılım 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 merkez lokasyonlarında ihtiyaç duyulan güvenlik fonksiyonuna özel üretilen yazılımların kullanılması önerilmektedir. Örneğin; kritik öneme sahip yerlerde URL filtering çözümü ile güvenlik duvarı çözümünün aynı yazılım üzerinde olması performans ve iş süreklilik açısından önerilmemektedir.

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

Yeni alım yapılacak güvenlik yazılımlarının üzerinde çalışacağı sunucu, mevcut sunucu altyapısıyla mı yoksa yeni sunucu alımı ile mi yapılacağı belirlenmelidir. Yeni sunucu alımına ihtiyaç varsa maliyete dâhil edilmelidir. Bazı üreticiler, yazılımlarının çalışacağı işletim sistemlerini kendileri düzenleyerek çözümlerini güvenlik yazılımı ve işletim sistemi bir arada olacak şekilde virtual appliance (sanal donanım) dediğimiz bir paket olarak sunarlar. Bu çözümlerden kurumun yapısına uygun olanın seçilmesi tavsiye edilir.

Alımı yapılacak güvenlik yazılımının çalışabilmesi sunucu dışında ek bir ürüne ihtiyaç olup olmadığı değerlendirilmelidir. Örneğin kurulacak güvenlik yazılımı 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. Veri tabanı ile birlikte kurulacağı sunucudaki işletim sistemi ihtiyacı da düşünülmelidir. Bu veri tabanı ve gerekli lisanslar (işletim sistemi gibi) ek maliyet oluşturabilir. Seçilecek güvenlik yazılımında bu ihtiyaçların önceden belirlenmesi ve bunları kurumun sağlayıp sağlayamayacağı belirlenmelidir.

Ayrıca, sunucuların 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 yazılımlarının çalışacağı sunucuların 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 yazılımlarının yönetim ara yüzü özellikleri değerlendirildi mi?

Güçlü, kolay ve görsel bir yönetim ilgili güvenlik yazılımının en etkin biçimde kullanılmasını sağlar. Bütün güvenlik yazılımları bir kullanıcı arabirimi üzerinden yönetilir. Bazı güvenlik yazılımları 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 yazılımlarının kendi üzerinde yönetim modülü olabildiği gibi ayrı bir yönetim modülü ile de yönetim imkânı sunabilir. Böylece dağıtık olarak çalışan birden fazla aynı tür güvenlik yazılımı ayrı ayrı yönetilmektense bir yönetim modülü ile merkezi olarak yönetilebilir. Bu nedenle güvenlik yazılımlarının nasıl bir yönetim özellikleri sahip olması gerektiği belirlenmelidir.

2.5. Yazılımın ihtiyaç duyulan raporlama yetenekleri belirlendi mi?

Seçilecek güvenlik yazılımının 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 mail ile gönderilen raporlar incelenerek farklılıklar değerlendirilebilir. Bu nedenle seçilecek güvenlik yazılımın raporlama yeteneğinin ihtiyaca yönelik olarak belirlenmesi gerekir. Aşağıdaki gibi örnek raporlama isterleri belirtilebilir;

- Güvenlik yazılımı sistem istatistiklerinin raporlanması,
- Güvenlik yazılım 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)
- Yazılım içinde 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 yazılımdan log alınması planlanıyor mu?

Güvenlik yazılımları ana fonksiyonu (firewall, antivirüs vb.) ile birlikte üzerinde çalıştığı sistem ile ilgili (CPU, memory, çalışan servisler) loglar da üretir. Bu loglar güvenlik yazılımının 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 yazılımlarından beklenen alarm isterleri belirlendi mi?

Birçok güvenlik yazılımı, üzerinde oluşan bir problem anında veya ana fonksiyonu gereği bir güvenlik ihlali oluşması durumunda alarm üretme kabiliyetlerine sahiptir. Örneğin güvenlik yazılımında bir fonksiyon devre dışı kaldığında, disk belli bir yüzde oranında dolduğunda veya bu güvenlik yazılımı bir e-posta güvenlik yazılımı 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 yazılımdan 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 yazılımından beklenen güncelleme hakları ve sürelerinin belirlenmesi gerekir. Özellikle içerik kontrolü yapılan güvenlik yazılımlarında (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 yazılımının 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. Ayrıca, yazılımın ihtiyaç duyulan süreye göre bakım ve destek maliyetinin de hesaba katılması faydalı olacaktır.

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

Temin edilecek güvenlik yazılımı kritik önemdeki hizmetlere altyapı sağlayacaksa, hizmet sürekliliğinin değerlendirilmesi amacıyla yedekliliğinin göz önünde bulundurulması ve yatırımın bu doğrultuda planlanması gerekir. Örneğin güvenlik duvarı yazılımı 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 yazılımı ürünlerinin yedekli olarak planlanması önemlidir.

2.10. Devreye alınma süreci proje süresini etkileyecek riskler içeriyor mu?

Güvenlik yazılımlarının devreye alınma sürecinin hesaba katılması proje süresi açısından önemlidir. Proje süresini ne kadar etkilediğini tespit etmek için, mevcut yapıdan öngörülen yapıya geçişle ilgili bir Geçiş Planı hazırlanmalıdır. Geçiş Planı aşağıdaki başlıkları içermelidir:

- Hangi güvenlik yazılımlarının devreye alınacağı
- Güvenlik yazılımlarının devre alınma sıraları ve prosedürleri
- Devreye alınma sürecini etkileyebilecek riskler ve bu risklere karşı uygulanacak önlemler
- Mevcut ise Değişiklik Yönetimi Prosedürü'nün takibi

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

- Geçişten önce yoksa tüm ağ ve güvenlik topolojisinin ayrıntılı olarak çıkartılması
- 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
- Yapılacak çalışmalarla ilgili kullanıcıları ve operatörlerin önceden bilgilendirilmesi, yine çalışma tamamlandığında güncellenmesi
- Sistemler devreye alınmadan önce bir test ortamında yapılan konfigurasyonların öngörülen şekilde çalışıp çalışmadığının test edilmesi.
- Projenin mümkünse, önce bir pilot lokasyonda devreye alınması ve belli bir süre kullanımı sağlanarak yaygınlaştırmadan önce gözden kaçmış olabilecek noktaların belirlenmesi.

Yukardaki konularla ilgili mevcut durum değerlendirilip belirsiz noktalar ve karar verilmesi gereken konular varsa projesi süresine etkileri göz önünde bulundurulmalıdır.

3. İŞ MODELİ

3.1. Farklı üretici çözümleri değerlendirildi mi?

İhtiyaç duyulan güvenlik yazılımı ürün/hizmeti farklı üretici ve yüklenici tarafından farklı çözümler sunularak sağlanabilir. Bir üretici endpoint security güvenlik yazılımında sadece antivirüs ana fonksiyonunu sunarken farklı bir üretici endpoint security güvenlik yazılımında antivirüs ana fonksiyonu dışında firewall, IPS, DLP, disk şifreleme 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 yazılımları için açık kaynak kodlu çözümler incelendi mi?

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

3.4. Bu yazılımın 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 yazılımı 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 güvenlik yazılımlarına ilişkin bir teknik şartname hazırlanmalıdır.

Teknik şartnamede net ve anlaşılır bir biçimde istenilen yazılım 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 güvenlik yazılımları tarafından sağlanması beklenen performans, çalışma şartları, kullanım yeri ve amacı açıkça belirtilerek fonksiyonel istekler yazılmalı; varsa yazılımın 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.

Güvenlik yazılımları ile birlikte istenecek ek modül, bakım setleri, dokümanlar ile ilgili hususlar teknik şartnameye dahil edilmeli, bu tür malzeme, cihaz ve dokümanın miktarı belirtilmelidir.

Tedarik edilecek güvenlik yazılımlarını 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.

Yazılım ile ilgili garanti şartları ve bakım koşulları teknik şartnameye eklenmelidir.

4.2. Sözleşme hazırlandı mı?

Kurum ile güvenlik yazılımlarının 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 yazılımın teslim edilmesi,
- Söz konusu yazılımın sunucular üzerine kurulması, kullanıma hazır hale getirilmesi,

- Yazılımın kuruma teslim edilmesi

Kurum Sorumlulukları:

- Yazılımın üzerine kurulacağı sunucunun hazırlanması,
- Gerekli sunucu yapılandırmasının (ağ ayarları, vb.) gerçekleştirilmesi,
- 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. Yazılımın devreye alınması için bir geçiş planı yapıldı mı?

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

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

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

- Güvenlik yazılımlarının kurulacağı sunucuların fiziksel veya sanal olup olmayacağının belirlenmesi,
- Güvenlik yazılımlarının kurulacağı sunucuların belirlenmesi,
- Bu sunucular üzerinde mevcut ortalama ve maksimum kaynak (işlemci, bellek, disk ve ağ) kullanım oranlarının tespit edilmesi,
- Güvenlik sistemleri yazılımlarına ilişkin kullanıcı sayılarının ve servislerinin analiz edilmesi, ihtiyaç

duyulacak kaynak miktarının belirlenmesi,

• Mevcut sunucuların yazılım için elverişli olup olmadığının belirlenmesi, gerekirse yeni sunucu tedariki için gerekli planların yapılması,

• Güvenlik yazılımlarının kullanılacak işletim sistemleri ile uyumluluğunun değerlendirilmesi,

• Tedarik edilmesi planlanan yazılımların versiyonları ile mevcut ürünlerin versiyonları arasındaki farklılıkların değerlendirilmesi,

• Ürünlerin kullanılacak özelliklerinin analiz edilmesi ve güvenlik yazılımları için uygun lisanslama modelinin seçilmesi,

• Mevcut sistemde kullanılmakta olan lisansların kullanılabilirliğinin değerlendirilmesi (üretici ile olan anlaşmaya bağlı olarak yükseltme yapılarak yeni sistemde mevcut lisanslar kullanılabilir mi?),

• Tedarik edilecek yazılımların yükseltme mi yoksa yeni kurulum mu olacağının belirlenmesi,

• Geçişten önce mevcut yazılımlara ilişkin yedeklerin alınması ve geri dönüş testlerinin yapılması,

• Geçiş sırasında bir problem olması durumunda yazılımın geçişten önceki başlangıç durumuna geri dönülmesi için izlenecek alternatif prosedürlerin belirlenmesi,

• Yazılımlar devreye alınmadan önce bir test ortamında yapılan konfigurasyonların öngörülen şekilde çalışıp çalışmadığının test edilmesi.

• Yapılacak çalışmalarla ilgili kullanıcıların ve BT ekiplerinin önceden bilgilendirilmesi, yine çalışma boyunca bu kişilerin güncellenmesi,

• Yazılımların 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. Yazılımların teknik dokümanları ve kullanıcı kılavuzları alındı mı?

Güvenlik yazılımları tedarik edildiğinde üretici firma tarafından kutuları içinde bulunan kullanım kılavuzları cd, kullanım kitapları vs. saklanmalıdır. Yazılımı kurup, çalışmaya hazır hale getiren yüklenici firmadan da kullanıcı kılavuzları ile teknik dokümanlar temin edilebilir.

4.5. Yazılımların garanti belgeleri ve lisans belgeleri alındı mı?

Her yazılımın üreticisi tarafından verilen lisans ve garanti belgeleri mevcuttur. Bu belgeler gerektiğinde yararlanmak üzere, üretici veya yüklenici firmadan talep edilmeli, kurum tarafından yetkili kişilerce saklanmalıdır.

TÜBİTAK-BİLGEM-YTE