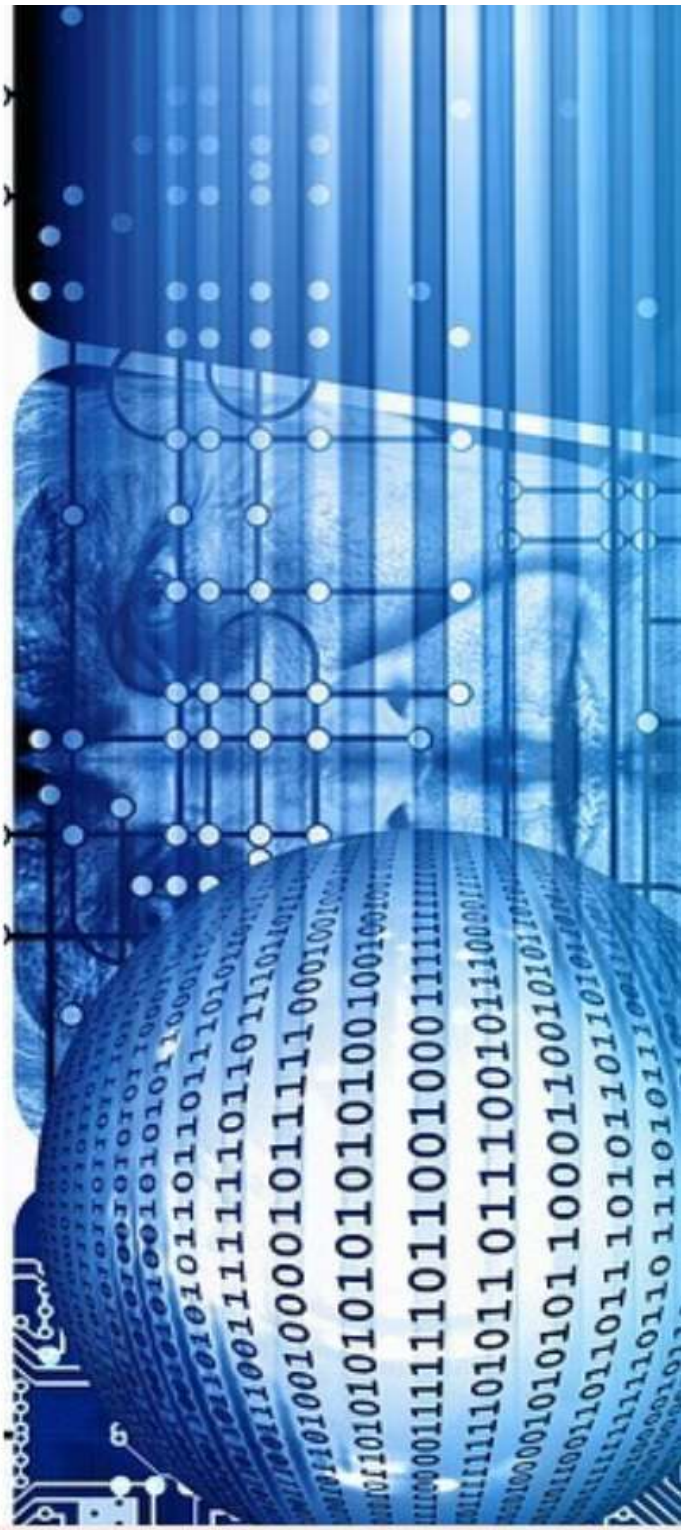
KÜÇÜK VE ORTA ÖLÇEKLI İŞLETMELER İÇIN 60 DAKİKADA AĞ GÜVENLİĞİ



Sparta Bilişim

Sparta Bilişim, kuruluşların siber güvenlik konusunda ihtiyaç duydukları profesyonel hizmetleri sunmak amacıyla 2013 yılında kurulmuştur. Bugüne kadar 200'ün üzerinde kuruluşa sızma testinden, siber olaylara müdahaleye kadar geniş bir alanda hizmet veren Sparta, iş birliği yaptığı kuruluşların mevcut bilgi teknolojileri ve bilgi güvenliği ekiplerinin bir uzantısı gibi çalışmaya özen göstermektedir.

Güvenlik Yaklaşımımız

Eski Yunan'da etrafı surlarla çevrili olmayan tek şehir Sparta'dır. Bunun nedeni kral Agesilaus'a sorulduğunda askerlerinin mızraklarını gösterip "Sparta'nın surları bunlar" dermiş. Kuruluşların siber güvenlik seviyesini artırmak için savunma (firewall, antivirüs, vb.) çözümleri sunmuyoruz. Başta sızma testleri olmak üzere sunduğumuz hizmetler "saldırı" tarafında. Hackerların ve zararlı yazılımların neler yapabileceğini önceden tespit ederek gerekli ve doğru tedbirleri almanızı sağlıyoruz.

Duvar gibi reaktif değil, proaktif güvenlik süreçleriyle hizmet verdiğimiz kuruluşların surlarını sağlamalaştırıyoruz.

Bilişim Teknolojileri alt yapısının güvenliğini sağlamak karmaşık ve genellikle tecrübeli siber güvenlik uzmanlarını ilgilendiren bir konu. Ancak günümüzde ağ güvenliğinin sağlanabilmesi için çok daha fazla kişinin ağ yapısının bileşenlerini anlamaya ihtiyacı oluyor.

Bu "Ağ Güvenliği Raporu"nu oluştururken elimizden geldiğince tüm bilişim teknolojisi çalışanlarına ve sistem yöneticilerine uygun bir çalışma ile karşılaşılan riskler konusunda bilgi vermeye ve farkındalık yaratmaya çalıştık.

Siber saldırganların hız kesmeden zafiyetleri istimar etmeye çalıştığı bir dünyada, bu döküman içerisinde de bahsedeceğimiz gibi aslında açıkların kolaylıkla tespit edilebildiğini ancak çoğu zaman kapatılmadıklarını görüyoruz.

Sistem yöneticileri, BT altyapısı genelinde mevcut çok sayıda güvenlik açığına karşı bir risk yönetimi seviyesi sağlamaya çalışırken bu görevin sorumluluğu büyük oluyor. Güvenlik tarayıcıları sistem yöneticilerinin binlerce güvenlik açığını tanılamasına yardımcı olabilirken, tanı koyulmuş olan açıklara karşı BT ekibinin ağı korumak için tüm bilgileri etkili bir şekilde kullanma yeteneği zorlanabilir.

Bu rapor, mümkün olduğunca anlaşılabilir bir dil ile Bilişim Teknolojileri personelinin ağ güvenliğini sağlamasına yardımcı olmak amacıyla hazırlanmıştır. Ağ güvenliği sağlayabilmek için yapılması gereken çok sayıda görev arasında nereden başlanacağı, nereye odaklanılması gerektiği, ilk yapılması gerekenler ve mümkün çözümler gibi konularda bir rehber niteliği taşımaktadır. Ancak ağ güvenliğinin özet bir rehber ile sağlanamayacak kadar geniş ve önemli bir konu olduğunu, bu rehberin yalnız genel olarak güvenlik konusunda bir bakış açısı sağlamak ve ağ güvenliği riskini azaltmak amacını taşıdığını da belirtmek isteriz.

İÇİNDEKİLER

ÖZET ÖNERİLER

Küçük ve orta ölçekli işletmelerin ağ güvenliği konusunda alması gereken önemli eylem önerilerinin özeti aşağıdaki gibidir:

- Kuruluşunuza yönelik tehditleri modelleyin ve güvenlik risk değerlendirmesi yapın
- Bir güvenlik politikası belirleyin ve kullanıcılarınızı eğitin
- Güvenli bir ağ tasarlayın, router paket filtreleyici kullanın, firewall kullanın, internet erişimi bulunan sunucular için DMZ (Demilitarized Zone yani iç network ile dış dünyayı birbirinden ayıran bölge) ağı kullanın.
- Her ağ geçidi ve bilgisayarda bir antivirüs kullanın.
- Sadece yeterli güvenlik özellikleri bulunan işletim sistemlerini kullanın.
- Ağınızı tanıyın, gereksiz uygulamaları ağdan kaldırarak yapısını güçlendirin, işletim sistemleri ve kullanılan uygulamaların güncellemelerinin ve yamalarının yapılması için bir prosedür uygulayın.
- Özellikle mobil kullanıcılar için kişisel firewall kullanımı sağlayın.
- Güçlü parola kullanımı konusunda tüm kullanıcıları bilinçlendirin.
- Olay müdahale planı oluşturun
- Hemen başlayın

1000 çalışandan az kişiye sahip işletmeler “Küçük ve orta ölçekli işletme” (KOBİ) sınıfına dahil edilmektedir. Özellikle bu gruptaki işletmelerde görülen genel yanılgı siber saldırılara hedef olmak için fazla ufak veya önemsiz olduklarını düşünmeleridir. Aynı şekilde, sahip oldukları verilerin hassas veri olmaması veya yüksek değer taşımaması nedeniyle saldırganlara çekici gelmeyeceği yanılgısına da rastlanmaktadır. Geçmişte yaşanmış pek çok örnek ile gördüğümüz gibi, bir kuruluşun kurban haline gelmesi için mutlaka hedef olması gerekmez. Yaşanmış geniş çaplı siber saldırıların çoğunda küçük ve orta ölçekli kuruluşlar direkt olarak hedeflenmemiş olmasına rağmen kurban durumuna düşmüştür. Hatta kitlesel siber saldırı olaylarında büyük ölçekli işletmelere göre daha fazla sayıda KOBİ’nin zarar gördüğü de tespit edilmiştir.

Büyük işletmelerde tek sorumluluğu bilişim teknolojileri güvenliğinin sağlanması olan personeller bulunabilirken, bunun aksine sınırlı kaynaklar ile çok iş başarmaya çalışan KOBİ’lerde bu görev genellikle BT personelinden bir kişinin yarı zamanlı görevidir.

Bir araştırma kuruluşu olan Gartner’ın 2003 yılında yayınladığı “SMB’s Show Preference for Security Services” raporunda kendi bilişim teknolojileri güvenliğini kendisi yöneten ve internette e-posta göndermekten fazlasını yapan her KOBİ’nin başarılı bir siber saldırı yaşayacağı ve %50’sinin bunu yaşadığını fark etmeyeceği yazılmıştı. Üzerinden geçen 16 yılda kullanıcılar bilinçlendi, koruma için çok sayıda yazılım ve donanım geliştirildi ancak siber saldırganlar da aynı hızla geliştiği için gelinen noktada durum çok da değişmedi.

Açıkça, her kuruluşun kendi yapısına uygun bir güvenlik mimarisi belirlemesi gerekiyor ve KOBİ’ler de bu gereklilikten muaf değil, onlar da aynı oranda güvenlik riski altında.

AĞ GÜVENLİĞİ İLE İLGİLİ GENEL BİLGİLER

Bilişim Teknolojileri ve ağ güvenliğinin doğru anlaşılabilmesi için bazı terimlerin açıklanması gerekmektedir:

Zafiyetler (Vulnerabilities): Zafiyetler genel şekliyle "yazılımlardaki güvenlik boşlukları" olarak tanımlanabilir. Bilgisayarda, sunucuda, routerda ya da kısaca üzerinde yazılım çalışan her cihazda zafiyet bulunabilir. Tüm zafiyetler aynı soruna yol açmaz; kimilerinde yalnız cihazın çalışması etkilenir/bozulurken, bazı zafiyetler siber saldırganların yönetici yetkilerini kazanmasına ve sistemi kontrol etmesine neden olabilmektedir.

Bir zafiyetin ortaya çıkmasının ardından yazılım geliştiricinin de hızlıca bir yama yayınlaması ve bunun kullanıcılarına duyurulması beklenir. Her zaman beklendiği kadar hızlı olmamakla birlikte esas karşılaşılan sorun kullanıcıların bu güncellemeleri (yamaları) yapmaması ve zafiyetlerin kötü niyetli kişilerce istismar edilmeye açık halde kalmasıdır.

İstismar Kodları (Exploits): Yazılımlarda zafiyetler bulunduğunda siber saldırganlar harekete geçer ve bir saldırı kodu oluşturmaya çalışır. Bu saldırı kodlarına (yazılımlarına) ise istismar kodu adı verilir. İstismar kodları genelde siber saldırganlar arasında forum ve benzeri platformlarda paylaşılarak yayılır ve daha karmaşık saldırılarda kullanılmak üzere geliştirilmeye çalışılır.

Tehdit veya saldırılar: Amaçlarına göre tehdit ve saldırılar birkaç gruba ayrılabilir; Tek bir kuruluşu hedef alan saldırılar ve kitlesel saldırılar (genellikle bir virüs veya solucanın kendisini olabildiğince hızlı ve fazla sayıda bilgisayarda kopyalayarak yayılması).

NEREDEN BAŞLAMALI?

Güvenlik mimarisinin oluşturulması konusunda bir genelleme yapmak tehlikeli ve yanlış bir iş olacaktır. Her kuruluşun ağ ve BT oluşumu birbirinden farklı özelliklere sahip, farklı seviyelerde, farklı bilgisayarlar, işletim sistemleri, uygulamalar ve farklı erişim ihtiyaçlarına sahip olduğundan genel geçer kurallar koyularak bunlara uyulmasının istenmesini doğru bulmuyoruz. Ancak genel anlamda aynı özelliklere sahip KOBİ'lerin ağ güvenliğini iyileştirmek amacıyla hızla gerçekleştirilebilecek ve güvenlik seviyesinde ciddi bir iyileşmeye yol açabilecek bazı özellikleri sıralamaya çalıştık.

KOBİ'ler olarak genellediğimiz grubun aynı olması beklenen özellikleri:

- Her daim açık durumda bir internet bağlantılarının bulunması
- Kuruluş bünyesinde bir mail sunucusu bulundurmaları
- Kuruluş bünyesinde bir web sunucusu bulundurmaları
- Kuruluş bünyesinde internet kullanıcıları bulundurmaları
- Bir dosya sunucusu ve/veya veritabanında müşteri ve diğer iş bilgilerinini bulundurmaları

Ağ güvenliğinin sağlanması için malesef tek bir mükemmel çözüm sunmak mümkün değil. Gerçekten güvenli bir ağ yapısının oluşturulması ancak tehditlerin iyi anlaşılması ve sürekli olarak güncellenen/değişen bu tehditlerin kuruluş üzerinde yarattığı potansiyel riskin doğru hesaplanabilmesi ile mümkün olabilecektir. Riskler değerlendirildikten sonra özellikle en yüksek kategoride görülen tehditler için hemen harekete geçilmesi ancak bu şekilde sağlanabilecektir.

10 ADIMDA 11 ADIM ATMAK

1. Kuruluşunuza yönelik tehditleri belirleyin, güvenlik risk değerlendirmesi oluşturun:

Her kuruluşun kendine özgü bir yapısı olduğundan özellikle kendi kuruluşunuza yönelik tehditleri bilmeniz önemlidir. Potansiyel tehditlerin listesi sonu gelmeyecek denli uzayabileceğinden, BT personeli ile kuruluş yöneticileri birlikte çalışarak bu tehditlerin hangilerinin gerçekten endişelenilmesi gerekenler sınıfında olduğuna karar vermesi gereklidir. Risk değerlendirmesi yapılırken kuruluşu ilgilendirebilecek tüm riskler, bunların bir yılda kaç defa gerçekleşme ihtimali olduğu ve gerçekleştiği takdirde oluşması muhtemel zararın tutarı belirlenir. Bu şekilde her bir risk için "yıllık yaşanması muhtemel kayıp tutarı" ortaya çıkacaktır.

Risk değerlendirmesinin avantajı, elinizde böyle bir liste olduğunda hangi kayıpları göze alıp hangilerini alamayacağınıza karar vermenizi kolaylaştırmasıdır.

Aşağıdaki gibi bir tabloyu kendi kuruluşunuz için uyarlayarak oluşturabilirsiniz:

RİSKLER	KURULUŞA ETKİLERİ	YILLIK YAŞANMASI BEKLENEN OLAY SAYISI	OLAY BAŞINA TAHMİNİ OLUŞACAK KAYIP	TOPLAM YILLIK KAYIP BEKLENTİSİ	İYİLEŞTİRME ADIMLARI
Virüs Bulaşması	Bilgisayarlardan virüslerin temizlenmesi bilgisayarların tekrar kurulması ve yedek verilerin yüklenmesi için harcanacak zaman. Ağda kesinti yaşanması.	15	15.000TL	225.000TL	Ağ geçidi ve tüm bilgisayarlar için antivirüs alınması

Tablodaki örnekte görüldüğü gibi toplam kayıp beklentisi iyileştirme adımı için gerekli olan tutardan yüksek olduğunda bu iyileştirme adımını beklemeden atmak mantıklıdır. Bazı durumlarda ise yaşanacak olan kayıp iyileştirme için yapılması gerekenden daha düşük çıktığından kuruluşlar riski göze almayı tercih etmektedir.

Ayrıca tüm kuruluşların kendi yapılarına bağlı olarak neye öncelik vereceğine de karar vermesi gereklidir.

Örneğin, gelirlerinin büyük çoğunluğunu internet üzerinden satış ile yürüten bir kuruluşun web sunucusunun güvende olduğundan emin olması gerekir. Aynı şekilde, toplam yıllık kayıp beklentisinin de özellikle DoS saldırıları için yüksek belirlenmesi gereklidir çünkü özellikle bu saldırılar sonucunda büyük miktarda gelir kaybı yaşanabilecektir.

Acil tehdit ve zafiyet duyurularının takip edilmesi, siber güvenlik ile ilgili bültenlerin, web sayfalarının takip edilmesi ve bilgilerin güncel tutulması riskler konusunda her daim güncel olmak konusunda yardımcı olacaktır.

2. Güvenlik Politikası oluşturun ve kuruluş çalışanlarını eğitin:

Güvenlik politikası, bir kuruluşun teknolojisine ve bilgi varlıklarına erişim izni verilen kişilerin uyması gereken kuralların resmi bir ifadesidir. Belirlenen güvenlik politikası kuruluşun güvenlik hedeflerini tüm kullanıcılara, sistem yöneticilerine ve kuruluş yöneticilerine iletir.

Güvenlik politikasının temel amacı; kuruluş çalışanlarını ve sistem yöneticilerini teknoloji ve bilgi varlıklarının korunması için zorunlu gereklilikleri konusunda bilgilendirmektir.

Bir diğer amaç ise; bilgisayar sistemlerini ve ağlarını politikaya uygun bir hale getirmek, yapılandırmak ve denetlemek için bir temel oluşturmaktır.

Bu gerekliliklerin karşılanabilmesi için gerekli olan mekanizmalar güvenlik politikası içerisinde yer almalıdır.

Güvenlik politikasının etkili olabilmesi için;
- Kuruluş içerisindeki her seviye çalışanı kapsamalıdır,

- Sistem yönetimi prosedürleri, kullanım kılavuzları veya benzeri yöntemler ile uygulanabilir olmalıdır,
- Gerekli görüldüğü takdirde, güvenlik araçları veya yaptırımlar ile uygulanabilir olmalıdır,
- Kuruluşun tüm çalışanlarının ve yöneticilerinin sorumlulukları açıkça tanımlanmış olmalıdır,
- Herkes tarafından bilinir ve erişilebilir durumda olmalıdır,
- Bilgisayar ağının değişimine göre değişebilen, esnek ve yaşayan bir belge olmalıdır.

Açıkça belirlenmiş bir güvenlik politikası oluşturulması ve tüm kuruluş çalışanlarının bilgilendirilmesi ağ güvenliğinin temelini oluşturacaktır. Örneğin, tüm bilgisayarda bulunacak yazılımların belirlenmesi, bu yazılımların öncelikle BT personeli tarafından test edilip ardından her bir bilgisayara yükleneceği ile ilgili bir prosedür oluşturulması hem BT personeline gelecek telefonları azaltarak iş yükünü düşürecek hem de güvenliği güçlendirecektir. Aynı şekilde, kuruluşun bir güvenli parola kullanımı prosedürü belirlemesi ve kullanıcıları bilgilendirmesi de ağ güvenliği için önemli bir adım olacaktır.

Tüm bilgisayar kullanıcılarının kuruluş siber güvenliğinde kendi rollerini anlamaları kritik bir önem taşır. Bu nedenle tüm kuruluş çalışanlarının siber güvenlik farkındalık eğitimi alması önerilir.

Üçüncü partilere uzaktan erişim izni verildiği durumlarda (örneğin iş ortakları, tedarikçiler, danışmanlar vb.) ne tür bir ağ trafiğine izin verileceğinin, uzaktan bağlanan tarafta ne tür güvenlik önlemleri alınması gerektiğinin (firewall, antivirüs vb.) de prosedürler ile belirlenmiş olması önemlidir.

3. Yeterli güvenlik yeteneklerine sahip işletim sistemleri ve uygulamalar kullanın:

Mümkün olduğu kadar işletim sistemlerinin ve istemciler, sunucular, anahtarlar (switchler), routerlar, güvenlik duvarları ve izinsiz giriş algılama sistemleri gibi ağda yer alan tüm bilgisayarlarda bulunan uygulamaların en son sürümlerini kullanmak gereklidir. Yamalar, servis paketleri, düzeltmeler takip edilerek, özellikle saldırganların uzaktan kod yürütmesine neden olabilecek güvenlik açıkları kapatılmalı, işletim sistemleri ve uygulamalar güncel tutulmalıdır.

Örneğin, Microsoft Windows 98 için yama yayımlamayı bıraktı ve bu eski işletim sistemine ait güvenlik zafiyetleri için artık herhangi bir düzeltme/yama çıkmıyor. Ayrıca Windows 98'in kullanıcı girişleri esnasında gerçek bir güvenlik sağlamadığı da (kullanıcı adı ve parolanın esc tuşuyla atlatılabilmesi nedeniyle) zaten biliniyor. Bu nedenle, eğer ağınızda birtane bile Windows 98 yüklü bilgisayar varsa onun hemen ağdan ayrılması gereklidir.

Kullanıcılara yönetici yetkilerinin verilmemesi de tavsiye edilir. Sistemlerin kullanıcılara "kilitli" modda teslim edilmesi ve bu sayede ilave bir yazılım yüklemelerinin engellenmesi sayesinde de BT personeli bilgisi ve yetkisi dışında ağda yazılım/donanım bulunması mümkün olmayacaktır.

4. Ağ yapısını tanıyın:

Ağda yer alan tüm donanım ve yazılımların bir listesine sahip olmak ve bu listeyi güncellemek BT altyapısının güvenliği için çok önemlidir. Bilgisayar sistemleri üzerinde varsayılan olarak gelen yazılımları anlamak da aynı derecede önem taşır. Ağınızda yer alan her bir sistem üzerinde neyin çalıştığını ve gerekli yamaların yapılıp yapılmadığını takip etmeniz gerekir.

Ağda çalışan servislerin envanterini çıkartabilmek için port taraması yapmak hızlı bir yöntemdir. Gereksiz sunucu ve servislerin tespit edilmesi ve kapatılması gereklidir. Gerekli sunuculara ise yalnız erişim ihtiyacı olan bilgisayarlardan erişim

izni verilmelidir. Nadiren kullanılan ancak güvenlik açığı bulunan işlevsel bölgeleri kapatmak, saldırganların bu açıklardan yararlanmasını önleyecektir.

Ağı, hostları ve işletim sistemlerini tanımak her birinde çalışan sistemi, zafiyetlerini bilmek anlamına gelir ve ancak bu zafiyetlerin giderilmesi ile güvenli bir ağ yapısı sağlanabilir. Bunun yapılabilmesi için Microsoft Baseline Security Analyzer, Nessus, NMAP gibi birçok araçtan yararlanılabilir.

Tüm kuruluş sunucuları (e-posta sunucusu, web sunucusu, dosya sunucuları, veritabanları vb.) gerekli olmayan yazılım ve işlemlerin temizlenmesi ile sıkılaştırılmalıdır. İşletim sistemlerinin varsayılan ayarlarda kurulması ile gelen ancak gerçekte gerekli olmayan pek çok program ve servis kaldırılarak saldırganlara daha az saldırı alanı bırakılacaktır.

5. Router'da paket filtrelemek, firewall kullanmak, internet erişimi olan sunucularda DMZ ağı kullanmak ve güvenli bir ağ oluşturmak:

Güvenli bir ağ oluşturmak için çok daha fazla madde sayılabilecektir ancak bazı kilit noktalar aşağıdaki gibi özetlenebilir;

- Kademeli savunma stratejisi kullanın. Basitçe; güvenliğinizi sağlaması için tek bir cihaz veya ürüne bağlı kalmayın. Bunun yerine router, firewall gibi cihazların güvenlik becerilerini de kullanın, host ve sunuculardaki yazılımların güncel olduğundan da emin olun, daha gelişmiş BT ortamlarında sızma tespit ve engelleme sistemleri de kullanın (IPS/IDS), şifreleme çözümlerini de değerlendirin yani kısaca pek çok farklı cihaz ve yazılım ile çok kademeli bir savunma sistemi kurmaya çalışın.

- 3 farklı bölge arasındaki geçişi firewall ile denetleyin (LAN, WAN ve DMZ).

- Web ve e-posta protokolleri gibi yaygın olarak kullanılan uygulamalar ve protokoller için uygulama proxy'leri kullanın.

- Ağ kaynaklarına erişimde "en az yetki" ilkesini benimseyin. Eğer kuruluş dışından veya içinden kişilerin belirli sistemlere veya uygulamalara erişmesine gerek yoksa, erişimlerini engelleyin.

- Sisteme yüklenen her bir bileşenin yüklemesi tamamlandıktan sonra beklendiği gibi çalışıp çalışmadığını kontrol edin. (Güvenlik açıklarına ve zafiyetlere yol açabileceğinden özellikle firewall ve router kurulumlarına dikkat edilmesi gerekmektedir. Örneğin, router'da uzaktan Telnet erişiminin yanlışlıkla açık bırakılması ciddi sorunlara yol açabilir.)

6. Ağ geçidinde ve ağa bağlanan her bilgisarda antivirüs kullanın:

Günümüzde antivirüs kullanımı bir seçenek değil, hem bilgisayarlar hem de ağ geçidi için bir zorunluluk. ".exe" gibi uzantıya sahip eklentili dosyaların direkt olarak engellenmesi de yarar sağlayacaktır.

7. Laptop ve mobil kullanıcıları için kişisel firewall kullanımını destekleyin:

Kuruluş ağı dışında kullanılan laptop ve mobil cihazların beraberinde getirebileceği güvenlik sorunları nedeniyle kişisel firewall kullanımının desteklenmesi önerilmektedir. Kuruluşların bilinen siber saldırılara karşı kendi firewall'larında gerekli önlemleri almasına karşın yabancı bir ağdan bulaşan bir virüs veya solucan nedeniyle etkilenmeleri sıklıkla karşılaşılabilen bir durumdur.

Ayrıca hassas veriler barındıran laptoplarda güçlü parola ve şifrelenmiş dosya/veri kullanılması da çalınma veya kaybolma gibi durumlara karşı zorunlu hale getirilmelidir.

8. Güçlü parola kullanımı:
Güçlü parola kullanımı denilince ilk akla gelen uzun, içerisinde büyük harf, küçük harf, sembol ve rakam barındıran parolalar gelse de bu tip parolaların kullanılmasının talep edilmesi kullanıcıları hatırlamakta ve kullanmakta güçlük çekecekleri parolalar belirlemeye ve ardından kullanmaktan kaçınmaya veya kolay erişilebilecek yerlere yazmaya itiyor. Bu nedenle de aslında güçlü parola seçimi işlevsiz bir hale geliyor.

NIST ((U.S. National Institute of Standards and Technology – A.B.D. Ulusal Teknoloji Standartları Enstitüsü), yakın zaman önce parola belirleme önerilerini güncelleyerek semboller ve rakamlardan
oluşan karmakarışık parolalar yerine en az 64 karakterden oluşan, kelimelerin arasında boşlukların bulunduğu cümlelerden parola oluşturmanın daha güvenilir olduğunu duyurdu.

Anlamsız dizilimlerdense kelimelerin akılda tutulmasının daha kolay olacaktır. Üstelik yine NIST'in açıklamasına göre eğer bir kere gerçekten iyi bir parola seçildiyse değiştirmeye de gerek yok, yeterki farklı yerlerde aynı parolayı kullanılmasın.

Ancak özellikle yüksek risk taşıyan işlemler için “güçlü parola” tek başına yeterli değil çünkü siber saldırganlar oturup tek tek parola tahmini yapmıyor. Bu nedenle iki (veya daha çok) kademeli kimlik doğrulama kullanımını da mutlaka önerilmekte.

Çoklu erişim kontrolü (Single sign-on (SSO) denilen, farklı uygulamaların tek bir kullanıcı adı ve parola ile açılabildiği yazılımlar da değerlendirilebilecek seçenekler arasında.

9. Olay Müdahale Planı oluşturun:
Her kuruluşun bir siber güvenlik olayı yaşadığında nasıl müdahale edeceğine dair önceden hazırlanmış bir planı olması gerekiyor. Bu planın yapılması büyük, orta veya küçük ölçekli bir kuruluş olmakla bağlantılı değil zira her ölçekte kuruluş günümüzde en az bir olay yaşıyor (bazıları sadece fark etmiyor). Olay müdahale planında; olayı analiz etmekte kullanılacak kaynaklar ve olaydan kurtulmak için gerekli kaynaklar belirlenmiş olmalı. Küçük ölçekli kuruluşlar için bu kaynaklar “dış kaynak” olarak belirlenebilir ve bu tip bir durum ile karşılaşıldığında bir siber güvenlik uzmanı veya danışman yardımına başvurulabilir.

10. Hemen başlayın:
Çoğunlukla karşılaştığımız olaylardan öğrendiğimiz şu; başımıza bir şey gelmediği sürece harekete geçmiyoruz ve biz harekete geçmeye karar verdiğimizde genellikle “çok geç” oluyor. Verilerimizi veya paramızı veya hem verilerimizi hem paramızı kaybetmiş oluyoruz ve kaybedeceklerimiz de bunlarla sınırlı kalmıyor; ciddi bir iş gücü ve zaman kaybı yaşanan siber güvenlik olaylarının ardından bizi bekliyor. Bir siber saldırı yaşamanız için büyük kazançlar elde eden, sistemlerinde çok önemli/gizli/hassas veriler barındıran veya ilgi çekici bir sektörde iş yapan bir kuruluş olmanıza gerek yok. İnternet kullanıyor olmanız bir saldırıya denk gelmeniz için yeterli. Virüsler ve benzeri zararlı yazılımlar “sizin için” yazılmıyor ancak genellikle sizi de buluyor bu nedenle hazır olmak ve hemen şimdi hazırlanmaya başlamak gerekiyor.

11. Adım
Yukarıda yazılı 10 adıma ek olarak bir iş sürekliliği planı yapılması da alınan önlemlerin işe yaramaya devam etmesinde fayda sağlayacaktır. Verilerin düzenli olarak yedeklerinin alınması, bu yedeklerin gerçekten çalışır durumda olduklarının kontrol edilmesi, yedeklenen verilerin doğru (güvenli) saklanması, BT ekipmanlarının fiziksel olarak da güvenliğinin sağlandığından emin olmak gibi önlemler bu listeye eklenebilir.

Ayrıca, sızma testi hizmeti alınarak kuruluş güvenliğinin dışarıdan bir firma tarafından ölçülmesi güvenlik problemlerinin tespiti ve giderilmesi için büyük fayda sağlayacaktır.

SPARTA BİLİŞİM

Sparta kuruluşların siber güvenlik konusunda ihtiyaç duydukları profesyonel hizmetleri sunmak amacıyla 2013 yılında kurulmuştur. Bugüne kadar 200'ün üzerinde kuruluşa sızma testinden, siber olaylara müdahaleye kadar geniş bir alanda hizmet veren Sparta; iş birliği yaptığı kuruluşların mevcut bilgi teknolojileri ve bilgi güvenliği ekiplerinin bir uzantısı gibi çalışmaya özen göstermektedir.

- **Hizmetlerimiz**
- Test Hizmetleri
- İç ve Dış ağ sızma testleri
- Web uygulama sızma testleri
- Mobil uygulama sızma testleri
- Altyapı ve güvenlik mimarisi testleri
- Senaryo tabanlı güvenlik testleri
- SCADA güvenlik testleri
- Fiziksel sızma testleri
- VoIP ve Video Konferans testleri
- Hastane Bilgi Yönetim Sistemi (HBYS) güvenlik testleri
- Elektronik Belge Yönetimi Sistemi (EBYS) güvenlik testleri

Test hizmetlerimiz NIST, EC-Council, OWASP ve SANS gibi uluslararası olarak kabul görmüş standart ve metodolojilere uygun olarak verilir.

- **Analiz ve Danışmanlık Hizmetleri**
- Siber güvenlik risk seviyesi değerlendirmesi
- Siber risk iş etki analizleri
- Taşeron/Tedarikçi risk analizleri
- KVKK (Kişisel Verilerin Korunması Kanunu) danışmanlığı ve ISO27001 belgelendirme hizmeti
- Güvenlik envanteri değerlendirmesi
- FKM (Felaket Kurulum Merkezi) danışmanlığı
- SIEM (Security Incident and Events Management) danışmanlığı
- SOME (Siber Olaylara Müdahale Ekibi) danışmanlığı
- İç tehdit değerlendirme hizmeti
- SANS Critical Security Controls
- Center for Internet Security sistem sıkılaştırma danışmanlığı
- Olay müdahale (incident response) danışmanlığı
- Siber güvenlik stratejisi danışmanlığı
- **Eğitimlerimiz**
- Sızma testi eğitimleri
- SOME Eğitimleri
- Zararlı yazılım analizi eğitimleri
- Trafik analizi eğitimleri
- Log analizi eğitimleri
- Siber kriz yönetimi eğitimleri

YASAL UYARI

Bu dokümanda yer alan her türlü yazı, materyaller, tablo ve grafikler herhangi bir ortamda basılamaz, yayımlanamaz, basılmak ya da yayımlanmak üzere yeniden yazılamaz, doğrudan ya da dolaylı olarak dağıtılamaz.

Dokümanda yer alan bilgileri herhangi bir ticari ve çıkar amacı olmadan kişisel bilgi edinmek amacıyla kullanabilir, indirebilir, kopyalayabilir, yazdırabilirsiniz ya da herhangi bir ticari ve çıkar amacı olmadan üçüncü şahıslara sadece kişisel bilgilendirmeleri amacıyla bu bilgilerin Sparta Bilişim LTD. ŞTİ.'den temin edildiğini belirtmek şartıyla verebilir ve gönderebilirsiniz.

Söz konusu bilgiler tarafsız ve dürüst bir bakış açısıyla düzenlenmiş olup, alıcısının menfaatlerine ve/veya ihtiyaçlarına uygunluğu gözetilmeksizin ve karşılığında maddi menfaat elde etme beklentisi bulunmaksızın hazırlanmıştır. Dokümanda yer alan bilgilere dayanak teşkil eden bilgi ve veriler, güvenilir olduğuna inanılan kaynaklardan derlenmiştir. Bu nedenle, bu bilgilerin tam veya doğru olmamasından, kullanılan kaynaklardaki hata ve eksik bilgilerden dolayı doğabilecek zararlar konusunda Sparta Bilişim LTD. ŞTİ. ve çalışanları herhangi bir sorumluluk kabul etmez.

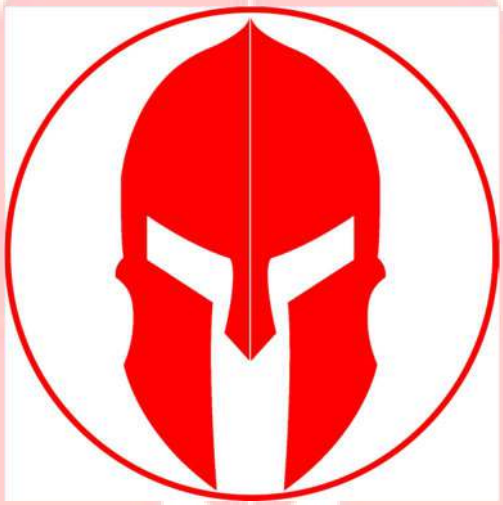
Dokümanda yer alan bilgiler okuyucuların genel olarak bilgi edinmeleri amacıyla hazırlanmış olup, Sparta Bilişim LTD. ŞTİ. tarafından herhangi bir garanti verilmemektedir. Dokümanda yer alan bilgilerden kaynaklanabilecek zararlardan dolayı Sparta Bilişim LTD. ŞTİ. herhangi bir sorumluluk üstlenmemektedir. Burada yer alan bilgi, yorum ve tavsiyeler siber güvenlik danışmanlığı kapsamında değildir.

Dokümanda yer alan bilgi, materyal ve bunlara ilişkin telif hakkı ve/veya diğer fikri mülkiyet hakları, Sparta Bilişim LTD. ŞTİ.'ye ait ve ilgili kanunlarca korunmakta olup, herhangi bir kişi/kuruluş, önceden yazılı izin almadıkça, dokümanın belli bir kısmını veya tamamını kullanamaz, dokümanda yer alan içerikler kopyalanamaz.

Sparta Bilişim LTD. ŞTİ. bu yasal uyarıda yer alan tüm koşulları ve hükümleri önceden bir ihbara gerek kalmaksızın değiştirme ve güncelleme hakkına haizdir. Değişiklikler dokümanın yayım anında yürürlüğe girer. Dokümanın indirilmesi ile birlikte bu değişiklikler de kabul edilmiş sayılır.

Bilgilerin gerek doğrudan, gerekse dolaylı kullanımından kaynaklanan doğrudan ve/veya dolaylı maddi ve/veya manevi velhasıl her türlü zarardan ve kayıplardan ve her ne şekilde olursa olsun üçüncü kişilerin uğrayabileceği her türlü zarar ve/veya kayıplardan dolayı Sparta Bilişim LTD. ŞTİ. çalışanları ve bu dokümanda yer alan bilgileri hazırlayan kişiler sorumlu tutulamaz.

İş bu dokümanın kullanımından doğan ve/veya yasal uyarıda yer alan koşul ve hükümlere ilişkin ve/veya bu doküman ile bağlantılı olarak çıkabilecek uyuşmazlıklarda Türkçe yasal uyarı metni esas olup, Ankara Merkez Mahkemeleri ve İcra İflas Daireleri yetkilidir.



Sparta Bilişim Teknolojileri Yazılım Danışmanlık Sanayi ve Ticaret Ltd. Şti.

Adres: Mustafa Kemal Mahallesi Dumlupınar Bulvarı No: 266 A/82 Çankaya/Ankara

Telefon: 0 312 909 33 02

Web: www.sparta.com.tr