FİZİKSEL DİJİTAL İLE BULUŞUYOR

EN İYİ SİBER GÜVENLİK UYGULAMALARI

IRON MOUNTAIN®

EN İYİ SİBER GÜVENLİK UYGULAMALARI

Son araştırmaların da gösterdiği gibi, **veri ihlalleri** kuruluşlar için büyük bir sorun teşkil ediyor. Avrupa ve ABD'deki 4200 şirkette yapılan bir araştırmaya göre:

- Araştırmaya katılan şirketlerin **neredeyse yarısı**, geçtiğimiz yılda bir ihlal bildirdi [1].
- Türkiye'de **veri ihlalinin ortalama toplam maliyeti** önceki yıla kıyasla yüzde 18,5 artarak **11,15 milyon TL'ye** yükseldi.

İşletmeler için risk sadece cezaların miktarı değildir. Düşen hisse fiyatları, müşterinin güven kaybı ve itibarın zarar görmesi marka üzerinde olumsuz bir etkiye neden olur.

İşletmelerin saldırıları önlemek için kullanabilecekleri birçok araç bulunuyor. Biz bu yazıda, büyük resmi ele alıyoruz. Bilgi sistemlerinizin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak ve onları **bir ihlal durumunda kurtarmak** için en iyi siber güvenlik uygulamalarını kuruluşunuz genelinde nasıl uygulayabilirsiniz?

HER BÜYÜKLÜKTEKİ İŞLETMENİN SİBER GÜVENLİK KONUSUNDA ENDİŞELENMESİ GEREKİYOR MU?

Saldırganlar kuruluşun büyüklüğüne ya da küçüklüğüne bakmazlar. Büyük kuruluşlar tarafından saklanan müşteri verilerinin hacmini cazip bulsalar da; küçük işletmelerin tedarik ve ödeme sistemlerine erişmek de yeterince ilgilerini çekiyor.

Bazı açılardan küçük ve orta ölçekli işletmeler için sorun daha da büyüktür. Güvenlik önlemleri için kısıtlı bütçeleri vardır ancak kısa bir süre için bile işlerinin kesintiye uğramasını göze alamazlar.

1. IBM / Ponemon Institute: The 2020 Cost of a Data Breach Report

NE TÜR SALDIRILARA MARUZ KALABİLİRSİNİZ?

Siber saldırıların çeşitliliğinden ve sizi nasıl etkileyebileceklerinden haberdar mısınız? İşletmenizi etkileyebilecek birçok saldırı türü vardır.

- İstatistikler, **kötü amaçlı yazılımların**, her gün uğraşmak zorunda olduğumuz en büyük tehdit olmaya devam ettiğine işaret ediyor. Virüsler, solucanlar, Truva atları ve casus yazılımların tümü kötü amaçlı yazılım türleridir. Kötü amaçlı yazılımların bilgisayar sistemlerinize girmesine izin vermek için masum görünen bir bağlantıya tıklamak yeterli olabilir.
- **Fidye yazılımlar** giderek daha popüler hale geliyor. Verileri şifrelediğini ve yalnızca fidye ödenmesi üzerine anahtarı vereceğini iddia eden bir siber terörist kuruluşla iletişime geçer. Kuruluş, bu tehdidin gerçek olup olmadığını ve fidye ödemesinin bir işe yarayıp yaramayacağını bilmiyorken gerçekten doğruysa kesinlikle olumsuz etkileneceğini bilir.
- **Kimlik avı (oltalama)** ise kullanıcılara odaklanır ve kişisel ve finansal bilgilerini vermeleri için onları güvenilir görünen e-postalarla kandırmaya çalışır.

Ulus devletlerden organize suç örgütlerine ya da hacktivistlere kadar çok çeşitli oyuncular tarafından başlatılan birçok başka saldırı türü vardır. Neredeyse tüm veri türlerinin alıcısı olması sebebiyle siber saldırıların şekli, ölçeği ve karmaşıklığı hızla değişmeye devam edecektir.

Bu alandaki uzmanlar genel olarak her kuruluşun önlem alsın almasın bir gün siber saldırıya uğrayacağı konusunda hemfikirdirler. Saldırıları önlemek için bir strateji geliştirmek, her büyüklükteki işletme için zaruridir.

HANGİ TÜR VERİLERE SAHİPSİNİZ?

Hangi tür verilere sahip olduğunuzu ve bunlara neden sahip olduğunuzu biliyor musunuz? Acaba zaten elinizde tutmamanız gereken verileri mi riske atıyorsunuz?

Elinizdeki verileri anlamak ilk adımdır. Verilerin etkin ve yasalara uygun olarak **yönetilmesi ve korunması** çok önemlidir. Veriyi iyi yönetmek, verilerinizin kuruluş içinde nasıl aktığını anlamak ve **yaşam döngüsünün her aşamasında** güvenliğini sağlamak gerekir.

RİSK TABANLI BİR STRATEJİ OLUŞTURUN

Yönetilmesi gereken üç temel risk, **operasyonel risk, itibar riski ve yasalara uyum riskidir**. Siber saldırı riskini yönetmek için herkese uyan tek bir yaklaşım olmasa da, TS ISO/IEC 27001 gibi güvenlik standartlarına uyum sağlamanın büyük önemi vardır.

Hangi standartların sizin durumunuza en uygun olacağı konusunda doğru kararı almak önemlidir.

İŞLETMENİZİ BÜTÜNÜYLE ELE ALIN

Siber güvenlik sadece teknoloji ile ilgili değildir. Ancak BT, hukuk ve güvenlik uzmanlığının bir araya gelmesiyle bir strateji geliştirilebilir ve tehditlere meydan okunabilir. Kuruluştaki her bireyin dolandırılmanın ne kadar kolay olduğunun farkında olması çok önemlidir.

GÜVENLİK BİLİNCİNE SAHİP BİR ÇALIŞMA KÜLTÜRÜNÜ TEŞVİK EDİN

İnsan unsuru, güvenli bir ortam yaratmada kritik öneme sahiptir.

Güvenlik açıkları her zaman insanların kötü niyetli olmasıyla ilgili değildir, ancak yanlış bir linke masum bir tıklama, kötü bir oyuncunun sisteme girmesine izin verebilir.

Çalışanların riskin ve sorumluluklarının farkında olması gerekir ve burada güvenlik bilinci ve eğitimi kritik önem taşır. Tutarlı olmanın ve güvenlik politikalarına bağlılığın önemini tüm ilgili kişilere açıklayarak uygun eğitimi verin.

Hoşnutsuz çalışanlar veya eski çalışanlar konusunu ise şu şekilde ele alın:

- **Davranışlarını izleyin** ve gözle görülür bir hoşnutsuzluk varsa tespit edin.
- Risk oluşturabilecek çalışanları tespit etmek ve riski ortadan kaldırmak için **süreçler belirleyin ve uygulayın**.
- Rol tabanlı **erişim izinlerini** uygulayın ve en kritik sistemlere ve verilere erişimi sınırlandırın.

GÜÇLÜ BİR YÖNETİM STRATEJİSİ OLUŞTURUN

Stratejinizin başarılı olması için kuruluşunuzun güçlü bir **yönetime ve liderliğe** ihtiyacı var. Ancak bu şekilde tüm işletme **siber güvenlik stratejileriyle uyumlu** hale gelebilir, veri ihlallerinin etkisi azalır ve güvenlik kaynakları daha iyi tahsis edilip yönetilebilir.

Güçlü bir strateji şunları içerir:

- Üst düzey yöneticilerin desteği
- Siber güvenlikten ne şekilde sorumlu olduğu net olarak tanımlanmış bir kişi
- Net politikalar ve prosedürler
- Güçlü bir siber güvenlik kültürü
- Güvenlik ihlali anında yürürlüğe girecek bir plan

UÇTAN UCA BİR SAVUNMA SİSTEMİ GELİŞTİRİN

Savunma tedbirleri ihlal edilebilir; bu nedenle veriye erişim haklarından başlayarak uçtan uca derinlemesine bir **savunma stratejisi** geliştirmek önemlidir. Saldırgan bir savunma hattını geçerse, onu diğer savunma hatlarıyla karşılamış olursunuz.

Örneğin fiziksel güvenlik önlemleri yetkisiz kişilerin erişimini engellemelidir. Aynı zamanda, gelişmiş savunma araçlarının yanı sıra ağ ve sistem kontrolleri, güvenlik duvarları, izinsiz giriş önleme ve erişim kontrol önlemleri gibi geleneksel önlemler de kullanılmalıdır.

FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ: EN KÖTÜ DURUMA HAZIRLIKLI OLUN

Birçok işletmenin felaket kurtarma ve iş sürekliliği planları vardır ancak bunlar genellikle sel veya yangın gibi beklenmeyen fiziksel olaylara hazırlanmakla ilgilidir. Ancak bütün işletmeyi çalışmaz hale getiren siber saldırılar da bir felaket olarak adlandırılabilir.

Başarıya ulaşan bir saldırının işletmeniz üzerinde yaratacağı olumsuz etkinin boyutlarını düşünün ve bunu nasıl yöneteceğinizi planlayın.

Şu soruları sormalısınız:

- İşletmeniz bir kesintiye ne kadar dayanabilir ve mümkün olan en kısa sürede geri yüklenmesi gereken kritik uygulamalar nelerdir? Nakit akışını etkileyen saldırılar karşısında küçük işletmeler daha hassastır.
- Bir saldırıdan kurtulmak için ne kadar harcamaya hazırsınız? Örneğin, verileri birden çok ağda saklamak daha pahalı olabilir ama daha etkilidir.
- Veri merkezinin içinde ve dışında bağlantı sağlayan fibere kadar, fiziksel kurulumunuzda gereksiz olabilecek her bir parçayı gözden geçiriyor musunuz?
- Bir siber saldırının gerçekleşmesi durumuna karşı personelinizi eğitiyor, felaket kurtarma programlarınızı düzenli olarak test ediyor ve bu tatbikatlara tedarikçilerinizi ve ortaklarınızı da dahil ediyor musunuz?

Resmi bir müdahale planı, bir saldırıyla başa çıkmayı ve ondan kurtulmayı kolaylaştırır.

Saldırılara karşı bir müdahale ekibi oluşturun ve bu ekibi sürekli olarak eğitin. Planı gözden geçirin, masa başında prova edin ve insan hatasını nasıl en aza indirebileceğinizi planlayın. **Profesyonel bir müdahale firmasıyla anlaşmak** ve herhangi bir olay meydana gelmeden önce onlarla müdahale süreleri konusunu netleştirmek iyi bir seçenek olabilir.

- Hem kurum içi hem de kurum dışı paydaşlara hitap eden bir kriz yönetimi planı geliştirin.
- Planlamanızı bir ihlal halinde normal iletişim sistemlerinin çalışmayabileceğini göz önünde bulundurarak yapın.
- Son olarak verilerinizi güvenli bir şekilde yedeklediğinizden emin olun.

BİR İHLAL VARSA HIZLI HAREKET EDİN

Bir ihlali tespit etmek ortalama 220 gün sürerken, bu ihlale karşı harekete geçmek ise ortalama olarak fazladan 73 gün sürer[2]. Ne kadar hızlı hareket ederseniz, ihlalin olumsuz etkisi ve yarattığı maliyet o kadar düşük olur. Araştırmaya göre ihlali 30 günden daha kısa bir sürede çözüme kavuşturan şirketler bir milyon doların üzerinde tasarruf sağlıyor.

BİR İHLALİ OLABİLDİĞİNCE ERKEN RAPORLAYIN

Tüm planlamanıza rağmen bir veri ihlali yaşadığınızda, raporu daha sonra güncellemeniz gerekse bile, bunu olabildiğince çabuk bildirin. Bu şekilde ödediğiniz para cezasından önemli ölçüde tasarruf edebilirsiniz.

PLANINIZI GÜNCEL TUTUN

Sürekli olarak verileri yöneten ve analiz eden yeni teknolojiler geliştiriliyor ve işletmelerin bu teknolojileri siber güvenlik planlamasının bir parçası haline getirmek için kendilerini güncel tutmaları gerekiyor.

Siber saldırılara karşı savunma sisteminizi geliştirmek için yapay zeka ve makine öğrenimi gibi yeni teknolojileri kullanabilirsiniz. Saldırıların da aynı hızda gelişeceğini unutmayın.

Siber saldırılar ve siber güvenlik bir kedi-fare oyunu olmaya devam edeceğinden, herkesin her an tetikte olması hayati önem taşıyor.

VERİ MERKEZİNİZİ AKILLICA SEÇİN

Sistemlerinizi bir üçüncü taraf veri merkezine taşımayı tercih ederseniz, fiziksel ortamlarından politikalarına ve prosedürlerine kadar her şey hakkında soru sormayı unutmayın. Erişim yetkisi olan kişiler konusunda endişeniz var mı? Herhangi bir veri ihlali durumunda ne kadar sürede bilgilendirileceğinize dair bir garanti veriliyor mu? Denetim haklarınız var mı? Sağlayıcınızın TS ISO/IEC 27001 gibi bir standarda uyum sağlıyor mu?

TEDARİKÇİ VE İŞ ORTAKLARINIZI DA UNUTMAYIN

Siber güvenlikte ne kadar iyi olursanız olun dış dünyadan izole bir şekilde iş yapamazsınız.

Üçüncü taraf bağlantılarınızı da gözden geçirip, her ne kadar kolay olmasa da onların da kendi kuruluşunuz için yaptığınız gibi aynı tür gözetim ve kontrollere sahip olmaları için elinizden geleni yapın.

2. IBM / Ponemon Institute: The 2020 Cost of a Data Breach Report

HEPSİNİ KENDİNİZ YAPAMIYORSANIZ YARDIM ALIN

Üçüncü taraf bir danışman, verilerinizi bulundukları yerde kontrol ederek onları sınıflandırıp sınıflandırmayacağınızı belirleyebilir. Her duruma göre farklı bir savunma modeli önereceklerdir.

Küçük ve orta ölçekli işletmelerin tam zamanlı güvenlik görevlisi çalıştırması pek olası değildir. Bunun yerine yılda birkaç kez gelip inceleme yapacak ve tavsiyede bulunacak **bir iş ortağı bulun**. Saldırı anında yardıma hazır birilerinin olması için iş ortağınızı hızlı aramaya kayıt edin.

Güvenlik konusundaki eğitimlere yatırım yapın. Bu eğitim şirketleri sadece eğitim vermekle kalmayıp aynı zamanda çalışanların öğrendiklerini pekiştirmek için teste de tabi tutacak şirketler arasından seçilmeli.

Gerçekten dışarıdan yardım alacak durumda değilseniz online olarak tehdit değerlendirme şablonları bulabilirsiniz.

IRON MOUNTAIN HAKKINDA

1951 yılında kurulan Iron Mountain Incorporated (NYSE: IRM), saklama ve bilgi yönetimi hizmetlerinde dünya lideridir. Dünya çapında 225.000'den fazla kuruluş tarafından güvenilmektedir. 56 ülkedeki 1.450'den fazla tesiste 8,5 milyon metrekareyi aşan gayrimenkul ağıyla Iron Mountain, kritik bilgiler, son derece hassas veriler, kültürel ve tarihi eserler dahil olmak üzere maddi manevi çok değerli varlıkları saklıyor ve koruyor. Fiziksel arşiv yönetimi, bilgi yönetimi, dijital dönüşüm, güvenli imhanın yanı sıra veri merkezleri, bulut hizmetleri, sanat eseri saklama ve lojistiği içeren çözümler sunan Iron Mountain, işletmelerin maliyet ve risklerini düşürmelerine, düzenlemelere uymalarına, felaket durumlarından kurtulmalarına ve daha dijital bir çalışma ortamı benimsemelerine yardımcı oluyor. Daha fazla bilgi için www.ironmountain.com.tr adresini ziyaret edin.

IRON MOUNTAIN®

EN DEĞERLİ VARLIKLARINIZI KORUYORUZ.