İNCELEME YAZISI

ÇALIŞANLARIN VERİ İLE İMTİHANI

IRON MOUNTAIN®

ÇALIŞANLARINIZ HANGİ VERİLERE ERİŞEBİLİYOR VE BU VERİLERLE NE YAPIYORLAR?

İŞ HAYATI MI ÖZEL HAYAT MI?

Son on yılda şirketlerin çalışma şekli oldukça değişti. İş hayatı ve özel hayatın sınırları belirsizleşti. Günün sonunda ofisin kapısını kapattığınızda her şeyi geri dönene kadar güvenli bir şekilde arkanızda bırakma fikri geçmişte kaldı. Paylaşımlı masalar, uzaktan çalışma, internet üzerinden yapılan toplantılar dünyanın her tarafında günlük hayatın bir parçası oldu.

Aynı zamanda dijital dönüşüm ile birlikte çalışanların erişebildiği bilgi miktarı haddinden fazla arttı. Bir bilgiyi kopyalayıp yan masada çalışan iş arkadaşına ya da dünyanın öbür ucuna göndermek hiç bu kadar kolay olmadı. Bilgiyi paylaşıyoruz, yüklüyoruz, indiriyoruz, insanları bizi takip etmeleri için teşvik ediyoruz ve sıklıkla kişisel cihazlarımız ile iş için kullandığımız cihazlar arasında bilgi paylaşıyoruz.

Bilgi yönetimi sadece teknolojik gelişmelerin getirdiği yeniliklere ayak uydurmak ile değil, aynı zamanda bu teknolojileri kullanan insanların davranışları ile de mücadele ediyor. Kısacası şirketlerin bilgiyi korumak için oluşturduğu altyapılar içinde bulunduğumuz zamandan çok, artık var olmayan bir dönem için geçerli.

KASITLI OLMAYAN GÜVENLİK İHLALLERİ

Bilgi güvenliği konusundaki güncel haberler genelde bir hackerın şirketlerin sunucusunu hacklemesi ve şirket sırlarını internet dünyasına açması üzerine yoğunlaşıyor. Bu gibi saldırılar tahrip edici olsa da, dünyada her gün dolaşımda olan bilgi miktarını düşündüğümüzde aslında bu vakalarla çok sık karşılaştığımız söylenemez. Asıl tehlike şirketlerde bilgiye erişimi olan çalışanların kasıtlı ya da kasıtsız davranışlarında yatıyor. İster fotokopi makinesinde kişisel veri içeren bir belgenin unutulması olsun, ister yanlışlıkla tüm e-posta adreslerine gönderilmiş gizli bir stratejik dosya olsun ya da masanın üzerinde duran ve gelecek yılın pazarlama stratejisini içeren bir taşınabilir bellek olsun, çalışanların yaratabileceği sayısız potansiyel veri ihlali durumu söz konusu. Bu durumların çoğunda şansları yaver gidiyor ancak bu ihlaller olumsuz bir sonuç doğurduğunda bireyler ve şirketler için durum içinden çıkılamaz bir hal alabiliyor.

KÖTÜ BİR NİYETİM YOKTU: SIRADAN BİR ÖRNEK

Günlük iş hayatımızdan şu örneğe bir göz atalım:

Yönetici: "Üzerinde çalıştığın pazar analizi raporunu bitirdin mi?"

Çalışan: "Neredeyse bitirdim, bu gece son bir kez kontrol edeceğim."

Yönetici: "Kimseye göndermeden önce benim de kontrol edebilmem için önce bana gönderebilirsen sevinirim."

Çalışan: "Elbette."

Bu gibi bir konuşma ile dünyanın herhangi bir yerindeki ofiste karşılaşabiliriz. İlk bakışta bir yöneticinin çalışanın yaptığı işi kontrol etmesiyle ilgili zararsız bir konuşma gibi görünebilir. Ancak bilgi alışverişini incelemeye başladığınızda riskler de görünür hale gelir.

Bu bilgi akışındaki başlangıç noktası çalışanın hazırladığı rapordur. Çalışan, hassas verilere erişim durumuna göre raporu yazar ve şirketin sistemine kaydeder. Buraya kadar her şey normal görünüyor. Teslim tarihi geldiğinde raporu kişisel bilgisayarına göndermeye karar verir ve son dokunuşları evde yapar. O ana kadar şirketin güvenli sunucularında saklanan bu gizli belge, artık kişisel bir bilgisayarda ve e-posta adresindedir. Daha sonra raporu evden yöneticisinin şahsi e-posta adresine gönderir ve bunu yaparken birkaç farklı iş arkadaşını da kopyalar. O gece iş arkadaşlarından biri şans eseri taksidedir ve telefonunu arka koltukta düşürür. Bu gibi veri ihlalleri olağanüstü görünse de aslında her gün defalarca gerçekleşir. Hepsi de sorumluluk sahibi bir çalışanın elinden geldiğince iyi bir iş çıkarmak istediği içindir. Bu sürece dahil olan herkesin niyeti iyidir, hiç kimse şirkete ya da çalışanlarına zarar vermek istemiyordur. Çalışanlar kasıtlı bir şekilde zarar vermek istemediğinde bu veri ihlalleri gerçekleşiyorsa işin içinde kasıt olduğunda verecekleri zararı siz hayal edin.

FİKRİ MÜLKİYET

Fikri mülkiyet konusunda karşımıza çıkabilecek sorunlardan biri yasaların söylediği ile çalışanların doğru olduğuna inandığı şeyin farklı olmasıdır. Ne kadar çok çalışanın bir sunum, müşteri veri tabanı ya da rapor oluşturduklarında tüm bunlara sahip olduklarını düşündüklerini bilseniz şaşırırdınız.

Aslında yasalara göre tam tersi geçerlidir. Yasalara göre bir çalışan şirket bilgisayarında şirkette olması gereken zaman içinde, şirketin verilerini kullanarak bir belge oluşturduğunda, çalışanın fikri katkısı ne olursa olsun bu belgenin sahibi şirkettir. Yasal açıdan çalışanın katkısı, harcadığı zaman ve kullandığı iş gücüne ödenen maaş ve diğer haklar ile ödenir. Çalışanlar işten ayrıldığında ve ürettikleri belgeleri yanlarında götürdüklerinde bu durum büyük bir sorun olarak karşımıza çıkar. Tüm gizli bilgilerinizin yeni işverenini etkilemek isteyen bir çalışan tarafından rakip firmaya taşındığını düşünün!

Bu sorunlar karşısında alınabilecek aksiyon doğal olarak eğitimdir. Eğer çalışanlar üzerinde çalıştıkları belgelerde hak iddia edemeyeceklerini ve yanlarında götürmeleri halinde yasalara aykırı davrandıklarını bilirlerse, bu durumun haksızlık olduğunu düşünseler de daha az veri ihlaline yol açmaları muhtemeldir.

İŞTEN AYRILMA

İşten ayrılan birisinin genelde içinde kişisel eşyalarını taşıdıkları bir kutu ya da çantayla şirketin güvenlik personeli tarafından şirket dışına kadar eşlik edildiğine çoğumuz şahit olmuşuzdur. Henüz işten ayrılmadan önceki son görüşmelerini yaparken şifreleri ve şirkete giriş için kullandığı kart geçersiz hale getirilir. Üzücü bir durum gibi görünse de tüm bu önlemler zorunluluktan doğmuştur. İster yeni pozisyonlarında ihtiyacı olduğu için olsun isterse ayrıldığı işverenine zarar vermek amacıyla olsun, çalışanların yanlarında şirkete ait gizli bilgileri götürdüğü sayısız örnek vardır. Şirketler hem kendilerini hem de hissedarlarını korumak zorundadır.

SIK İŞ DEĞİŞTİREN KİŞİLERİN İK PERSONELİ AÇISINDAN YARATTIĞI OLUMSUZ SONUÇLAR

Tek bir işte uzun süre çalışmak eskide kaldı. Özellikle 20'li ve 30'lu yaşlarındaki çalışanlar, kariyer merdivenlerini tırmanırken genelde her iki üç yılda bir şirket değiştirirler. Bu sık iş değiştiren personelin şirketin sahip olduğu veriler açısından iki temel sorunu vardır. Birincisi bu kişilerin iş değiştirirken yanlarında şirkete ait gizli bilgileri götürmemelerini sağlamaktır. Şirketler bu veri ihlalinin önüne geçmek için çalışanın işten ayrılma şartlarına göre atılacak adımları belirlemişlerdir. İkinci sorun ise şirketin çalışan hakkında ellerinde tuttuğu kişisel verilerle ilgilidir. Bunlar özlük dosyaları, performans görüşmeleri, sağlık raporları ya da şirketlerin kayıtlarındaki farklı veriler olabilir. Çalışan işten ayrıldığında İK ve BT yöneticileri yasal zorunluluklar çerçevesinde doğru adımların atıldığından, bu verilerin gerekli sürelerde saklandığından ya da zamanında doğru yöntemlerle imha edildiğinden emin olmalıdırlar. Böyle bir durumda izlenecek süreçleri henüz belirlemediyseniz, en kısa zamanda belirlemeniz gerekir.

Şirketler çalışanlarının veriye olan erişimlerini ne ölçüde kısıtlamalı? Elbette çalışanların işlerini verimli bir şekilde yapabilmeleri için veriye ihtiyaçları var. Şirketler çalışanların gerekli veriye erişimini sağlarken, kendilerine rekabet avantajı sağlayan veriler ile özellikle müşteri veri tabanı ya da çalışanlara ait kişisel veriler gibi yasalarla korunması zorunlu kılınan verileri güvende tutmalıdır.

İdeal olan, her bir çalışanın işini en iyi seviyede yapabilmesi için gerekli verilere erişebilmesi ve bu verilerin sadece bu amaç için kullanıldığından emin olunmasıdır. Bu hedefe ulaşmak için şirketler şu adımları izleyebilirler:

1. Çalışanlarınızı Eğitin

Birçok çalışan veri ihlaline yol açacağını bilmeden hareket eder. Kendi başlarına asla gelmeyeceğini düşünürler. Çalışanlarınızı erişebildikleri veri hakkında eğitin, onlara bu verileri korumaktan sorumlu olduklarını anlatın. Çalışanlar gizli bir belgeyi kişisel bilgisayarlarına kopyalamanın neden sakıncalı olabileceğini anlarlarsa, bunu yapmaktan daha fazla kaçınacaklardır.

2. Daha Gerçekçi Bilgi Politikaları Oluşturun

Şirketler çalışanlarının işlerini iyi bir şekilde yapmalarına yardımcı olan bilgiyi korumak amacıyla gerçekçi politikalar oluşturmalıdır. Aksi takdirde çalışanlar iş dünyasının gerçekliğinden uzak bu politikaları takip etmemeyi tercih edeceklerdir.

3. Tüm Platformlardaki Bilgilerinizi Koruyun

Bu maddeyi en sona koymamızın sebebi, teknolojiye sığınmanın atılan ilk adım olması. Çalışanlar daha güvenli bir sistemin her sorunu çözdüğüne, kendilerinin bir şey yapmasına gerek olmadığına inanır. Ancak durum tam olarak öyle değildir. Yine de şirketlerin kullandıkları tüm platformlarda bilginin güvenliğini sağlaması, sistemlerinin güvenli ve güncel olduğundan emin olması gerekir.

SONUÇ

Çalışanların bilgi güvenliğinden haberdar olduğu ve erişebildikleri verilere saygı duyduğu bir ortam yaratmak zaman alır. Ayrıca üst yönetimin bu konu üzerinde yoğunlaşmasını gerektirir. Birçok şirket bu süreçte kendilerine yardımcı olması için üçüncü taraflarla işbirliği yapar. Iron Mountain olarak Fortune 1000 listesinin %95'ini oluşturan büyük şirketlerden, küçük ve orta ölçekli şirketlere kadar dünyada 230.000'den fazla Türkiye'de 1500'den fazla müşterimizin belgelerini yönetiyor ve güvenli tesislerimizde saklıyoruz.

Size nasıl yardımcı olabiliriz? Danışmanlarımızla ihtiyaçlarınıza özel toplantı organize etmek için bizimle iletişime geçin.

+90 212 288 95 03 | IRONMOUNTAIN.COM.TR

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.