Kron
www.kron.com.tr

KRON
HIGHLIGHTS

HAZİRAN, 2021

Kron
www.kron.com.tr

İçindekiler

Siber Güvenlikte İç Tehditler: Nedir? Türleri Nelerdir?

İş dünyasının yaşadığı dijital dönüşüm sürecinde şirketlerin karşılaştığı en önemli sorunların başında iç tehditlerin neden olduğu veri ihlalleri geliyor. Veri güvenliği ve siber güvenlik sistemlerindeki çeşitli açıklar ya da bilinçli/bilinçsiz insan hatalarından kaynaklı olarak meydana gelen ihlaller özellikle şirketlere ait kritik veri yığınlarının korunmasını önemli ölçüde zorlaştırıyor. Bu nedenle şirket içi erişim yönetimini eksiksiz şekilde yapılandırmanız gerekiyor.

Siber Güvenlik Alanındaki Tehditler

Şirketlerin siber güvenlik alanında karşılaştığı birçok farklı tehdit mevcut. Ransomware (Fidye yazılım), malware (kötü amaçlı yazılım), sosyal mühendislik çalışmaları ve phishing (oltalama) veri güvenliğini tehdit eden başlıca unsurlar arasında yer alıyor. Öte yandan uzaktan erişim sırasında yaşanabilecek ihlaller ve insan kaynaklı hatalar da siber güvenlikte karşılaşılan önemli veri ihlali türlerinden bazıları.

İlgili alandaki dikkat çeken güvenlik sorunlarından birini de iç tehditler (insider threats) oluşturuyor. Birçok farklı sektör için veri ve erişim güvenliği açısından ciddi bir problem konumundaki iç tehditler, siber saldırı yapılması planlanan şirketten kaynaklanan güvenlik riskleri olarak

tanımlanabilir. Bir başka deyişle iç tehditler, şirketlerin kritik verilerine erişim yetkisi olan kişilerin söz konusu yetkileri kasıtlı ya da kasıtsız biçimde kötüye kullanmasıyla ortaya çıkan siber güvenlik sorunları şeklinde de ifade edilebilir.

İç tehdidin kaynağının hâlihazırda şirketinizde çalışan bir profesyonel olması gerekmiyor. Mevcut çalışanlarınızdan kaynaklı veri ihlalleri yaşayabileceğinizi gibi, eski çalışan, iş ortağı, yönetim kurulu üyesi ve size danışmanlık hizmeti veren profesyoneller de iç tehdit yaratarak başınızı derde sokabilir. Tam da bu sebeple aktif şekilde kurumsal iletişimde olup olmadığınız fark etmeksizin, şirketiniz ile bağlantılı tüm profesyonellerin erişebildikleri verilerin sınırlarını ve erişebilme yöntemlerini birkaç farklı adımdan oluşan önlemler ile kontrol altında tutmanız öneriliyor.

İç Tehditler (Insider Threats) ve Türleri

Çalışanlarınız ya da profesyonel bağlamda ilişki kurduğunuz kişilerin dışında, şirket verilerinize doğrudan erişim yetkisine sahip olan bir kişi de iç tehdit unsuru kabul ediliyor. Yine iş modeliniz gereği iletişimde olduğunuz tedarikçi ve satıcılar da iç tehdit yaratabilecek önemli kaynaklar arasında dikkat çekiyor.

İç tehditler motivasyon, farkındalık, erişim düzeyi ve niyet açısından farklı gruplara ayrılıyor. IBM'in yapmış olduğu çalışma ile Ponemon Enstitüsü iç tehditleri ihmalkâr, suçlu ve kimlik bilgisi hırsızlığı kavramlarını kullanarak tanımlıyor. Gartner ise iç tehditleri dört farklı grup altında ele almayı tercih ediyor. Gartner'a göre iç tehditler piyonlar, kolaya kaçanlar, iş birlikçiler ve yalnız kurtlardan oluşuyor. Bu arada Ponemon Enstitüsü ve Gartner'ın bağımsız kuruluşlar olduğunu ve farklı alanlarda hazırladıkları raporları devlet kurumlarına sunduklarını belirtmekte de yarar var

Piyonlar

İç tehdit gruplarının ilk ayağını oluşturan piyonlar, farkında olmadan veri ihlaline sebep olabilecek, kötü niyetli faaliyetlerde bulunmak üzere manipüle edilen şirket çalışanlarını kapsıyor. Piyonlar kötü amaçlı yazılımlar indirerek şirketinizin veri güvenliğine zarar verebileceği gibi, kimlik avı ve sosyal mühendislik saldırıları sonucunda da kimlik bilgilerini ifşa edebilir. Her iki yöntem de siber saldırgan ve piyonlar arasındaki ilişkinin zeminini inşa ediyor. Piyonlar genelde bilişim ve finans sektöründe iç tehditler kategorisinde öne çıkıyor.

Kolaya Kaçanlar

Önemli bir iç tehdit unsuru konumundaki kolaya kaçanlar, şirket içi veri güvenliği politikalarından muaf olduklarını düşünüyor. Cahil ya da kibirli olarak tanımlanabilecek ilgili grubun iç tehdit yaratmasının temel nedeni ise kolaya kaçmaları veya yetersizlik nedeniyle güvenlik protokollerini atlamaya çalışmaları. Bunun sonucunda şirket içi veriler savunmasız ve saldırıya açık hâle geliyor.

Donanım eksiklikleri sebebiyle bu grup, büyük oranda dünya genelindeki kamu alanında yer alan iç tehditler başlığı altında karşılaşılıyor.

İş Birlikçiler

Siber suç işlemek için şirketinizin rakipleri ya da yabancı devletler ile iş birliği yapan çalışanlara iş birlikçiler ismi veriliyor. İş birlikçiler şirket içi ayrıcalıklı erişimlerini çoğunlukla fikri mülkiyet ve müşteri bilgilerini çalmak amacıyla kullanıyor. Ayrıca söz konusu grup, ortaklık kurduğu şirket/devlet çıkarı ya da kendi kişisel kazancı için şirket operasyonlarında bilinçli kesintilere de neden oluyor. İş birlikçilere finans sektöründe sıkça rastlamak mümkün.

Yalnız Kurtlar

Yalnız kurtlar, özellikle ağ ya da veri tabanı yöneticisi gibi yüksek erişim ayrıcalığına sahip kişiler ise bir hayli tehlikeli olabilir. Doğrudan finansal kazanç için manipüle edilmesine gerek kalmadan kötü niyetli davranışlar sergileyen yalnız kurtları, kişisel sağlık verilerini satmak amacı da güdebilmeleri sebebiyle, sağlık sektöründe iç tehditler konulu araştırmalarda bol bol görebilirsiniz.

İç Tehdit Göstergeleri (Indicators)

Şirketinizde ortaya çıkabilecek iç tehditlerin göstergeleri, dijital ve davranışsal olmak üzere iki farklı başlık altında inceleniyor:

Dijital Göstergeler

- Önemli miktarda veri indirme ve veri erişimi
- İş tanımları dışındaki hassas verilere erişim
- Davranış profillerinin dışında kalan verilere erişim
- Şirket içi görevleri dışındaki kaynaklara erişim için birden çok istek
- Yetkisiz depolama aygıtlarının kullanılması
- Ağ taraması
- Veri istifleme
- Hassas verileri şirket dışı bir ağa e-posta ile gönderme

Davranışsal Göstergeler

- Güvenlik protokollerini atlama girişimleri
- Mesai saatleri dışında sık sık ofiste kalma
- Meslektaşlarına karşı olumsuz davranışlar
- Kurumsal politikaların ihlali
- İstifa ve yeni iş fırsatlarına yönelik tartışmalar

Örneğin bir çalışanınız yetkisi dışındaki verilere erişim için yönetici onayı almaya çalışıyorsa ya da erişim yetkisine sahip olduğu verileri istiflemeye veya şirket dışı bir ağa e-posta aracılığıyla gönderme girişimlerinde bulunuyorsa bir iç tehditten bahsetmek pekala mümkün.

Nitekim IBM tarafından yayımlanan “Cost of Insider Threats: Global Report 2020” isimli rapora göre iç tehditlerden kaynaklanan veri ihlali sıklığı 2016’dan bu yana üç kat arttı. Ayrıca 2019’da iç tehditlerin gerçekleştirdiği sızıntılardan meydana gelen ortalama zarar 493.093 $’dan 871.686 $’a yükseldi.

204 farklı şirkette, 964 IT departmanı çalışanı üzerinde gerçekleştirilen araştırma, raporlanan 4716 ihlalin 2962'sinin ihmalkârlık veya kasıtsız eylem nedeniyle oluştuğunu ortaya koyuyor. Yine aynı araştırma 1105 ihlalin doğrudan kötü niyetli veri ihlali girişimleri ile olduğunu belirtirken 649 olayda kimlik bilgilerinin çalındığını gösteriyor. Ayrıca 191 olayda ise ayrıcalıklı erişime sahip kullanıcıların kimlik bilgilerinin çalındığı, raporda yer alan bir diğer önemli konu.

Raporda siber güvenlikte iç tehdit sorununun %63 ihmallerden, %23 şirket çalışanlarının kasıtlı zarar verme girişimlerinden ve %14 kullanıcıların kimlik bilgilerinin manipüle edilmesi ve çalınmasından kaynaklandığı aktarılıyor.

Hassas veriler ve siber güvenlik uygulamaları söz konusu olduğunda şirketinizde tehdit analizi yaparak iç ve dış tehditlerin belirlenmesini sağlamanız gerekiyor. IBM tarafından yapılan araştırmanın da gösterdiği gibi, yetkili hesapların denetlenmesi, kontrolü ve yönetimi şirketler açısından oldukça önem taşıyor. Bu aşamada Ayrıcalıklı Erişim Yönetimi (Privileged Access Management - PAM) uygulamaları iç tehditleri azaltmanızda önemli görevler üstleniyor. Yetkili oturumları kayıt altına alarak raporlama yapabilmenizi sağlayacak Yetkili Oturum Yöneticisi, çalışanlar arasında şifre paylaşımını ortadan kaldırarak şifre kasası özelliği bulunan Merkezi Parola Yönetimi, tek kullanımlık parolalar üreterek coğrafi konum doğrulama (geo-location) özelliği bulunan İki Faktörlü Kimlik Doğrulama (2FA) gibi ürünler iç tehditleri bertaraf etmenize yardımcı olacaktır.

Alanında uzman ve deneyimli ekibimiz ile Ayrıcalıklı Erişim Yönetimi (PAM) alanında geliştirdiğimiz platformumuz **Single Connect**, Gartner tarafından hazırlanan ve en iyi PAM uygulamalarının iş dünyasıyla paylaşıldığı Magic Quadrant for Privileged Access Management **raporunda** da yer alarak dünyanın önde gelen Ayrıcalıklı Erişim Yönetimi sistemlerinden biri olduğunu kanıtlıyor.

İç tehditleri azaltmaya yönelik yapısı ve üst düzey güvenlik sunan modülleri ile uçtan uca veri güvenliği sağlayan Ayrıcalıklı Erişim Yönetimi (PAM) yaklaşımını kullanarak iç tehditlere karşı nasıl önlem alabileceğinizi bir sonraki yazımızda ele alacağız.

Siz de Single Connect hakkında merak ettiklerinizi öğrenmek için bizimle irtibata **geçebilirsiniz.** Ayrıca düzenli olarak güncellediğimiz, güncel içeriklere sahip **Kron Blog** üzerinden siber güvenlik ile ilgili farklı bilgilere de ulaşabilirsiniz.

Güvenli Uzaktan Erişim Nasıl Sağlanır?

COVID-19 pandemisinin yarattığı uzaktan çalışma koşulları ile birlikte güvenli uzaktan erişim, şirketler için vazgeçilmez bir hale geldi. Bugün küresel ve ulusal şirketlerin büyük bölümü uzaktan çalışma programları inşa ediyor ve çalışanlarının mesai saatlerini ilgili programlara göre düzenliyor. Fakat teknolojik gelişmelerle doğru orantılı şekilde siber tehditlerin de arttığı düşünüldüğünde uzaktan erişim işleyişini güvenli kılmak her zamankinden daha büyük önem taşıyor.

Zira iş dünyasındaki profesyoneller evlerinden uzaktan erişim yoluyla çalışmaya devam ettiği sürece siber tehditlerle karşılaşma olasılıkları artıyor. Bu nedenle veri güvenliği çözümlerine önem vererek uzaktan erişim riskleri ile ilgili karşınıza çıkabilecek tüm senaryolara hazır olmanız gerekiyor. Hazırlık sürecini ve alacağınız güvenlik önlemlerini başarıyla şekillendirmek için de öncelikle güvenli uzaktan erişim tanımına ve kapsamına sorunsuz biçimde hâkim olmalısınız.

Güvenli Uzaktan Erişim Nasıl Sağlanır?

Şirket çalışanlarının normal şartlarda ofis ortamında yaptığı elektronik işlemlerin çeşitli dijital yöntemler ve bulut bilişim aracılığıyla ofis dışı alanlarda gerçekleştirilmesi uzaktan erişimin en yalın tanımı olarak ifade edilebilir.

Profesyonellere ve kurumlara önemli ölçüde esneklik vadeden uzaktan erişim, maliyet tasarrufu açısından da son derece yararlı. COVID-19 pandemisiyle iş dünyasında çalışma düzenlerinin geçirdiği dönüşümün temelinde de uzaktan erişim uygulamaları yatıyor.

Nitekim uzaktan erişim uygulamalarının yaygınlaşması sonucunda güvenlik riskleri de artıyor. Uzaktan çalışan insanlar kişisel elektronik aygıtları üzerinde yerel yönetici haklarına sahip olup şirket verilerine bu yolla erişim sağlıyorlar. Kişisel cihazlar aracılığıyla gerçekleştirilen uzaktan erişimin geleneksel ofis tabanlı işleyişlerden daha az risk içermesi ise teknik olarak pek mümkün olmuyor.

Bir şirket çalışanı uzaktan erişim uygulamalarını kullanırken farkında olmadan ağ üzerinde çeşitli hatalar yapabilir. Şifreleme erişimi ve düzenlemesi ile ilgili aksaklıklar meydana gelebileceği gibi, onaylanmamış uygulamaların indirilmesi sonucu veri ihlalleri de ortaya çıkabilir. Ayrıca iş birliği içinde olduğunuz uygulamalar aracılığıyla yapılan güvenli olmayan veri paylaşımları da uzaktan erişim yöntemi sırasında karşılaşabileceğiniz güvenlik riskleri arasında yer alıyor.

Uzaktan Erişim İhlalleri Nasıl Önlenir?

Verizon tarafından yayımlanan **"Mobile Security Index 2021"** raporuna göre COVID-19 pandemisinin bir sonucu olarak iş dünyasının %79'unun uzaktan erişim kullanımında artış gözlendi. Aynı rapora göre çalışanların %97'si uzaktan erişim yöntemi ile çalışmanın geleneksel ofis ortamına nazaran daha fazla risk içerdiği görüşünde birleşmiş durumda.

Araştırma günümüzde çalışanların %50'sinin iş hesaplarına erişim için şifrelerini iş arkadaşlarıyla paylaştığını ortaya koyuyor. Yine çalışanların %49'u iş için kullandıkları cihazları aileleri ve arkadaşlarına da veriyor. Üstelik bu çalışma şu an internet dünyasındaki her 25 uygulamadan birinin kimlik bilgilerini sızdırdığı sonucuna da ulaşıyor

Mobile Security Index araştırmasının da gösterdiği üzere, aslında profesyoneller uzaktan erişim güvenliği konusunda çeşitli endişeler taşıyor. Söz konusu endişeleri ortadan kaldırmak, bir başka deyişle, uzaktan erişim sonucu oluşabilecek veri ihlali riskini en aza indirmek bir dizi siber güvenlik önlemi almaktan geçiyor.

Öncelikle güvenli uzaktan erişimin çok sayıda güvenlik çözümünden oluştuğunun altını çizmek gerekiyor. Bunlardan ilki VPN (Virtual Private Network) kullanımı. Özel bir ağa bağlanmak amacıyla şifreli tüneller kullanan VPN yönteminin çeşitli güvenlik risklerini de bünyesinde barındırdığını unutmamalısınız. Tek başına yeterli bir güvenlik yöntemi olmayan VPN uygulamaları, İki Faktörlü Kimlik Doğrulama (Two-Factor Authentication – 2FA) uygulamaları veya parola yönetimi uygulamaları gibi güvenlik yöntemleriyle desteklenebilir. Bunlara ek olarak kullanıcılara, ağa yerleştirmeden ve uygulamaları internet

erişimine açmadan erişim kontrol politikalarını baz alan ve güvenli bağlantı sağlayan Zero Trust Network Access (ZTNA) de uzaktan erişim güvenliğini sağlamak gayesiyle tercih edilen yöntemlerden biri olabilir.

Tüm bunların yanı sıra üçüncü taraf erişimi (Third party access), Endpoint Security ve Network Access Control (NAC) de uzaktan erişim ile güvenli çalışma olanağı sunuyor. Fakat özellikle VPN ve üçüncü taraf erişimi, çeşitli veri güvenliği zafiyetlerine sahip oldukları için söz konusu yöntemleri mutlaka Ayrıcalıklı Erişim Yönetimi (Privileged Access Management – PAM) çatısı altında yapılandırmanız öneriliyor. Bugün dünya üzerindeki şirketlerin sadece %34'ünün üçüncü taraf kullanıcılar ile ilişkilendirilebilecek oturum açma ve erişim sayısını bildiği düşünüldüğünde uzaktan erişimi güvenli kılmanın en işlevsel yolu olan PAM'in ortaya koyduğu ayrıcalıklar çok daha değerli hale geliyor.

Ayrıcalıklı Erişim Yönetimi (PAM) ve Güvenli Uzaktan Erişim

Phishing (oltalama) saldırılarının oranının 2019'a kıyasla 2020'de %364 arttığı dijital ortamda güçlü bir PAM stratejisinin fonksiyonel avantajlarından yararlanmaya çalışmalısınız. Ayrıcalık Erişim Yönetimi, ele geçirilmesi kurumsal ağa ciddi zararlar verebilecek ayrıcalıklı hesaplara odaklanıyor. Yetkilendirilmiş hesaplar uzaktan erişim sırasında bir bilgisayar korsanının hedef tahtasına koyduğu en değerli varlıklar arasında bulunuyor. Bu nedenle ağ içinde ayrıcalıklı hesapların güvenliğinin sağlanması için ek önlemler almanız son derece mühim.

PAM çözümleri şüpheli etkinliklerin gerçek zamanlı tespitini mümkün kıldığı gibi, kimlik bilgilerine erişimi sınırlandırarak yazılım ve donanımın kötüye kullanılmasının önüne geçiyor. Ayrıcalıklı erişim talebi için eş zamanlı olarak konum ve zaman bilgisi talep eden PAM, bağlam analizi ve örüntü tanımlama yoluyla sistemdeki veri ihlali girişimlerini tespit edebiliyor.

Ayrıca PAM'in gerçek zamanlı şekilde çalışması uzaktan erişimin işleyişi ile de benzerlik gösteriyor. PAM ağ yapısında çalışmaya devam ettiği için uzaktan erişim sırasında karşılaşabileceğiniz veri ihlallerini tespit etmek kolaylaşıyor. Bunların yanı sıra PAM'in rutin görevleri otomatik hale getiren Ayrıcalıklı Görev Otomasyonu (PTA), yetkili hesapların oturumlarını kontrol eden Yetkili Oturum Yöneticisi, zaman ve konum bazlı sınırlamalar getirebilen İki Faktörlü Kimlik Doğrulama (2FA), şifre kasası özelliği barındıran Merkezi Parola Yönetimi (Dynamic Password Controller) ve oturumları kayıt altına alma ve maskeleme özelliği sunan Dinamik Veri Maskeleme özelliklerine sahip olması sistemin verimliliğini hatırı sayılır seviyede artırıyor

Ayrıcalıklı Erişim Yönetimi ürünümüz **Single Connect** güvenli uzaktan erişim için ihtiyaç duyduğunuz uçtan uca tüm özellikleri sizinle paylaşıyor. Gartner Magic Quadrant for Privileged

Access Management raporunda da yer alarak siber güvenlik alanında sunduğu üst düzey özellikleri kanıtlayan platformumuz kullanıcılardan **tam not alıyor.**

Dijital dünyanın önde gelen PAM platformlarından biri olan ve sorunsuz şekilde güvenli uzaktan erişim olanağı yaratan Single Connect altı modüle sahip: Yetkili Oturum Yöneticisi, Merkezi Parola Yönetimi, İki Faktörlü Kimlik Doğrulama (2FA), Dinamik Veri Maskeleme, Ayrıcalıklı Görev Otomasyonu (PTA) ve TACACS+ / RADIUS Erişim Yönetimi.

Tüm bu veriler ışığında uzaktan erişim güvenliğini üst seviyede tutmak amacıyla **Single Connect** ürünümüzü kullanmak için bizimle iletişime **geçebilirsiniz.** Ayrıcalıklı Erişim Yönetimi'nin tüm avantajlarını sunan Single Connect ile uzaktan erişimi güvence altına alabilir, böylece hem yetkili hesapların hem de şirketinizin veri güvenliği sorunları yaşamasını önleyebilirsiniz.

Veri İhlallerinde İnsan Kaynaklı Hataları Önlemenin Yolları

Veri ihlali, enformasyon yığınları üzerinden şekillenen dijital iş dünyasının en önemli sorunlarından biri. İnsan kaynaklı hatalar (human error) ise veri güvenliği ihlallerinin yaşanmasının başlıca nedenleri arasında yer alıyor.

Şirketinizde çalışan profesyonellerin dijital ortamda yaptıkları ya da yapmadıkları hareketlerden kaynaklanan insan kaynaklı veri ihlalleri, iş sürekliliğinin aksamasına ve şirketinizin mali kayıplar yaşamasına neden olabiliyor.

İnsan kaynaklı hatalar nedeniyle ortaya çıkabilecek veri ihlallerinin önüne geçmek ve muhtemel zararları en aza indirmek için önce hatanın kaynağına ve nedenlerine inmeniz gerekiyor.

Veri İhlali ve İnsan Kaynaklı Hatalar

Siber güvenlik alanında insan kaynaklı hatalar, şirket çalışanları ya da kullanıcılar tarafından yapılan ve hem güvenlik ihlali ortaya çıkmasına hem de söz konusu ihlalin yayılmasına neden olan kasıtsız yanlış eylemler ve eylem eksiklikleri anlamına geliyor.

Amerika Birleşik Devletleri'nde Stanford Üniversitesi ve siber güvenlik firması Tessian'daki araştırmacılar tarafından yapılan çalışmaya göre

2021'deki veri ihlallerinin yaklaşık %88'i insan kaynaklı hatalardan oluşuyor. Araştırmanın ortaya koyduğu sonuç gösteriyor ki otomasyon sistemlerinin oldukça geliştiği 21. yüzyılın üçüncü on yıllık döneminde bile kullanıcıların çevrim içi hatalı faaliyetleri majör siber güvenlik sorun ve sızıntılarının ardındaki itici güç olmaya devam ediyor.

İnsan Kaynaklı Hataların Kaynağı: Yetenek ve Karar Mekanizması

Her şeyden önce insan kaynaklı oluşabilecek hataların herhangi bir sınırı olduğunu unutmamalısınız. Araştırmaların gösterdiği sonuçlar baz alınarak oluşturulan veri güvenliği literatürüne bakıldığında hataların kaynağında iki ayrı grup göze çarpıyor. Yetenek tabanlı hatalar ve karar mekanizması tabanlı hatalar, insanların neden olduğu veri ihlali türlerinin kaynağını meydana getirirken iki grup arasındaki fark ise kullanıcının doğru eylemi yapabilmek için gerekli donanıma sahip olup olmaması şeklinde tanımlanıyor.

- **Yetenek Tabanlı Hatalar**

Yeteneğe dayalı insan hatası kaymalardan ve atlamalardan oluşuyor. Şirket çalışanınızın aşina olduğu bir görev ya da etkinlik sırasında yaptığı küçük yanlışları işaret eden yetenek tabanlı hatalarda genelde gecikme ve ihmal, sorunun kaynağında yatan nedenler oluyor. Söz konusu senaryoda çalışanınızın doğru hareket tarzını bildiği hâlde bunu eyleme dönüştürememesi ise yorgunluk, dikkat eksikliği, yoğunluk ve motivasyon kaybı gibi nedenlere bağlanıyor.

- **Karara Dayalı Hatalar**

Şirket çalışanınızın hatalı karar vermesini içeren ilgili türde birçok farklı neden ön plana çıkıyor. Kullanıcının kararı alacak bilgi birikimine sahip olmaması, karşılaştığı özel duruma yönelik donanımının yetersiz olması ya da sorumluluk almaktan kaçınarak eylemsizliği tercih etmesi karara dayalı hatalara zemin hazırlıyor.

Çalışanlarınızın siber güvenlik farkındalığını artıracak otomasyonlardan yararlanarak ve onları güvenli eylemlere yönlendirerek insan kaynaklı hataları azaltabilirsiniz.

İnsan Hatasının Psikolojisi

"Psychology of Human Error" isimli çalışma, soruşturma ve yargı süreci ile karşı karşıya kalınması durumunda şirket çalışanlarının önemli bölümünün hata yaptıklarını reddetme eğiliminde olduklarını ortaya koyuyor. Yine aynı çalışmaya göre çalışanların %50'si şirket verilerinin güvenliğini tehlikeye atabilecek bir hata yaptıklarından son derece emin olduklarını belirtiyor.

Öte yandan çalışanların yaş dağılımı da insan kaynaklı hataların yönetimi açısından bir hayli mühim. Söz konusu çalışmaya göre genç çalışanlar hata yaptıklarını kabul etmeye beş kat daha fazla meyilli. 18-30 yaş arası çalışanların

%50'si hata yaptığını kabul ederken 51 yaş üstü çalışanların sadece %10'u hata yaptığını kabul ediyor.

Aynı çalışmanın ortaya koyduğu üzere, şirket çalışanlarının %25'i bir phishing e-postasına tıklıyor. Erkek çalışanların %34'ü kimlik avı saldırısı için düzenlenen e-postaları açarken kadın çalışanlarda ise bu oran %17. Phishing e-postalarına tıklama konusunda da yaş önemli bir faktör olarak dikkat çekiyor. Araştırmaya katılan örneklemdeki 51 yaş üstü çalışanların %8'i phishing e-postalarını açarken 31-40 yaş aralığındaki çalışanların %32'si ilgili e-postaları açıyor.

Söz konusu sonuçları göz önüne aldığınızda şirketinize ait verileri başarılı şekilde koruyacak bir siber güvenlik çözümüne başvurmanız oldukça önemli hâle geliyor. Privileged Access Management (PAM), Türkçe karşılığıyla Ayrıcalıklı Erişim Yönetimi, insan kaynaklı hatalara çözüm getirmeniz için uygulayabileceğiniz başlıca yöntemler arasında bulunuyor.

PAM ile İnsan Kaynaklı Hataları Önlemek

Siber suçlular, şirketinize ait verileri ele geçirmek için öncelikle verileriniz ile bağlantıya sahip yetkilendirilmiş hesapları ele geçirmeye çalışıyor. PAM tam da bu noktada devreye girerek ağ üzerinde verilerinize ulaşma yetkisine sahip ayrıcalıklı kullanıcıların bilgilerini izole ederek, çok katmalı güvenlik uygulamalarıyla üst düzey koruma sağlıyor. Böylece ilgili kullanıcı hesapları, daima kontrol altında oluyor. Bu da yetki sahibi kullanıcıların yapabileceği insan kaynaklı hataların önüne geçilmesini ve çalışanların sıkı bir denetime tabi tutulmasını kolaylaştırıyor. PAM'in temel bileşenleri arasında yer alan dört özellik ise insan kaynaklı hatalar nedeniyle veri güvenliği ihlali yaşanmasını önlüyor.

- **Ayrıcalıklı Görev Otomasyonu (Privileged Task Automation)**

PTA, kullanıcıların yapacağı rutin görevleri otomatik hâle getirerek servis kesintilerini, gecikmeleri ve güvenlik ihlallerini ortadan kaldırıyor.

- **Merkezi Parola Yönetimi (Dynamic Password Controller)**

İlgili özellik ağınızdaki tüm yetkili oturumları doğruluyor ve tamamı şifrelenmiş bir altyapı ortaya koyuyor. Ek olarak şifre kasası fonksiyonuna da sahip olan özellik sayesinde yetkili kullanıcıların şifrelerinin paylaşılması ve siber suçluların eline geçmesi engelleniyor.

- **İki Faktörlü Kimlik Doğrulama (Two-Factor Authentication - 2FA)**

2FA, standart doğrulama sistemlerinden farklı şekilde, ayrıcalıklı erişim talebi için zaman ve konum doğrulaması da talep ediyor. Böylece erişim talep eden kullanıcıların kimliği güvenli biçimde doğrulanıyor, kötü niyetli girişimler 9reddediliyor.

- **Dinamik Veri Maskeleme (Dynamic Data Masking)**

Bu özellik ayrıcalık sahibi yetkili hesapların ve ağ yöneticilerinin sistemde yaptığı tüm işlemleri kaydedip maskeliyor. Bu sayede ağ üzerindeki hareketlerle ilgili herhangi bir soru işareti oluşmuyor.

Tüm bunlara ek olarak insan kaynaklı hataları önlemenin yolları arasında Ayrıcalıklı Erişim Yönetimi uygulamalarıyla ilişkili olan **Sıfır Güven (Zero-Trust)** ve **En Az Ayrıcalık İlkesi (Least Privilege)** yöntemlerinden bahsetmek de mümkün. Sıfır Güven (Zero-Trust) prensibi "Asla güvenme, her zaman doğrula" ilkesini esas alıyor. Buna göre şirketler ağ içi ve dışı hiçbir dijital kimliğe güvenmeyerek erişim izni talep eden herkesi kapsamlı güvenlik taramasından geçiriyor. Zero-Trust ilkesi, PAM'in ayrıcalıklı erişim iznini denetleyen yapısıyla entegre şekilde kullanıldığında ortaya harika sonuçlar çıkıyor.

En Az Ayrıcalık İlkesi (PoLP) ise veriye ulaşmak için farklı seviyede profiller oluşturma prensibine dayanıyor. Farklı kullanıcıların farklı düzeyde erişim hakkına sahip olduğu yöntemde veriyi koruma amacından hareketle tüm ağ erişimleri için özel izin talep ediliyor. PoLP ve PAM'in birlikte kullanımı çok yönlü bir siber güvenlik çözümüne sahip olmanızı kolaylaştırıyor.

Ayrıcalıklı Erişim Yönetimi (PAM) ürünümüz Single Connect, yukarıdaki dört modülün yanı sıra Yetkili Oturum Yöneticisi (Privileged Session Manager) ve TACACS+ / RADIUS Erişim Yönetimi (Unified Access Manager) modüllerini de bünyesinde barındırıyor.

İnsan kaynaklı veri ihlallerini engellemek için uçtan uca güvenlik sağlayan kapsamlı PAM ürünümüz **Single Connect** ile şirket verilerinizi güvence altına alabilir ve sadece belirli kullanıcılara ayrıcalıklı erişim imkânı sunabilirsiniz.

Siz de **Single Connect** ürünümüz hakkında merak ettiklerinizi öğrenmek ve gelişmiş bir siber güvenlik çözümüne sahip olmak için bizimle iletişime **geçebilirsiniz.** Ayrıca **Kron Blog**'u takip ederek veri güvenliği konusundaki güncel ve detaylı içeriklere ulaşabilirsiniz.

Verizon DBIR 2021: Fidye Yazılımları, Phishing, İnsan Kaynaklı Hatalar ve Dahası

Siber güvenlik tehditleri, 21. yüzyıl iş dünyasının en önemli sorunlarından biri. Özellikle dijitalleşmenin inanılmaz boyutlara ulaştığı yakın dönemde fidye yazılımları (ransomware), phishing (oltalama) ve sosyal mühendislik kaynaklı çeşitli veri ihlalleri büyük bir artış eğilimi içinde. Nitekim siber güvenlik alanında her yıl Verizon tarafından yayımlanan Data Breach Investigations Report 2021'de veri ihlali konusunda yaşanan artışı net şekilde ortaya koyuyor.

Verizon DBIR 2021 raporunda farklı türdeki siber güvenlik ihlallerine yönelik yapılan kapsamlı araştırmaların sonuçları yer alıyor. Rapora göre fidye yazılımları ve phishing saldırıları sonucu oluşan veri ihlalinde yüksek seviyede artış gözleniyor. Diğer taraftan insan kaynaklı hatalarda ise %5'lik düşüş söz konusu iken veri ihlallerinin %85'inin insan kaynaklı hatalar sebebiyle gerçekleştiği ortaya çıkıyor. Ayrıca şirketinize ya da size ait verileri çalmak, manipüle etmek ve ortadan kaldırmak amacıyla yapılan saldırılar artık sadece kimlik bilgileri (credentials) üzerine değil, kişisel bilgiler üzerine de yoğunlaşıyor.

Verizon DBIR 2021: Artış Oranları ve Önemli Çıkarımlar

Verizon Data Breach Investigations Report 2021, 79.000'den fazla güvenlik olayının detaylı şekilde

incelenmesiyle hazırlandı. Raporda aktarılan verilere göre incelenen 79.000'den fazla güvenlik olayında doğrulanmış 5258 veri ihlali vakası tespit edildi. Tespit edilen vakalar ise ağırlıklı olarak ransomware, phishing, sosyal mühendislik ve credentials saldırılarından kaynaklı.

1. **Fidye yazılımları (ransomware):** Raporda fidye yazılımı saldırılarının geçen yıla kıyasla %10 civarı artış gösterdiği belirtiliyor. %10'luk artış, tüm ihlal türleri içinde ransomware saldırılarını üçüncü sıraya yükseltirken rapora göre saldırganların yöntem değişiklikleri ve yeni taktikleri de oldukça dikkat çekici.

2. Phishing (oltalama) ve sosyal mühendislik: Phishing saldırılarının oranı geçen yıl %25 iken bu yıl %36'ya çıkmış durumda. Genel olarak sosyal mühendislik saldırıları ise %22'den %35'e yükselerek en çok artış gösteren veri ihlali türü oluyor. Business Email Compromises (BECs), phishing ve spam en çok tercih edilen sosyal mühendislik saldırı türleri arasında bulunuyor. Oltalamadan sonra en ciddi artışı gösteren sosyal mühendislik türü konumundaki BECs saldırıları da geçen seneye kıyasla 15 kat arttı.

3. İnsan kaynaklı hatalar: Raporda yüzdesel azalış gözlenen tek başlık insan kaynaklı hatalar. 2021'de insan kaynaklı veri ihlalleri %22'den %17'ye düştü fakat araştırma sonucuna göre insan kaynaklı hatalar nedeniyle ortaya çıkan ihlal vakalarının sayısı 883'ten 905'e yükseldi.

4. Web saldırıları: Web siteleri ve uygulamalarına yönelik saldırılar artmaya devam ediyor. Hacking saldırılarının %80'i web portallarını hedef alıyor. Masaüstü paylaşımı ise bilgisayar korsanlarının işini kolaylaştıran hackleme vektörleri arasında ikinci sıraya yerleşti.

5. Bulut ortam varlıkları: Verizon DBIR 2021'e göre güvenlik ihlali yaratan harici bulut ortam varlıkları, veri ihlali vakalarında şirket içi varlıklara oranla daha yaygın şekilde kullanılıyor. Buna karşın güvenlik ihlali ile karşılaşan şirket içi kullanıcı cihazlarında (masaüstü ve dizüstü bilgisayarlar) düşüş söz konusu.

6. Kimlik bilgileri (credentials): Rapor, alışılageldiği üzere ihlallerin büyük oranda finansal kazanç odaklı dış faktörler aracılığıyla gerçekleştirildiğini ortaya koyuyor. Siber saldırılara dair bazı unsurların hiç değişmediğinin kanıtlarından birisi de güvenlik ihlallerinin %61'inin kullanıcıların kimlik bilgilerini içermesi.

Verizon'un yaptığı araştırmada veri güvenliği ihlali yaşayan şirketlerin sadece %14'ünün ekonomik anlamda kayba uğramadığı tespit edildi. Maddi kayıplar veren şirketlerin ihlaller sonucu ödedikleri tutarın medyanı ise $21.659.

DBIR 2021'in açık biçimde gösterdiği üzere, veri ihlali ile şirketinizi çeşitli kayıplardan kurtarmak için Ayrıcalıklı Erişim Yönetimi, PAM (Privileged Access Management), çözümlerinden yararlanmanız büyük önem taşıyor.

Privileged Access Management (PAM) Nedir?

Türkçe ismiyle Ayrıcalıklı Erişim Yönetimi (PAM), şirketinize ait önemli verilere çeşitli siber saldırılar sonucu ulaşmaya çalışan bilgisayar kullanıcılarını tespit, analiz ve kontrol etmek amacıyla kullanılıyor. Verizon DBIR 2021'de veriler ile ortaya konan güvenlik ihlallerini şirketinizde yaşamamanız için kullanabileceğiniz PAM yazılımları, veri kaynaklarınızı güvence altına almanızı sağlıyor.

Bir başka deyişle PAM, şirketinize ait kritik varlıklara ayrıcalıklı erişimi denetlemenizi, kontrol altında tutmanızı ve yönetmenizi kolaylaştırıyor. Sistemdeki ayrıcalıklı hesapların kimlik bilgilerini, çalınma riskine karşı, güvenli bir ekosisteme çeviren PAM uygulamaları, beş aşamadan oluşan bir güvenlik ağı meydana getiriyor. Ağın her bir aşamasında sisteme yapılan girişler kontrol ediliyor, veri güvenliği sağlanıyor ve yapılan işlemlerin tamamı kayıt altına alınıyor.

Bir PAM yazılımında süreç, yetkili oturum yöneticisi, merkezi parola yönetimi, ayrıcalıklı görev otomasyonu (PTA), iki faktörlü kimlik doğrulama (2FA) ve dinamik veri maskeleme adımlarından meydana geliyor. Tüm aşamalar veri güvenliğinizi sağlayarak karşılaşabileceğiniz olası siber güvenlik saldırılarının yaratacağı sorunların önüne geçiyor.

Single Connect ile Üst Düzey Veri Güvenliği

Dünyanın sayılı Ayrıcalıklı Erişim Yönetimi ürünleri arasındaki **Single Connect**, çok katmanlı güvenlik altyapısının yardımıyla hem iç hem de dış veri güvenliği ihlallerine karşı kritik verilerinizi korumayı başarıyor. Modüler yapısıyla dikkat çeken ve bir PAM platformunda olması gereken bileşenlerin tamamını bünyesinde barındıran Single Connect, Gartner Magic Quadrant for Privileged Access Management (PAM) raporunda da yer alıyor.

Bir Kron ürünü olan Single Connect'te yetkili oturum yöneticisi, merkezi parola yönetimi, ayrıcalıklı görev otomasyonu (PTA), iki faktörlü kimlik doğrulama (2FA), dinamik veri maskeleme ve TACACS+/RADIUS erişim yönetimi modülleri mevcut. Söz konusu modüller genel PAM yapısıyla tam uyumluluk gösteriyor.

Veri ihlalleri, siber saldırılar ve sızıntılara karşı üst düzey veri güvenliği sağlayan Single Connect, kullanıcı dostu arayüzü, güçlü teknik altyapısı ve işlevsel modülleriyle dikkat çeken bir platform olarak Verizon DBIR 2021'de bahsedilen veri ihlali türlerine karşı şirketinizi korumanız için oldukça ideal.

Siz de dünyanın önde gelen PAM çözümlerinden olan **Single Connect** hakkında merak ettiklerinizi öğrenmek ve isterseniz ürünümüzü sunduğu avantajlardan hemen yararlanmak için **bizimle iletişime geçebilirsiniz.**

Kron
www.kron.com.tr

İSTANBUL

İ.T.Ü. Ayazağa Kampüsü, Koru Yolu,
ARI 3 Binası, Teknokent, No: B401, 34467, Maslak, İstanbul - TÜRKİYE
+90 (212) 286 51 22
+90 (212) 286 53 43
info@kron.com.tr

ANKARA

Bilkent CyberPark,
C - Blok, No: 321 Bilkent, Ankara - TÜRKİYE
+90 (312) 265 06 86
+90 (312) 265 06 87
info@kron.com.tr

İZMİR

Akdeniz Mah. 1353 Sk.
Armesa İş Merkezi, No: 2/11, Konak-İZMİR
+90 (232) 484 13 97
info@kron.com.tr

NEW JERSEY

3 2nd Street, Suite 201
Jersey City, NJ, 07302 United States Of America
+1 201 204 0808
info@ironsphere.com