Delinea

2025'te Fidye Yazılımında Durum Raporu

Hızla Değişen Tehdit Ortamında Çeviklikle Adapte Olma

Yönetici Özeti

Saldırganların daha gelişmiş saldırılar düzenlemek için yapay zeka kullanmasıyla birlikte fidye yazılımı ortamı tekrar değişiyor ve kuruluşları çabucak adapte olmaya ve savunmalarını güçlendirmeye zorluyor.

En yeni bilgisayar korsanlığı araçları ve ipuçları alışverişi için geniş gizli siber suç kaynaklarından yararlanan saldırganlar, deepfake odaklı sosyal mühendislik, akıllı algılamadan kaçınma ve otomatik hedef seçimiyle girişimlerini geliştiriyor. Giderek artan bir şekilde, ilk erişim için ana vektörü gizliliği ihlal edilen kimlik bilgileri oluşturuyor.

Delinea, manşetlerin ardında olan biteni tam olarak anlamak için mücadelenin ön safhasındakilere yöneldi: Kuruluşlarını korumak için yorgunluk nedir bilmeksizin çalışan BT ve güvenlik liderleri. Bu yılki çalışma 1.000'i aşkın güvenlik uzmanından içgörüleri toplayarak siber güvenliğin durumu hakkında geniş bir perspektif sunuyor. Mesaj açık ve net: Fidye yazılımı saldırıları artıyor ve fidyeler ödense dahi iş kesintileri haftalar boyunca sürebiliyor. Üstelik şantaj artık fidye yazılımı saldırılarının yarıdan fazlasını oluşturuyor. Ağ savunucuları yapay zeka kullanmaya başladı ancak bu tek başına başarıyı garantilemiyor.

Bu raporda, tehdit aktörlerinin nasıl giderek daha agresif ve gelişmiş hale geldiğinin yanı sıra kuruluşların fidye yazılımı saldırılarını tespit etmek, azaltmak ve önlemek için proaktif önlemleri nasıl benimsediğini öğrenerek kendi güvenlik programınız için bilinçli seçimler yapabileceksiniz.

Temel çıkarımlar

- **Fidye yazılımı ihlalleri ödeme yapan mağdur sayısının azalmasına rağmen artışta**
  - Fidye yazılımları her yerde, firmaların %69'u saldırıya uğradı ve dörtte birinden fazlası birden fazla kez hedef oldu
  - Fidye yazılımlarının %60'ı artık veri hırsızlığıyla ilişkili şantaj içeriyor
  - Daha az (%57) şirket ödeme yapıyor
  - Aktörleri saldırı düzenlemeye teşvik eden etkenler devam ediyor
- **Yöneticilerin kaygısı giderek artıyor ancak güvenlik eksik kalıyor**
  - Mağdurların 3/4'ünün kurtarma için iki hafta harcamasıyla birlikte fidye yazılımı kaosa neden oluyor
  - Üst düzey yöneticilerin %90'ı fidye yazılımları konusunda kaygılı
  - Geleneksel fidye yazılımıyla mücadele taktikleri sonuç vermiyor
  - Kuruluşların yalnızca üçte birinin en düşük ayrıcalık yaklaşımını benimsemesiyle kritik erişim yolları saldırganlara açık kalıyor
- **Fidye yazılımı tehditleri geliştikçe yapay zeka kullanımı artıyor**
  - Yapay zeka tehdit aktörlerine destek sağlıyor
  - Fidye yazılımı grupları esnekçe biçim değiştiriyor
  - Şirketlerin %90'ı fidye yazılımlarını ele almak için yapay zeka kullanıyor

Kritik Bulgu 1:

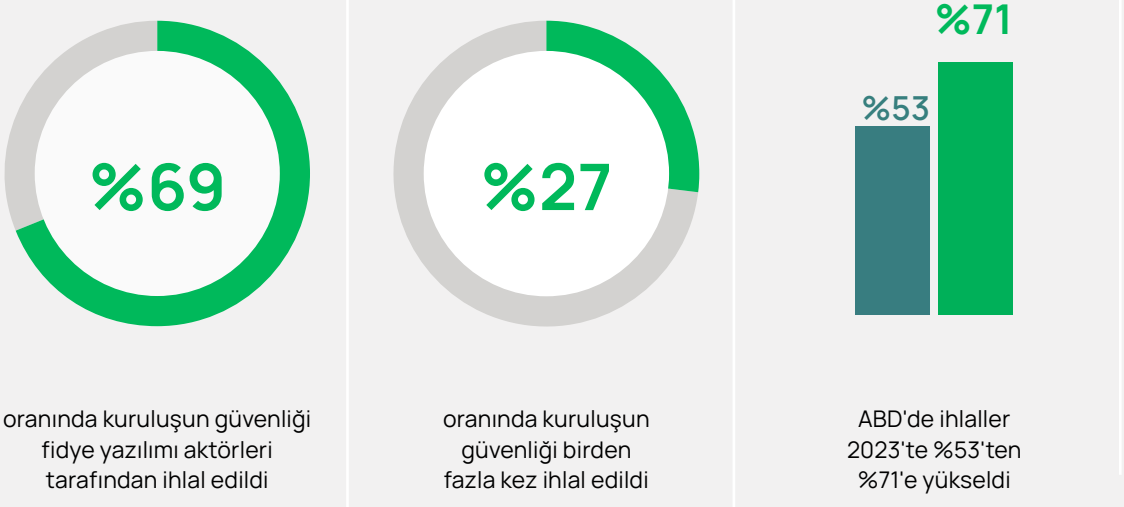
Fidye yazılımı ihlalleri ödeme yapan mağdur sayısının azalmasına rağmen hızla artışta

Fidye yazılımları her yerde

Başarılı fidye yazılımı saldırıları artmaya devam ediyor. Katılımcıların üçte ikisinden fazlası geçtiğimiz yıl bir fidye yazılımı ihlali yaşadı; ABD'deki ihlaller ise yaklaşık üçte bir oranında yükseldi. Üstelik katılımcıların dörtte birinden fazlası birden çok kez saldırıya uğradı. Kuruluşların mevcut önlemleri, giderek büyüyen dijital şantaj dalgasını durdurmaya yeterli değil.

Çoğu firma geçen yıl güvenlik ihlali yaşadı

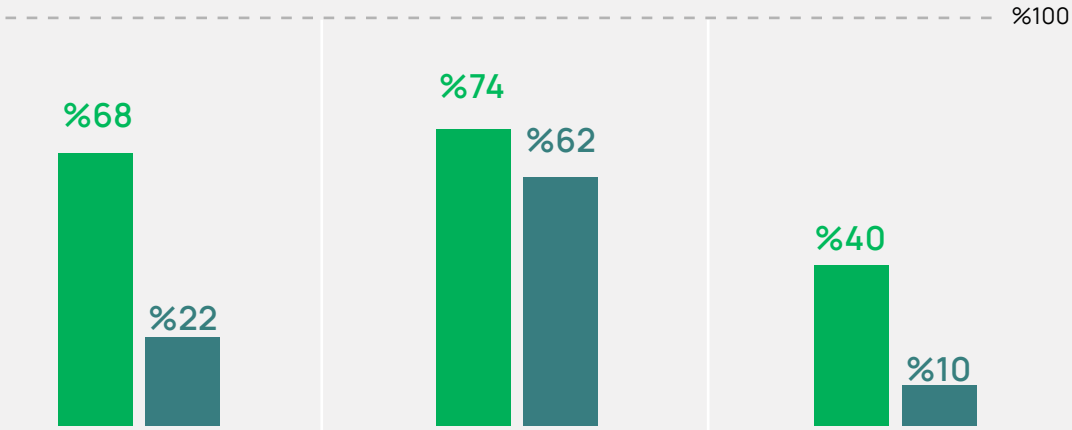
S: Şirketiniz son 12 ay içinde bir fidye yazılımı saldırısının kurbanı oldu mu?



ABD'de, en büyük güvenlik ihlallerini en büyük kuruluşlar yaşadı. Büyük ölçekli şirketler, "büyük av" olarak hedef alınıyor ve yüksek fidye ödemeleri için gelişmiş, "klavye başında" yürütülen saldırılara maruz kalıyor. Ancak küçük firmalar da güvende değil. Küçük firmalar genellikle daha basit ve hazır saldırı girişimleri için kolay av olarak görülüyor.

ABD'de fidye yazılımı saldırıları büyük artış gösterdi

S: Şirketiniz son 12 ay içinde bir fidye yazılımı saldırısının kurbanı oldu mu?



ABD'deki Büyük Ölçekli Kuruluşlar (500'den fazla çalışan): 2023'te %22'den %68'e yükseliş

ABD'deki Orta Ölçekli Kuruluşlar (50-500 çalışan): 2023'te %62'den %74'e yükseliş

ABD'deki Küçük Ölçekli Kuruluşlar (1-49 çalışan): 2023'te %10'dan %40'a yükseliş

En büyük tehdit artışı hangi sektörlerde görülüyor? Delinea anketine göre, ABD'deki bilişim ve telekom sektörü geçtiğimiz yıl bir önceki yıla kıyasla %65 daha fazla saldırıya uğradı. Perakende, yeme-içme ve eğlence sektörlerinde ise saldırılar %57 oranında arttı. Sağlık kuruluşları da her iki kurumdan birinin geçtiğimiz yıl saldırıya uğradığını bildirmesiyle popüler bir hedef olmaya devam ediyor. Her kurum birbirinden farklı olsa da bu sektörler, özellikle kesintilere düşük tolerans göstermeleri ve müşteri ile çalışanlara ait büyük miktarda hassas veriyi ellerinde bulundurmaları başta olmak üzere bazı ortak üst düzey özelliklere sahip.

En çok hangi sektörler hedef alınıyor?

Delinea Labs araştırma ekibinin "Siber Güvenlik ve Yapay Zeka Tehdit Ortamı" raporuna göre teknoloji, üretim ve sağlık sektörü geçen yıl en çok hedef alınan sektörler arasında yer aldı. Bu sektörlerin seçilme nedeni muhtemelen kesintilere karşı düşük toleransları ve bu nedenle ödeme yapma olasılıklarının daha yüksek olmasıydı. Özellikle sağlık sektörü hasta verilerinin hassas doğası nedeniyle savunmasızdı; ihlaller kritik bilgilerin açığa çıkmasına ve hayatların tehlikeye girmesine yol açtı.

Kaynak: Delinea Labs, "Siber Güvenlik ve Yapay Zeka Tehdit Ortamı", Ocak 2025

En önemli soru şu: Başarılı fidye yazılımı saldırılarının sayısı neden artmaya devam ediyor? İşte öne çıkan bazı etkenler:

- **Kimlik bilgisi hırsızlığı yaygınlaşmış durumda.** 2025 Verizon Veri İhlali Araştırmaları Raporu'na göre, geçen yıl yaşanan ihlallerin neredeyse üçte birinde (%32) çalıntı kimlik bilgilerinin kullanıldığı görüldü. Bu çalıntı kullanıcı adı/şifre kombinasyonları, saldırganların geleneksel savunmaları kolayca aşarak kurumsal ağlara sızmasına olanak tanıyor.
- **Hizmet olarak fidye yazılımları (RaaS) arttı.** Delinea Labs'in 2025 tarihli Siber Güvenlik ve Yapay Zeka Tehdit Ortamı raporu, hizmet olarak fidye yazılımlarının giderek daha yaygın hale geldiğini ve karmaşık saldırıların artık daha az yetkin aktörler tarafından da gerçekleştirilebildiğini ortaya koyuyor. Hizmet olarak fidye yazılımları genellikle teknoloji, üretim ve inşaat gibi sektörleri hedef alıyor.
- **İlk erişim aracıları (IAB) yükselişte.** Delinea Labs, mağdurları savunmasız bırakmaya odaklanan uzman tehdit aktörleri olan ilk erişim aracılarının fidye yazılımı saldırılarındaki artışa ek katkıda bulunduğuna inanıyor. Hatta bazı ilk erişim aracısı siteleri, potansiyel alıcıların satın almadan önce ele geçirilmiş kimlik bilgilerinin geçerli olup olmadığını test etmesine imkan tanıyor. Ayrıcalıklı hesap kimlik bilgileri en değerli hedefi oluşturuyor ve özellikle de "hazinenin anahtarlarını" barındıran Active Directory gibi kurumsal kimlik sistemlerine erişim sağlayan bilgiler büyük önem taşıyor.

Fidye yazılımı grupları esnekçe biçim değiştiriyor

Delinea araştırmaları en çok faaliyet gösteren beş fidye yazılımı grubunun, geçtiğimiz yıl incelenen 5.700 olayın %36'sından sorumlu olduğunu ortaya koyuyor. Araştırma siber suç yeraltı dünyasının ne kadar esnek ve dayanıklı olduğunu, grupların genellikle yeniden markalaşarak denetimden kaçtığını ve kolluk kuvvetlerinin müdahalelerine rağmen varlıklarını sürdürdüklerini vurguluyor. Delinea Labs Raporu'na göre, faaliyetleriyle öne çıkan ilk beş grup şunlar:

- **RansomHub:** Knight'ın yeniden markalanmış bir versiyonu olup, ağırlıklı olarak veri hırsızlığı yoluyla şantaj yapan büyük bir RaaS grubu.
- **LockBit:** 2019'dan bu yana faaliyet gösteren, gelişmiş şifreleme teknikleri kullanan kötü şöhretli ve üretken bir RaaS grubu. Gözaltılar ve operasyonlara rağmen daha sınırlı kapasiteyle varlığını sürdürüyor.
- **Play:** 2022'den beri aktif olan bu grup, çift şantaj taktiklerinin bir parçası olarak mağdurların dosyalarının daha hızlı şifrelenmesini sağlayan kesintili şifreleme yöntemini kullanıyor.
- **Akira:** 2023'te ortaya çıkan ve dağılan Conti grubuyla bağlantılı, agresif bir grup.
- **Hunters International:** Gelişmiş kötü amaçlı yazılımlarıyla dikkat çeken ve dağılan Hive fidye yazılımı grubunun bir uzantısı olduğuna inanılan bir diğer RaaS grubu.

Günümüzde çoğu fidye yazılımı veri hırsızlığı şantajı içeriyor

Delinea araştırmacıları, ana fidye yazılımı gruplarının çoğunun artık çift şantaj modelini takip ettiğini belirtiyor. Bu bulgular, anket yapılan fidye yazılımı mağdurlarının %60'ının veri ihlali yaşadığını, %85'inin ise verilerinin yayınlanması veya satılmasıyla tehdit edildiğini belirttiği bu çalışmayla da destekleniyor.

Eğer şantaj artık ağırlıklı olarak bilgi hırsızlığına odaklanıyorsa yalnızca yedekleme yapmak tek başına faydalı bir hafifletme stratejisi olmaktan çıkıyor. Kuruluşların bunun yerine çeşitli savunma tekniklerine sahip olması gerekiyor. En başta verilerin çalınmasını önleyen proaktif ve önleyici güvenlik önlemlerinin vurgulanması gerekiyor.

Daha az şirket ödeme yapıyor, ama iş hâlâ bitmiş değil

Anket yapılanların yarısından fazlası, geçen yıl kurtarma sürecini hızlandırmak amacıyla kolluk kuvvetleri ve devlet yetkililerinin tavsiyelerine karşı gelerek fidye ödediğini belirtti. Bununla beraber geçen yıl ABD'de daha az şirket ödeme yaptı.

Fidye ödemek her zaman istenen sonucu getirmiyor. Fidye ödeyen katılımcıların yaklaşık dörtte biri tüm verilerini geri alamadıklarını bildirirken, bu oran Birleşik Krallık'ta üçte bire kadar yükseliyor. Veriler geri alınsa bile saldırganların bu verileri yine de paraya çevirmeye çalışması muhtemel.

Fidye ödemek veri kurtarmayı garantilemiyor

S: Şirketiniz son 12 ay içinde bir fidye yazılımı saldırısının kurbanı olduysa şirketiniz fidyeyi ödedi mi? Şirketiniz fidye ödediyse verileri başarılı bir şekilde kurtardınız mı?

%57

oranında kuruluş fidye ödedi

%60

oranında ABD kuruluşu fidye ödedi, bu oran 2023'te %76'ydı

%54

oranında Birleşik Krallık kuruluşu fidye ödedi

%26

oranında kuruluş fidye ödedi ancak verilerini geri alamadı (Birleşik Krallık'ta %35, ABD'de %18)

Güvenlik açıkları, ödeme yapmaya istekli mağdurlar ve suç faaliyetlerine koruma sağlamaya hazır rejimler var oldukça tehdit de var olmaya devam edecek. Yapay zekanın saldırganlara yeni bir avantaj sağlamasıyla birlikte, ağınızı koruyan ekiplerin fidye yazılımı stratejilerini acilen gözden geçirmesi gerekiyor.

Kritik Bulgu 2:

Yöneticilerin kaygısı giderek artıyor ancak güvenlik eksik kalıyor

Fidye yazılımları kaos ve aksaklığa yol açıyor

Kuruluşlar fidye yazılımı saldırılarından ciddi şekilde etkilenmeyi sürdürüyor. Araştırmamıza göre, mağdurların neredeyse yarısı bir fidye yazılımı ihlalinden toparlanmak için bir haftaya (bir ila altı gün) kadar zaman harcadı. Katılımcıların üçte biri, toparlanmanın iki haftayı bulduğunu belirtti. Çok az mağdur 24 saatten kısa sürede toparlanabildi. Bu durumlarda ise muhtemelen saldırganlar hızlı bir şekilde tespit edildi ve verileri çalmak veya sistemleri şifrelemek için fırsat bulamadı.

Kurtarma süreci çok yavaş

S: Şirketiniz fidye yazılımları tarafından hedef alındıysa operasyonları tamamen kurtarmak ne kadar zaman aldı?

%46

oranında mağdurun fidye yazılımı ihlalinden sonra toparlanması bir haftaya kadar sürdü

(Birleşik Krallık firmalarının %50'si ve ABD firmalarının %42'si)

%75

oranında mağdurun toparlanması iki haftaya kadar sürdü

%18

Mağdurların yalnızca %18'i 24 saat içinde toparlanabildi

Birçok kuruluş bu kadar şanslı değil. Olay müdahalesi ve toparlanma sürecinde birden fazla aşamadan geçmek gerekiyor. Bu süreç, etkilenen sistemlerin izole edilmesi ve saldırının kapsamının belirlenmesiyle başlıyor. Ardından, kötü amaçlı yazılımın tamamen kaldırılması ve sistemlerin yeniden yapılandırılması geliyor. Daha sonra ilgili tarafların bilgilendirilmesi gerekiyor. Bazı durumlarda, tehdit aktörleriyle diyalog kurmak da faydalı olabiliyor. Son olarak, şifrelenmiş veriler yedekten geri yükleniyor. Tüm bunlar zaman ve maliyet gerektiriyor.

Araştırmamız, kuruluşların %1'den azının bir ay sonra hâlâ bir saldırıdan toparlanmakta olduğunu gösterse de, bu tür vakalar müşteriler ve bazen de tüm topluluklar üzerinde orantısız etkiler yaratabiliyor. Örneğin, Haziran 2024'te NHS tedarikçisi Synnovis'e yönelik bir fidye yazılımı saldırısı, Londra bölgesinde binlerce poliklinik randevusu ve elektif işlemin ertelenmesine yol açtı. Yeni kan bağışçıları için acil çağrı yapıldı. Hatta üç ay sonra bile tüm sistemler tamamen toparlanamamış halde oldu.

Benzer şekilde, Birleşik Krallık'taki perakendeciler Marks & Spencer ve Co-op'a yönelik son fidye yazılımı saldırıları operasyonları ciddi şekilde aksattı, hizmetleri ve tedarik zincirlerini etkiledi. Bazı kuruluşlarda ciddi bir fidye yazılımı ihlali, varoluşsal bir tehdit haline bile gelebiliyor. Haziran 2023'te Kettering merkezli KNP Logistics Group, bir fidye yazılımı saldırısının ardından tasfiye sürecine girmek zorunda kaldı ve 730 iş kaybı yaşandı.

Birleşik Krallık hükümetinin bir çalışmasına göre, fidye yazılımı saldırısına uğrayan kuruluşlar şu risklerle karşılaşabiliyor:

- Azalan kâr marjları
- Kaçırılan iş fırsatları
- Ekstra BT maliyetleri
- İtibarın zedelenmesi
- Üst yönetime olan güvenin azalması
- Personelde ekstra stres ve kaygı nedeniyle psikolojik ve fiziksel etkiler

Kuruluşunuz, iyi tasarlanmış ve prova edilmiş bir olay müdahale planı da dahil olmak üzere sağlam bir İş Sürekliliği ve Felaket Kurtarma (BCDR) programına sahip değilse zorlanabilir. En kötü senaryolara yönelik alıştırma yapmak, her paydaşın rolünü bilmesini ve gözden kaçabilecek sorunların tespit edilmesini sağlamak açısından hayati öneme sahiptir. Bu, yedeklerden verilerin hangi sırayla geri yükleneceğini belirlemek gibi basit bir konu bile olabilir. BT ekipleri, sırf her şey buluta yedeklendiği için bu sürecin kolay olacağını varsaymamalıdır.

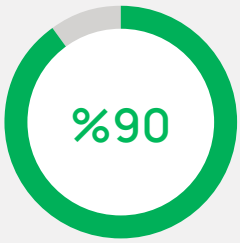
Ayrıcalıklı Erişim Yönetimi (PAM), saldırganların yatay hareketlerini en başından sınırlayarak toparlanma süresi ve maliyetlerini azaltmaya yardımcı olabilir. Saldırganların hareket edebileceği ve zarar verebileceği ortam küçüldüğünde alınacak veri miktarının da daha az olması muhtemeldir.

Yöneticiler haklı olarak endişeli

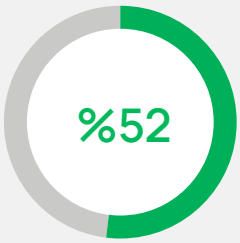
Fidye yazılımının kuruluşları üzerindeki potansiyel etkisi göz önüne alındığında, karar vericilerin dokuzda dokuzunun tehditle ilgili endişe duyduğunu ifade etmesi şaşırtıcı değil. Üstelik bu endişe giderek artıyor. Artık ABD'de yöneticilerin yarısından fazlası çok endişeli, 2023'te ise bu oran yalnızca dörtte birin biraz üzerindeydi. En büyük artış, en büyük şirketlerden geldi. Bu durum, hem bu büyüklükteki şirketler arasında mağdur sayısının artması hem de ciddi bir ihlalin potansiyel finansal ve itibar etkisi ile uyumlu.

Üst düzey yöneticilerin kaygısı giderek artıyor

S: Aşağıdaki ifadelerden hangisi yönetim kurulunuzun ve yönetici liderlik ekibinizin kuruluşunuzu hedef alan fidye yazılımlarıyla ilgili endişelerini en iyi şekilde dile getiriyor?

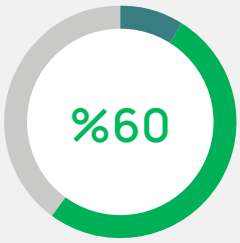


oranında yönetici/ yönetim kurulu fidye yazılımı tehdidinden kaygı duyuyor



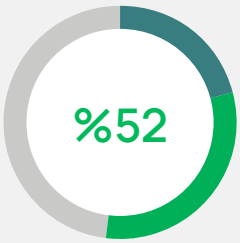
oranında ABD firması çok kaygılı, bu oran 2023'te %26'ydı

%9 (2023)



250-499 milyon $ geliri olan ABD firmaları: %60'ı çok kaygılı, bu oran 2023'te %9'du

%21 (2023)

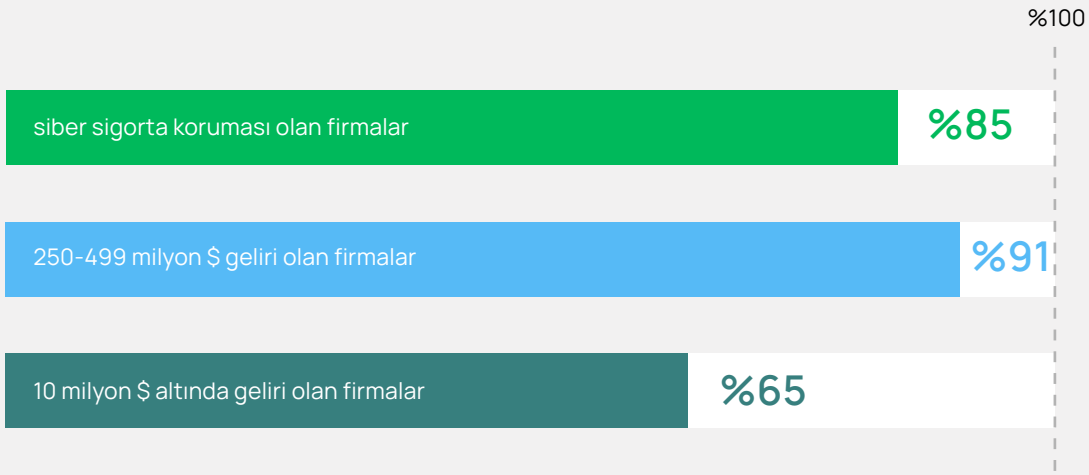


500 milyon $ üzeri geliri olan ABD firmaları: %52'si çok kaygılı, bu oran 2023'te %21'di

Bu endişeler, nispeten yüksek seviyede siber sigorta korumasına dönüşüyor olabilir. Ortalama olarak, her beş firmadan dördü siber sigortaya sahip olduğunu bildiriyor. Daha büyük şirketlerin sigortalı olma olasılığı daha yüksek. En küçük şirketler en düşük sigorta oranına sahip, ancak sigortayı bütüncül bir güvenlik duruşunun yararlı bir parçası olarak değerlendirmeleri gerekiyor.

Büyük firmaların siber sigorta yaptırma ihtimali daha fazla

S: Şirketiniz fidye yazılımı saldırılarına karşı koruma sağlayan siber sigortaya sahip mi?



Bir sigorta poliçesi, bir olaydan kaynaklanan finansal riski azaltmaya yardımcı olabiliyor. Ancak günümüzde sigortacılar, koruma sağlamak için giderek artan şekilde en iyi güvenlik uygulamalarının uygulanmasını şart koşuyor; bu durum, kurumsal güvenlik yaklaşımını iyileştirmeye de katkıda bulunabiliyor. Bazıları ayrıca önleyici güvenlik ve olay müdahalesi için destek ve kaynaklar sunuyor; bu da küçük ölçekli poliçe sahipleri için faydalı olabiliyor.

Fidye yazılımıyla mücadele taktikleri sonuç vermiyor

Peki üst düzey yöneticiler artan fidye yazılımı endişelerine karşı tam olarak nasıl adımlar atıyor?

Olay müdahale planına sahip katılımcıların oranı ortalama %90, bu da geçen yıla göre çok değişmemiş olsa da güven verici bir seviye. Ayrıca en küçük şirketlerin (50'den az çalışanı olan) olay müdahale planı sahipliğinde bir yıl içinde %60'tan %79'a yükselen oranla en büyük artışı göstermesi de dikkat çekiyor. Müdahale planınızı pragmatik bir şekilde tasarladığınız, işletmenin farklı alanlarından paydaşları dahil ettiğiniz ve düzenli olarak alıştırma yaptığınız sürece fidye yazılımı sonrası toparlanma sürecinin kolaylaşması beklenir.

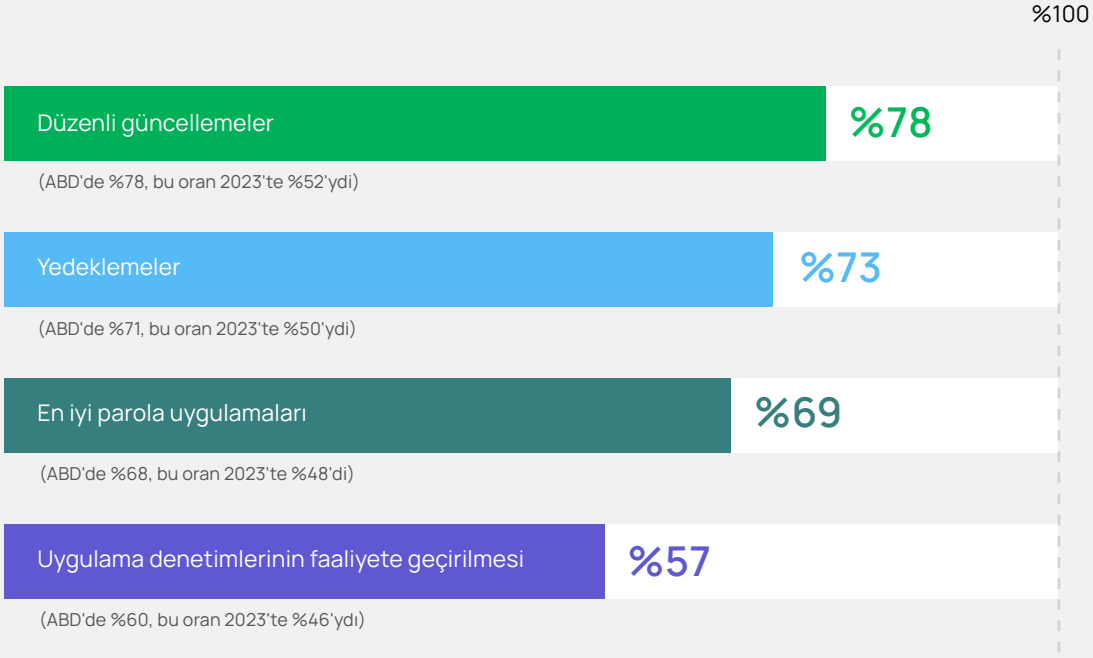
Ancak daha etkili bir strateji önlemeye odaklanmaktır, çünkü veriler bir kez çalındığında saldırganlar bunları büyük olasılıkla paraya çevirecektir. Katılımcıların geçen yıl uyguladığı başlıca dört önleyici tedbir şunlardır:

1. Düzenli sistem ve yazılım güncellemeleri
2. Kritik verilerin yedeklenmesi
3. En iyi parola uygulamalarının zorunlu kılınması
4. Uygulama denetimlerinin faaliyete geçirilmesi

ABD'de bu en iyi uygulamaların benimsenmesinde bir önceki yıla kıyasla önemli bir artış görüldü.

ABD önleyici tedbirleri artırdı

S: Fidye yazılımı saldırısını önlemek için (eğer geçerliyse) nasıl adımlar attınız? (Uygun olan tüm yanıtları seçin)



Bu tür en iyi siber hijyen uygulamaları ne kadar faydalı olursa olsun raporun başındaki fidye yazılımı mağduru sayısına bir bakış bunların açıkça işe yaramadığını gösteriyor. Bunun nedenlerinden birini kurumsal saldırı yüzeyinin büyüklüğü oluşturuyor. Uzaktan çalışma, bulut varlıklarına yapılan yatırımlar, Nesnelerin İnterneti (IoT) uç noktaları, kurum içi geliştirilen bulut tabanlı uygulamalar ve özerk yapay zekanın yükselişi sayesinde bu yüzey son yıllarda büyük ölçüde arttı.

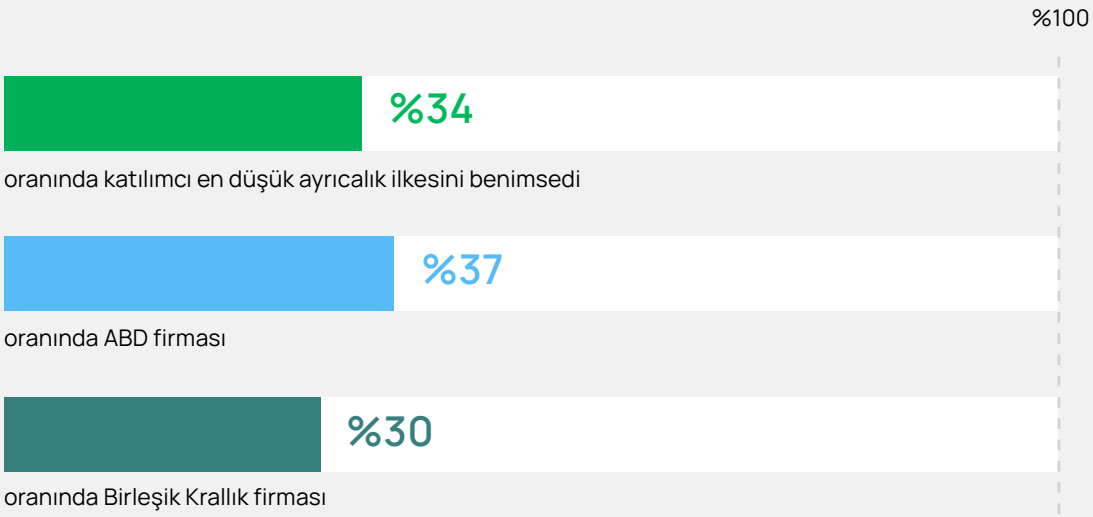
Pratikte bu, saldırganların hedef alabileceği büyük bir alan ve birçok olası saldırı vektörü olması anlamına geliyor. Paketlenmiş, hizmet tabanlı çözümler giriş engellerini düşürmeye yardımcı oluyor. İlk erişim aracıları kurumsal ağlara ve bulut hesaplarına kolay erişim sunuyor. Ayrıca çalınan verileri satabilecekleri hazır bir pazar bulunuyor.

En düşük ayrıcalık uygulaması yeterince kullanılmıyor

Fidye yazılımı aktörlerinin başarılı olmasının bir diğer nedeni, kuruluşların kimlik yönetimine yeterince önem vermemesi. Katılımcıların yaklaşık üçte biri en düşük ayrıcalık yaklaşımını benimsediğini belirtiyor. En düşük ayrıcalık, kullanıcılar ve makinelerin yalnızca görevlerini tamamlamak için gerekli izinlere sahip olmasını ve daha fazlasına erişememesini öngören bir en iyi güvenlik uygulama ilkesi.

Çok az firma en düşük ayrıcalık ilkesini benimsiyor

S: Fidye yazılımı saldırısını önlemek için (eğer geçerliyse) nasıl adımlar attınız? (Uygun olan tüm yanıtları seçin)



Bu neden önemli? Fidye yazılımı bağlamında, en düşük ayrıcalık yaklaşımı şunları sağlayarak saldırı yüzeyini ve saldırıların etkisini azaltmaya yardımcı oluyor:

- Kullanıcıların tehdit aktörleri için ilk erişim sağlayabilecek potansiyel olarak yetkisiz/ güvensiz uygulamalar yüklemesini önlemek.
- Kullanıcılar, hesaplar, uygulamalar ve hizmetlerin erişebileceği alanları kısıtlayarak yatay hareket yollarını engellemek.
- Potansiyel olarak riskli üçüncü taraf tedarikçilere erişimi sınırlamak.

Görevlerin ayrılması (SoD) ile birleştirildiğinde ve PAM, çok faktörlü kimlik doğrulama (MFA) ve yapay zeka destekli analizlerle desteklendiğinde en düşük ayrıcalık, sıfır güven yaklaşımının temel taşlarından biri haline gelebiliyor. Bu en iyi uygulama güvenlik yaklaşımı, hiçbir kullanıcı veya makinenin doğal olarak güvenilir olmaması gerektiğini ve herkesin kimliğinin sürekli olarak risk bazlı şekilde doğrulanması gerektiğini öngörüyor.

Buna rağmen en düşük ayrıcalığı uygulamak yamalama yapmak, yedekleme yapmak veya güçlü parola politikaları uygulamaktan daha zorlu olabiliyor; bu da katılımcılar arasında benimsenme oranının nispeten düşük olmasını açıklayabiliyor. Kuruluşunuzun büyüklüğüne bağlı olarak, bu yöntem binlerce kullanıcı, uygulama ve hizmetin sürekli olarak yönetilmesini gerektirebiliyor.

Bunu başarıyla uygulamak için, rollerin ve sorumlulukların iyi tanımlandığı, kullanıcılara bağlandığı ve erişim perspektifinden düzenli olarak denetlendiği olgun bir kimlik ve erişim yönetimi (IAM) programına ihtiyaç oluyor. Bulut Altyapısı Yetkilendirme Yönetimi (CIEM) ve Kimlik Hırsızlığı Tespiti ve Müdahalesi (ITDR) araçları, burada ayrıcalıklı hesapları sürekli olarak keşfetme, yönetme ve koruma, kullanımını izleme, anormal davranışları araştırma, olaylara müdahale etme ve ayrıcalıklı erişim kontrollerini değerlendirme konularında hayati öneme sahip. Ayrıca yönetişim de IAM stratejiniz için kritik bir katman oluşturarak insan, süreç ve teknolojiyi tek bir tutarlı yaklaşımda birleştiriyor.

Kritik Bulgu 3:

Fidye yazılımı tehditleri geliştikçe yapay zeka kullanımı artıyor

Yapay zeka fidye yazılımı aktörlerine destek sağlıyor

Sıfır Güven, PAM ve en düşük ayrıcalık uygulamaları, hızla değişen tehdit ortamında giderek daha önemli hale geliyor. Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), 2024 başında yapay zekanın "önümüzdeki iki yıl içinde neredeyse kesin olarak siber saldırıların sayısını artıracağı ve etkilerini yükselteceği" uyarısında bulundu. Bu öngörüler şimdiden gerçekleşmeye başladı. Örneğin, kendi kötü amaçlı yazılımını geliştirmek için üretken yapay zeka (GenAI) kullandığına inanılan FunkSec fidye yazılımı grubunu ele alalım.

Delinea Labs araştırmacıları, saldırganların gelecekte üretken yapay zekayı çalışanların, müşterilerin ve tedarikçilerin yazım tarzını taklit etmek için kullanarak kimlik avı saldırılarının başarı oranını artıracağını öngörüyor. Ayrıca, bir kuruluşun markasını taklit eden benzersiz kimlik avı siteleri oluşturmaları, güvenilen meslektaşların kimliğine bürünmek için deepfake ses veya video kullanmaları ve çalışanları kötü amaçlı yazılım indirmeye ikna etmeleri de muhtemel.

Yapay zekanın geleceği giderek özerk hale geliyor: Bu modelde yapay zeka, özerk ve dinamik şekilde hareket ederek hedeflerine ulaşmak için sorunları çözüyor ve görevleri anlık olarak tamamlıyor. Delinea, bu yeni teknolojinin tipik bir fidye yazılımı saldırısının keşif, istismar, araştırma ve veri sızdırma dahil olmak üzere birçok aşamasını otomatikleştirmek için kullanılmaya başlandığını gözlemliyor. Buradaki tehlike, bu durumun potansiyel fidye yazılımı ortakları için giriş engellerini daha da düşürmesi ve kötü niyetli aktörlerin az kaynakla çok hedefli saldırılar gerçekleştirmesini mümkün kılmasından ileri geliyor.

Kuruluşunuza yönelik zorluk ise bunun yalnızca saldırı sayısını artırmakla kalmayıp tipik bir saldırı zincirinin yaşam döngüsünü de kısaltabilmesi. Bu durum, tespit ve müdahaleyi çok daha zor hale getiriyor ve önleyici, proaktif güvenliğin önemini bir kez daha ön plana çıkarıyor.

Yapay zeka, fidye yazılımına karşı mücadelede yaygın olarak kullanılıyor

İyi haber şu ki, görüştüğümüz kurumsal BT güvenlik ekiplerinin %90'ı saldırganlarla başa çıkabilmek için yapay zekadan faydalanıyor. Bunu üç ana şekilde yapıyorlar:

1. **Güvenlik Operasyon Merkezi'nde (SOC)**

SOC ekipleri, fidye yazılımı da dahil olmak üzere gelen siber tehditlere karşı ön safta yer alıyor. Genellikle baskı altında ve yetersiz personel ile çalışarak uzman eksikliği ve aşırı uyarı yüküyle mücadele ediyorlar. İşte burada yapay zeka büyük bir yardım sunabiliyor: Olayları önceliklendirip ek verilerle zenginleştirerek doğru analiste yönlendiriyor ve böylece daha bilinçli kararlar alınmasını sağlıyor. Daha gelişmiş modeller, tehdit verilerini inceleyerek nasıl ilerlenmesi gerektiğine dair öneriler sunmak suretiyle 3. Kademe analist işlerini gerçekleştirebiliyor. Özerk yapay zeka, ağ içinde olası kötü niyetli faaliyetler hakkında faydalı bilgiler sunmak için özerk bir şekilde tehdit avcılığı yapabiliyor.

2. **İhlal Göstergelerini (IoC) analiz etmek için**

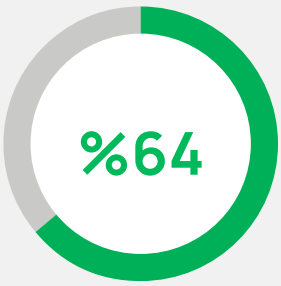
Yapay zeka büyük veri hacimlerini analiz etmek ve insan gözünün kaçırabileceği kalıpları bulmak konusunda çok başarılı, üstelik bunu yılın 365 günü, 7/24 yapabiliyor. Bu nedenle, özellikle SOC ortamında IoC'leri incelemeye yardımcı olmak için ideal. Yapay zeka farklı iç ve dış kaynaklardan çeşitli IoC'leri toplamak üzere programlanabiliyor. Amaç, insan uzmanların daha değerli güvenlik operasyon görevlerine odaklanabilmesi için onlara işlem yapılabilir bilgi sunmak. Bu, tehdit tespiti ve müdahalesini hızlandırabiliyor.

3. **Kimlik avını önleme**

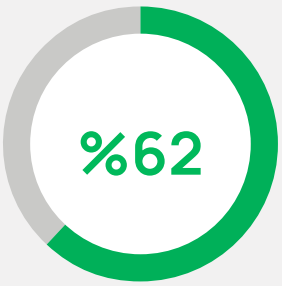
Yapay zeka algoritmaları, e-posta yazarına uymayan şüpheli yazım stillerini veya yanlış zamanda gönderilen ya da alışılmadık içerikli mesajlar gibi sıra dışı davranışları analiz etmek için eğitilebilir. Yapay zeka bağlantıları, ekleri ve QR kodları dahil olmak üzere görüntüleri analiz edebilir. Ayrıca personel eğitimi için gerçekçi simülasyon egzersizleri oluşturulmasına ve çalışan tepkilerinin izlenmesine yardımcı olabiliyor.

BT'nin yapay zekadan yararlandığı 3 alan

S: Kuruluşunuz günümüzde fidye yazılımı saldırılarına karşı koruma sağlamak için yapay zekayı nasıl kullanıyor? (Uygun olan tüm yanıtları seçin)



Güvenlik Operasyon Merkezi'nde



İhlal Göstergelerini analiz etmek için

Kimlik avını önleme

Diğer yapay zeka kullanım alanları

Bu kullanımların yanı sıra, yapay zeka teknolojisi IAM ve PAM araçlarına da entegre ediliyor ve etkileyici sonuçlar sağlıyor. Bunlar aşağıdakileri içeriyor:

- **Rutin görevlerin otomasyonu**

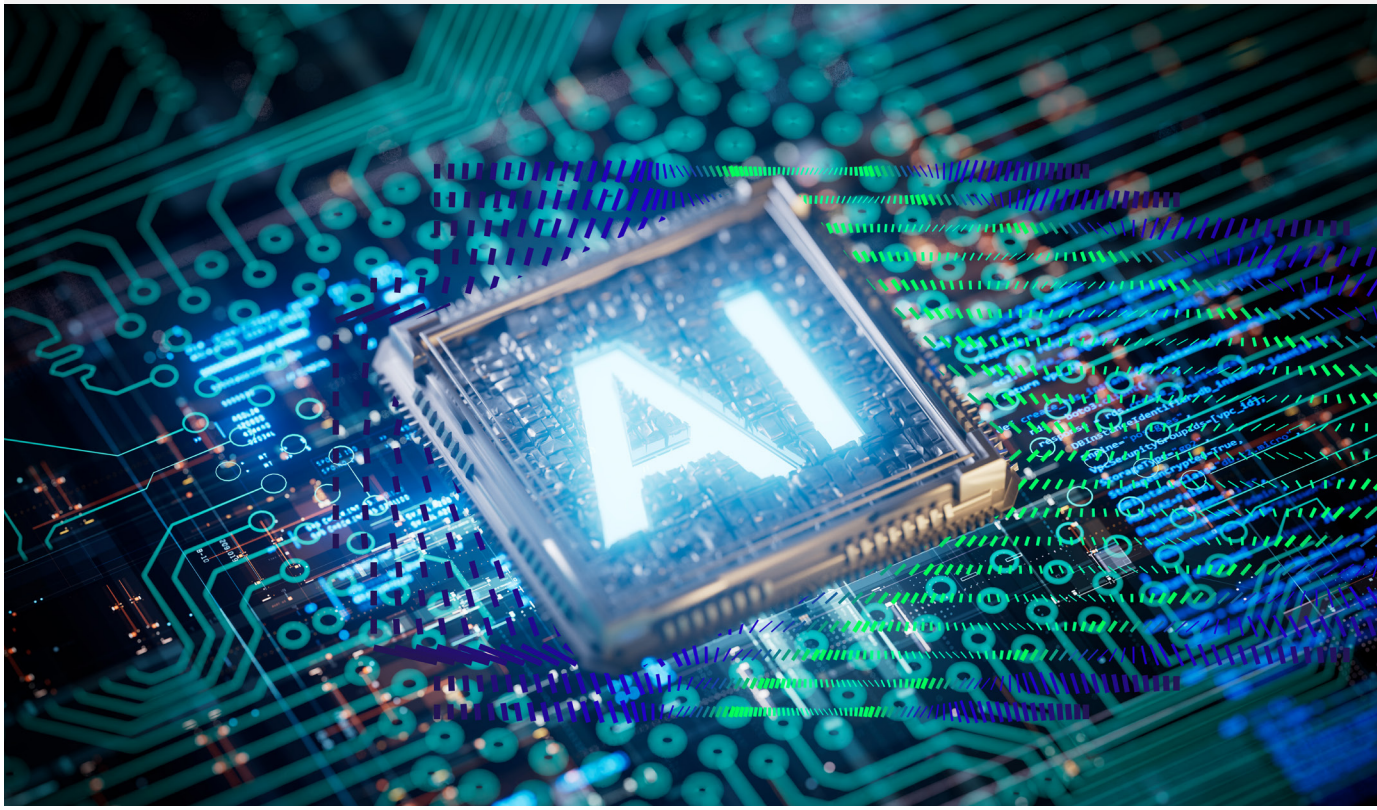
  Manuel yapıldığında, özellikle büyük kuruluşlarda insan hatasına açık işlemler olan hesap oluşturma, kullanıcı erişim incelemeleri, rol modelleme ve diğer zaman alıcı görevlerin otomatikleştirilmesi.

- **Oturum denetimi**

  Yapay zeka, oturumları izleyerek aşırı ayrıcalıklı kimlikler veya beklenmeyen ayrıcalıklı davranışlar gibi güvenlik sorunlarını tespit edebiliyor. Bu, zaman alıcı manuel günlük incelemelerine kıyasla ekipler için daha verimli bir yaklaşım sunuyor.

- **Fidye yazılımı savunması için akıllı yetkilendirme**

  Özerk yapay zeka, yetkilendirme politikalarını tanımlıyor, optimize ediyor ve otomatik olarak uyguluyor. Bu sayede kullanıcıların parola oluşturmasına veya hatırlamasına, BT ekiplerinin izinleri ayarlaması veya politika değişikliklerini takip etmesine gerek kalmıyor. Tehdit hacimleri, saldırı yüzeyleri, siber güvenlik uzman eksiklikleri ve ortamların karmaşıklığı arttıkça, bu tür yapay zeka destekli yetkilendirme, fidye yazılımı önleme için giderek daha kritik hale gelecek.



İşletmeler kendilerini nasıl koruyabilir?

Çalınan kimlik bilgileri, veri ihlallerinde başlıca faktörlerden biri olmayı sürdürüyor. Saldırganlara yalnızca kurumsal ağlara ilk erişimi sağlamakla kalmıyor, aynı zamanda ayrıcalıkları yükseltmelerine ve yatay hareket ederek maksimum zarar vermelerine de imkan tanıyor.

Bu, fidye yazılımı ihlallerinin artmasının birçok nedeninden biri. Yapay zeka saldırıları daha hızlı ve etkili hale getirdikçe, yöneticilerin endişeleri haklı olarak artıyor. Artık bu endişeyi eyleme dönüştürme zamanı.

Katmanlı savunmalar önem taşıyor. Bunların etkili eğitim ve farkındalık programları, risk bazlı yamalama, düzenli yedekleme, uygulama kontrolleri, kötü amaçlı yazılımlarla mücadele, ağ izleme ve düzenli olarak test edilen bir olay müdahale planını içermesi gerekiyor. Ayrıca, sağlam bir kimlik güvenliği stratejisi kesinlikle temel taşı niteliğinde. Tüm çalışan ve makine kimlikleriniz üzerinde kapsamlı ve merkezi görünürlük ile kontrol sağlamak, kötü niyetli aktörleri dışarıda tutmanıza ve kaynaklarınızı ele geçirmeleri durumunda verebilecekleri zararı sınırlamanıza yardımcı olur.

Tedarikçileri değerlendirirken zaman ayırın. Oturum izleme ve akıllı yetkilendirme gibi yapay zeka destekli özellikler sunan güvenilir bir isim seçin. Bu, bir taraftan engelleri en aza indirir, dirençliliği artırır ve fidye yazılımı savunmasını optimize ederken diğer taraftan sıfır güven için yolu açar.

İşinizi inşa ederken ve çalışanlarınızın gücünü kullanırken güvenlikten ödün vermeden ihtiyacınız olan huzuru sağlar.

Fidye yazılımıyla mücadelede güçlü bir Kimlik Güvenliği stratejisinin nasıl yardımcı olabileceğini öğrenmek için Delinea.com'u ziyaret edin.

Delinea

Her etkileşimde kimlik güvenliği

Delinea, akıllı ve merkezi yetkilendirme yoluyla insan ve makine kimliklerinin güvence altına alınmasında öncü bir role sahiptir ve modern firma genelindeki etkileşimlerini sorunsuz bir şekilde yöneterek kuruluşları destekler. Delinea'nın yapay zeka destekli istihbarattan yararlanan bulut tabanlı Kimlik Güvenliği Platformu, bağlamı kimliğin tüm yaşam döngüsü süresince, bulut ve geleneksel altyapı, veriler, SaaS uygulamaları ve yapay zeka genelinde uygular. Bu platform çalışan işgücü, BT yöneticisi, geliştiriciler ve makineler dâhil olmak üzere tüm kimlikleri keşfetmenize, uygun erişim seviyeleri atamanıza, kural dışı durumları tespit etmenize ve tehditlere gerçek zamanlı olarak yanıt vermenize olanak tanıyan tek platformdur. Delinea Platformu, aylar yerine haftalar içinde dağıtımı mümkün kılarak, yönetim için en yakın rakibe kıyasla %90 daha az kaynak gerektirerek ve %99,995'lik çalışır durumda kalma süresi sağlayarak, karmaşıklık olmadan sağlam güvenlik ve operasyonel verimlilik sunar. Delinea hakkında daha fazla bilgiyi **Delinea.com**, **LinkedIn**, **X** ve **YouTube** sitelerinde bulabilirsiniz.