Synology®

Kuruluşunuzu fidye yazılımlarına karşı koruyun

Fidye yazılımı saldırılarının, kuruluşlar için sadece 2023 yılında toplam 8 trilyon ABD doları tutarında maliyete yol açması öngörülüyor.[1] Hızlı geri yükleme seçenekleri sunan veri koruma planları, fidye yazılımların ve diğer siber suç türlerinin etkisini azaltmak için çok önemlidir.

Date 13 Eki 2023

Yedeklemeler: Felaket durumunda son savunma hattı

Kötü amaçlı silme veya değiştirme sonrasında veriler kaybolduğunda, yedeklemeler sayesinde kritik görev verilerinizi geri yükleyin ve maliyetli kesintileri önleyin. Tüm BT altyapınız için bir yedekleme stratejisi tasarlamak üzere Synology'nin veri koruma çözümlerinden yararlanın.

Eksiksiz koruma

Verileriniz için birden fazla güvenlik ağı oluşturmak üzere uç noktaları ve birincil yedekleri koruyun.

Hızlı kurtarma

Anında kurtarma seçenekleriyle, felaket durumunda kesintileri en aza indirin.

Değişmez depolama

Verilerde ve anlık görüntülerde yetkisiz değişiklikler yapılmasını önleyin.

Lisanssız yedeklemeler

Sınırlama olmadan veya gizli ücretler ödemeden depolamanızın izin verdiği ölçüde veri yedekleyin.

Fidye yazılımlarına karşı merkezi koruma

İş istasyonu filolarından, sunuculardan, sanal makinelerden ve bulut uygulamalarından gelen yedeklemeleri birleştirin. Veri tekilleştirme ve artımlı yedekleme teknolojileriyle, depolama tüketimini optimize edin ve bant genişliğinden kaynaklanan sorunlardan kaçının. https://www.synology.com/dsm/solution/infrastructure

Fiziksel iş yükleri

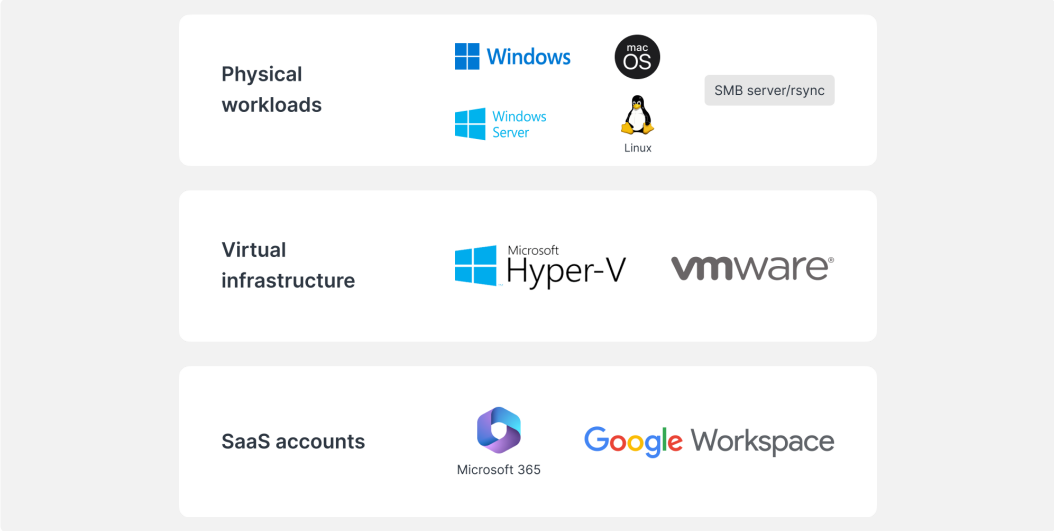
Kapsamlı bare metal yedekleme ve dosya düzeyinde esnek kurtarma ile kötü amaçlı saldırılar sırasında uç noktaları koruyun.

Sanal altyapı

VMware® vSphere™'i, Microsoft® Hyper-V® VM'leri ve LUN'leri güçlü veri azaltma teknolojileriyle yedekleyin.

SaaS hesapları

Yeni eklenen hesapların otomatik olarak algılanmasıyla bulutta depolanan verilere yönelik sürekli korumadan faydalanın.



Verimli kurtarma

Yerel veya tesis dışı bir Synology sisteminden yedeklemeleri hızla geri yükleyerek kritik üretim sistemlerinin kullanım dışı süresini en aza indirin.

Sıfıra yakın RTO

İşinize mümkün olan en kısa sürede devam edebilmek için yedekleme görüntülerini VMware®'a, Hyper-V®'ye veya Synology Virtual Machine Manager'a ekleyin. Hizmet kesintisini önlemek için VM'leri alternatif bir hipervizöre geri yükleyin.

Minimum RPO

Yedekleme sıklığını ihtiyaçlarınıza göre yapılandırarak saldırı sırasında potansiyel olarak etkilenen veri miktarını en aza indirin. Artımlı yedeklemeler ve veri tekilleştirme teknolojisi sayesinde sistemleri hızlı bir şekilde koruyun.

Sezgisel çalışma

Çalışanların e-postaları, kişileri ve dosyaları geri yüklemeden önce uygun bir portaldan incelemesine ve önizlemesine imkan tanıyarak daha kullanıcı dostu bir deneyim sunun ve BT ekiplerinin üzerindeki yükü azaltın.

Ekstra güvenlik katmanı ekleme

3-2-1 yedekleme stratejisini uygulayarak üçüncü bir veri setini tesis dışında veya bulut üzerinde saklayın ve verilerinizi yangına, doğal afete veya hırsızlığa karşı koruyun.

Tesis dışı sunucularda

Yedeklemeleri fiziksel felakete karşı korumak için ikinci bir konumda yer alan bir Synology sunucusunda saklayın ve fidye yazılımı korumasını artırmak için değişmez anlık görüntüleri çoğaltın.

Bulut üzerinde

Tüm büyük bulut depolama sağlayıcılarında yedekleme yaparak istemci tarafı AES-256 şifreleme ile verilerinizi yetkisiz erişime karşı koruyun. https://c2.synology.com/storage/nas

Farklı sektörlerin güvendiği çözüm

"Synology [...], sunucu donanım masraflarını azaltmamıza olanak tanırken [...] altyapı ve iş istasyonu yedeklerini, sistem günlük kayıtlarını ve dosya yönetimini çok daha kolay hale getirdi."
https://www.synology.com/company/case_study/Investortools

"Active Backup for Business sayesinde, tüm yedeklemelerimiz artık merkezidir ve 7/24 kullanılabilir. Bu sayede kesinti süresini en aza indirebilir ve FERPA yönetmeliklerine uyumlu kalabiliriz."
https://www.synology.com/company/case_study/University_of_Washington

"[...] Active Backup for Business inanılmaz yedekleme hızlarına sahip ve tekrarlayan verileri silme konusunda harikalar yaratıyor. Sunucudaki toplam 58 TB alanın yalnızca 28 TB'sini kapladı. [...]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[...] Active Backup for Business, [...] tüm yedekleme görevlerini tek bir konsolda merkezileştirmemizi ve buradan yönetmemizi sağlıyor. Hızlı ve güvenilir kurtarma da iş devamlılığını sağlıyor."
https://www.synology.com/company/case_study/UNESCO

Sık Sorulan Sorular

Fidye yazılımı nedir?

Fidye yazılımı, mağdurların dosyalarını şifreleyen kötü amaçlı bir yazılım türüdür. Saldırı sonrasında saldırganlar, veri erişimini geri yüklemek için fidye talep eder ve genellikle fidye ödenmediği takdirde, verileri kalıcı olarak imha etmekle tehdit ederler. Fidye yazılımı saldırıları ciddi sorunlara yol açabilir ve hem kişiler hem de kuruluşlar için önemli mali kayıplarla sonuçlanabilir. Yazılımlarınızı güncel tutarak ve dosyalarınızı düzenli olarak yedekleyerek kendinizi ve cihazlarınızı fidye yazılımlarına karşı korumanız önemlidir.

Ne tür fidye yazılımları bulunur?

Birçok farklı fidye yazılımı türü vardır ve sürekli olarak yenileri geliştirilmektedir. En yaygın fidye yazılımı türlerinden bazıları şunlardır:

- **Şifreleyen fidye yazılımı**: En yaygın fidye yazılımı türüdür; mağdurların dosyalarını şifreler ve bunlara şifre çözme anahtarı olmadan erişmeyi engeller. Saldırının ardından saldırganlar, anahtar karşılığında fidye ödemesi talep eder
- **Kilitleyen fidye yazılımı**: Bu fidye yazılımı türü, oturum açma bilgilerini değiştirerek mağdurun bilgisayarını kilitler veya sistemine erişmesini engelleyen bir mesaj görüntüler. Saldırının ardından saldırganlar bilgisayarın kilidini açma karşılığında fidye ödemesi talep eder
- **Hizmet olarak fidye yazılımı (RaaS)**: Saldırganların, saldırıyı gerçekleştirmeleri için başka kişilere veya gruplara fidye ödediği bir iş modelidir. İlk taraf genellikle fidye yazılımı sağlayıp ödemeleri yönetir, ikincisi taraf ise fidye ödemelerinden pay alır
- **Korkutma yazılımı**: Mağduru korkutarak fidye ödemesini sağlamayı amaçlayan fidye yazılımı. Genellikle kurbanın bilgisayarına virüs bulaştığını iddia eden sahte güvenlik uyarılarının veya mesajların görüntülenmesini sağlar. Saldırının ardından saldırgan, bulaştığı iddia edilen virüsü kaldırmak için fidye ödemesi talep eder

Fidye yazılımları nasıl yayılır?

Fidye yazılımları, genellikle kimlik avı e-postaları aracılığıyla veya bir bilgisayar sistemindeki güvenlik açıklarından faydalanarak yayılır. Kimlik avı saldırısında, saldırgan yasal bir kaynaktan (ör. banka veya bilinen bir şirket) geliyor gibi görünen bir e-posta gönderir. E-posta genellikle, tıklandığında mağdurun bilgisayarına fidye yazılımı yükleyen bir bağlantı veya ek içerir. Sistemdeki güvenlik açıkları benzer şekilde kullanılır ancak bu durumda saldırgan, fidye yazılımını mağdurun bilgisi olmadan yüklemek için sistemin güvenliğinde bulunan bir hatadan faydalanır. Her durumda, fidye yazılımı yüklendikten sonra aynı ağda bulunan diğer bilgisayarlara hızla yayılabilir.

Fidye yazılımı saldırısında yaşanan tipik süreç nedir?

Fidye yazılımı saldırısının adımları genellikle şu şekildedir:

1. Saldırgan, bir kimlik avı e-postası göndererek veya sistemdeki bir güvenlik açığından yararlanarak kurbanın bilgisayarına erişim kazanır
2. Saldırgan mağdurun bilgisayarına erişim kazandığında sisteme fidye yazılımını yükler
3. Ardından fidye yazılımı mağdurun dosyalarını şifreler ve dosyalarına erişmesini engeller
4. Bundan sonra saldırgan, genellikle şifrelenmiş dosyaların kilidini açacak bir şifre çözme anahtarı karşılığında, Bitcoin gibi dijital bir para birimi cinsinden fidye talep eder
5. Mağdurun fidyeyi ödemesi halinde, saldırgan şifre çözme anahtarını sağlar ve mağdur dosyalarına tekrar erişebilir. Ancak saldırganın anahtarı sağlayacağının bir garantisi yoktur ve bunu yapsa bile, mağdurun dosyaları şifreleme işlemi sonucunda zarar görmüş veya bozulmuş olabilir

Bu sürecin farklı şekillerde gerçekleşebileceğini ve tüm fidye yazılımı saldırılarının tam olarak bu adımlara göre gerçekleşmeyebileceğini belirtmek önemlidir. Örneğin, bazı saldırılarda dosyalar şifrelenmeyebilir, başkalarında ise farklı tehdit veya şantaj biçimleri kullanılabilir.

Fidye yazılımları nasıl bulaşır?

Fidye yazılımları birkaç farklı yoldan bulaşabilir. En yaygın yollardan biri, bir kimlik avı e-postasındaki kötü amaçlı bir bağlantıya veya eke tıklamaktır. Bu tür e-postalar meşru görünecek şekilde tasarlanmıştır ve genellikle tanınmış bir şirket veya kuruluştan gelmiş gibi görünür. Bağlantıya veya eke tıkladığınızda, bilgisayarınıza fidye yazılımı yüklenir. Fidye yazılımın bulaşabileceği bir diğer yol da riskli bir web sitesini ziyaret etmektir. Bu web siteleri saldırganlar tarafından ele geçirilmiştir ve saldırganlar, siteyi ziyaret ettiğinizde bilgisayarınıza fidye yazılımını otomatik olarak yükleyecek bir kod yerleştirmiştir. Fidye yazılımları, virüs içeren dosyaları internetten indirdiğinizde de bulaşabilir. Bu, örneğin şüpheli bir web sitesinden bir dosya indirdiğinizde veya tanımadığınız bir kişinin paylaştığı bir dosyayı indirdiğinizde gerçekleşebilir. Kısacası, internette gezinirken dikkatli olmak ve tanımadığınız kaynaklardaki bağlantılara tıklamaktan ve buralardan dosya indirmekten kaçınmak önemlidir. Bu, fidye yazılımlarına ve diğer kötü amaçlı yazılım türlerine karşı korunmanıza yardımcı olabilir.

Fidye yazılımının hedefleri kimlerdir?

Fidye yazılımı saldırıları, internete bağlı olan bir bilgisayar veya başka bir cihaz kullanan herkesi hedef alabilir. Ancak bazı grupların diğerlerine göre hedef alınması olasılığı daha yüksektir. Örneğin, fidye yazılımı saldırıları genellikle işletmeleri hedef alır, çünkü bunlar genellikle daha değerli verilere sahiptir ve bu verileri geri almak için fidye ödemeye daha istekli olabilirler. Hastaneler, okullar ve kritik hizmetler sağlayan diğer kuruluşlar da sıklıkla hedef alınır, çünkü fidye yazılımı saldırıları operasyonlarını kesintiye uğratabilir ve insanların yaşamlarını riske atabilir. Kişiler de fidye yazılımı saldırılarının hedefi olabilir. Bu gibi durumlarda saldırganlar, mağduru fidye ödenmediği takdirde kişisel dosyalarını silmekle veya hassas bilgilerini yayınlamakla tehdit ederek ondan para almaya çalışabilir. Fidye yazılımı saldırılarının hedefleri, genellikle verilerinin değerine ve verileri geri alma karşılığında fidye ödemeye ne kadar istekli olacaklarına göre seçilir.

Fidyeyi ödemenin riskleri nelerdir?

Bir fidye yazılımı saldırganına fidyeyi ödemek dosyalarınızı geri almanın en kolay yolu gibi görünebilir ancak bu çok riskli bir karar olabilir. Fidyeyi ödemenin aşağıdakiler gibi birçok risk vardır:

- Saldırganın şifre çözme anahtarını sağlayacağı garanti edilmez. Fidyeyi ödeyen mağdurlar çoğu durumda anahtarı asla alamaz ve dosyalarına erişemez
- Fidyeyi ödemek saldırganları saldırıları sürdürmeye teşvik edebilir. Saldırganlar mağdurların fidyeyi ödeme konusunda istekli olduğunu bildiğinde gelecekte daha fazla saldırı gerçekleştirme olasılıkları daha yüksek olabilir
- Fidyeyi ödemek gelecek saldırılarda hedef alınmanıza yol açabilir. Saldırgan fidye ödeme konusunda istekli olduğunuzu bildiğinde gelecekte sizi hedeflemesi ihtimali daha yüksek olabilir
- Fidyeyi ödemeniz yasal olmayabilir. Bazı durumlarda, bir suç örgütüne fidye ödemek terör veya diğer yasa dışı faaliyetlere kaynak sağlama şekli olarak değerlendirilebilir

Fidyeyi ödemek dosyalarınızı almanın en kolay yolu gibi görünse de, aslında bu çok riskli bir karar olabilir. Bir karar vermeden önce riskleri dikkatli bir şekilde değerlendirmek önemlidir.

Fidye yazılımının maliyeti nedir?

Fidye yazılımı saldırısının maliyeti; kullanılan fidye yazılımı türü, şifrelenmiş dosyaların sayısı ve saldırının etkinliği gibi çeşitli faktörlere bağlı olarak büyük ölçüde değişebilir. Bazı durumlarda fidye yazılımı saldırısının maliyeti nispeten düşük olabilir ve saldırganlar birkaç yüz dolar fidye talep edebilir. Diğer durumlarda maliyet çok daha yüksek olabilir ve saldırganlar mağdurun dosyalarına yeniden erişim sağlamak için binlerce dolar veya daha fazlasını talep edebilir. Fidye ödemeye ilişkin doğrudan maliyetlerin yanı sıra, fidye yazılımı saldırılarının önemli dolaylı maliyetleri de olabilir. Örneğin, fidye yazılımı saldırısı kesintiye ve üretkenlik kaybına yol açarak gelir ve kâr kaybıyla sonuçlanabilir. Ayrıca bir şirketin itibarına ve müşteri güvenine zarar verebilir ve bu da iş üzerinde uzun vadeli olumsuz etkilere yol açabilir. Bu tür dolaylı maliyetler genellikle fidyenin maliyetinden çok daha yüksektir.

Fidye yazılımının belirtileri nelerdir?

Fidye yazılımı saldırısının belirtileri, kullanılan belirli fidye yazılımı türüne bağlı olarak değişebilir. Ancak bazı yaygın belirtiler şunlardır:

- Dosyalarınız şifrelenir ve bunlara erişemezsiniz
- Saldırgandan şifre çözme anahtarı karşılığında fidye ödemesi talep eden bir mesaj alırsınız
- Bilgisayarınızda tanımadığınız programların veya işlemlerin yürütüldüğünü görürsünüz
- Bilgisayarınız yavaşlar veya yanıt vermez
- Bilgisayarınızda olağan dışı hata mesajları veya açılır pencereler görüntülenir

Bilgisayarınıza fidye yazılımı bulaştığından şüpheleniyorsanız hızlıca harekete geçmeniz önemlidir. Fidye yazılımının yayılmasını önlemek için bilgisayarınızın internet bağlantısını kesin.

Fidye yazılımı saldırıları nasıl önlenir?

Fidye yazılımı saldırılarını önlemek için atabileceğiniz birkaç adım vardır. Bunlardan bazıları şöyledir:

- Saygın bir antivirüs veya güvenlik yazılımı kullanın ve güncel tutun. Bu bilgisayarınızı fidye yazılımlarına ve diğer kötü amaçlı yazılım türlerine karşı korumaya yardımcı olabilir
- E-posta eklerini veya bağlantılarını açarken dikkatli olun. Fidye yazılımları sıklıkla kimlik avı e-postaları aracılığıyla gönderilir. Bu yüzden nelere tıkladığınız konusunda dikkatli olmalısınız
- İşletim sisteminizi ve diğer yazılımlarınızı güncel tutun. Yazılım güncellemeleri, genellikle bilgisayarınızı fidye yazılımlarına ve diğer tehditlere karşı korumaya yardımcı olabilecek güvenlik yamaları içerir
- Dosyalarınızı düzenli olarak yedekleyin. Bu, bilgisayarınıza fidye yazılımı bulaşmışsa verilerinizi korumanıza yardımcı olabilir. 3-2-1 yedekleme stratejisi gibi önerilen yedekleme stratejilerinden birine uyduğunuzdan emin olun
- Fidye yazılımı risklerinin farkında olun ve kuruluşunuzdaki diğer kişileri bu tehditler hakkında bilgilendirin. Bu, fidye yazılımı saldırılarının önlenmesine yardımcı olabilir ve gerçekleştiklerinde bunları algılamayı ve bunlara yanıt vermeyi kolaylaştırır

Fidye yazılımı saldırılarını önlemenin en iyi yolu dikkatli olmak ve gerekli adımları atarak bilgisayarınızı ve verilerinizi korumaktır. Bu, fidye yazılımı saldırısı riskini azaltmaya yardımcı olabilir ve gerçekleşmesi halinde verilerinizi kurtarmayı kolaylaştırabilir.

Synology beni fidye yazılımlarına karşı nasıl koruyabilir?

Fidye yazılımlarının kurbanı olmamak için önleyici faaliyetler çok önemlidir. Seçtiğiniz antivirüs yazılımına ek olarak bu Synology çözümlerini kullanın:

- **Erişimi engelleyin**: Secure SignIn ve C2 Password'ü kullanarak dosya, uygulama ve erişim izinleri ayarlayın ve güvenli oturum açma bilgileri yapılandırarak fidye yazılımının yayılmasını azaltın
- **Cihazları koruyun**: Eski sistemler daha fazla risk altındadır. Tüm NAS'nizi Synology Central Management System (CMS) ile tek seferde güncelleyin. Ayrıca Synology Directory Server ve C2 Identity'deki grup ilkelerini kullanarak diğer cihazları da koruyun
- **Şüpheli dosyaları açmaktan kaçının**: Spam e-postaları ve şüpheli dosyalar içeren kimlik avı e-postaları, fidye yazılımlarını yaymanın yaygın yöntemleridir. Synology MailPlus kötü amaçlı yazılımlardan korunmaya ve spam önlemeye yönelik güçlü bir çözüm sağlar
- **Güvenlik açıklarını kontrol edin**: Kötü amaçlı yazılımları, güvenlik açıklarını ve anormal oturum açma etkinliklerini düzenli olarak taramak için Synology Security Advisor'ı kullanın. NAS güvenliğinizi artırmak için önerilen değişiklikleri uygulayın. https://www.synology.com/dsm/overview/security

Verilerinizi korumanın diğer yolları

Filonuzu yönetin

Veri erişim izinlerini, yazılım durumunu, sistem sağlığını ve daha fazlasını merkezi olarak yönetmek için kapsamlı özelliklerden yararlanın.
https://www.synology.com/dsm/overview/administration

Tüm sistemlerinizi izleyin

Cihazlarınız nerede olursa olsun şüpheli oturum açma etkinliklerini belirleyin, güncellemeleri yönetin ve cihazların sağlık durumunu izleyin.
https://www.synology.com/dsm/feature/active-insight

Verilerinizi koruyun

Verilerinizi yanlışlıkla silmeye ve kötü amaçlı yazılımlar tarafından değiştirmeye ya da silinmeye karşı korumak için 3-2-1 yedekleme kuralını uygulayın.
https://www.synology.com/dsm/solution/data_backup

Her açıdan koruyun

Siber güvenlik kontrol listemizi indirin ve bir bilgisayar korsanı saldırısı durumunda zayıf noktalarınızı belirleyin.
https://global.download.synology.com/download/Document/Software/Brochure/Firmware/DSM/7.0/trk/Se

Başlayın

Bize ulaşın

Daha fazla bilgi için bölgesel satış ekibiyle iletişime geçin
https://www.synology.com/form/inquiry/sales

Nereden satın alınır?

Bölgenizde bir Synology iş ortağı bulun
https://www.synology.com/wheretobuy

Notlar:

1. eSentire, 2022 Resmi Siber Suç Raporu
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Kuruluşunuzu fidye yazılımlarına karşı koruyun

https://www.synology.com/tr-tr/dsm/solution/ransomware

Synology Web Sitesi

https://www.synology.com/

Bize ulaşın

https://www.synology.com/company/contact_us