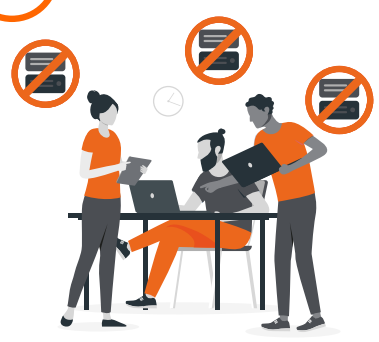
İhmal edilen yazılım güvenlik açıkları

Birçok hasar, güvenlik açığı bulunan yazılımların, siber suçluların istismar etme fırsatı bulmadan önce yamalanması ile önlenebilir. Aşağıdaki hasar örnekleri, yazılımı güncel tutmanın ne kadar önemli olduğunu gösteriyor. Ayrıca bilinen güvenlik açıklarından nasıl yararlanıldığı ve bunun sonucunda ortaya çıkan hasarların nasıl düzeltildiği incelenerek, detaylı bir şekilde ortaya konuluyor.

- Sunucu güvenlik açığı uyarı ikazı

1



1. Olay

16 Temmuz'da Örnek Şirket'in dış satışl ekibi, BT ekibini hiçbir sistemi kullanamadıklarına dair bilgilendirdi. Sunucu istatistiklerine bakıldığında, birçok sistemin çevrim dışı olduğunu görüldü. BT ekibi ilk soruşturmanda, sunucuların şifrelendiğini gösteren bir mesajla karşılaştı.. Şirketin bir fidye yazılımı saldırısının kurbanı olduğu sonucuna vardılar. Örnek Şirket'in BT ekibi, Chubb'ın Siber Olay Müdahale Merkezi ile temasa geçti. Soruşturmayı desteklemek üzere, bir olay yöneticisi ve BT adli tıp uzmanı görevlendirildi.

Sistemlerin ilk incelemesinde, ağın ve altyapının büyük bölümünün bir tehdit aktörü tarafından ele geçirildiği tespit edildi.

2

2. Sorun

Bunun üzerine Örnek Şirket, sunucuları kapatarak saldırıyı hızla kontrol altına aldı. Ancak tehdit aktörü, şirketin veri merkezlerindeki sanallaştırılmış sunucuları ve hipervizörleri çoktan şifrelemişti. Kurtarma seçeneklerini değerlendirirken, tehdit aktörü yedekleri şifreleyemediği veya onlara zarar veremediği için, yedeklemeleri kullanarak BT ortamını tamamen geri yüklemenin mümkün olduğunu gördüler. Örnek Şirket'in yedekleme stratejisi, BT'sini fidye yazılımı saldırılarına karşı daha iyi korumak için, çevrim dışı yedeklemeleri muhafaza ederek ve kimlik doğrulamasını Active Directory'den ayrı yedekleme sunucularında saklayarak, 12 ay önce güncellenmişti.

Sonraki günlerde BT müfettişleri ve adli tıp uzmanları, varlıkların kurtarılmasına öncelik verirken, durum değerlendirmesi yaparak ve tehdit aktörü ile iletişim kurarak, Örnek Şirket'e yardımcı oldu. Aynı zamanda, kurtarma işleminin güvenli ve sağlıklı ilerlemesi için, , olayın temel nedeni ve etkisine ilişkin adli araştırma başlattılar. Bu kapsamda, fidye notunda yer alan verilerin niteliğinin ve miktarının da doğruluğunu araştırarak, , tehdit aktörünün verileri şantaj amacıyla sızdırıp sızdırmadığını incelediler.

Yedeklemelerdeki günlük veriler incelendiğinde, tehdit aktörünün yaklaşık bir ay önce, 19 Haziran'da, “Fred.Bloggs” hesabına ait kimlik bilgileri ile 6X.XXX.XX.232 adresinden Avrupa'daki bir SSL-VPN sunucusuna giriş yaptığı görüldü. VPN sunucusu yerel olarak yönetiliyor ve güncel olmayan 6.2.0-vr sürümü kullanılıyordu. Bu giriş, TOR çıkış düğümü olduğu bilinen bir IP'den kaynaklanıyordu ve normalde bir kullanıcı TOR ağını kullanarak giriş yapmayacağı için şüpheliydi. Tehdit aktörü yaklaşık 25 dakika sonra, bu kez coğrafi olarak Örnek Şirket'in faaliyet göstermediği bir ülkede konumlandırılmış bir IP kullanarak tekrar kimlik doğrulaması yaptı.

Tehdit aktörü bir saatten kısa bir süre sonra, bir etki alanı yönetici hesabına erişim sağlayarak erişim ayrıcalıklarını artırdı. Bunu yapabildi, çünkü bu hesabın kimlik bilgileri, etki alanına bağlı tüm Windows cihazınlarındaki yapılandırma dosyalarında saklanıyordu. Bu, tehdit aktörünün İngiltere ve Almanya'da bulunan ve Örnek Şirket'in Avrupa operasyonlarını destekleyen sunucular ve hipervizörler arasında yatay olarak hareket etmesine izin verdi.

Temmuz ayında tehdit aktörü, uzaktan erişim yazılımı ve yazılım dağıtım aracı yükleyerek kalıcılık yarattı. Bu, fidye yazılımının etki alanındaki tüm sunuculara dağıtmasına ve yayılmasına olanak sağladı. Neyse ki uç noktalar, yani dizüstü bilgisayarlar ve iş istasyonları, sunucularda çalışmayan gelişmiş bir antivirüs birimi aracılığıyla fidye yazılımını engelleyebildiler.

"Fred.Bloggs" hesabından yapılan başarısız oturum açma girişimlerine dair kayıt bulunmadığından, tehdit aktörünün kaba kuvvet saldırısı gerçekleştirmeyeceği, , zira geçerli kimlik bilgilerine sahip olduğu anlaşıldı. Kayıtlarda r ayrıca, VPN yazılımının 6.2.0-vr sürümündeki bilinen bir güvenlik açığından (CVE-2022-123XXX) yararlanan tehdit aktörünün kod etkinliğini de görülüyordu. Bu güvenlik açığı istismar edildiğinde, bir kullanıcının yakın zamanda kullandığı geçerli kimlik bilgilerini elde etmesine olanak tanır. Tehdit aktörü, bu giriş yöntemini kullandığını, fidye notunda ve müzakereler sırasında doğruladı.

3

3. Çözüm

Yedeklemelerin kötü amaçlı yazılımdan etkilenmediğinin teyit edilmesinin ardından, veri ve sistem kurtarma çalışmaları ve güncellenmiş yapılandırma çalışmaları sonraki beş gün boyunca devam etti. Bu çalışmalar başarılı olduğundan, tehdit aktörü ile daha fazla müzakere etmeye gerek kalmadı ve herhangi bir fidye de ödenmedi.

Ulusal Güvenlik Açığı Veri Tabanı’nda ve VPN yazılım sağlayıcısının destek web sitesinde listelendiği üzere, yazılımın 6. sürümünde keşfedilen kritik bir güvenlik açığı vardı. Bu açık, kimlik bilgilerinin çalınmasına ve sisteme girilmesine izin veriyordu ve ilk olarak bu yılın Ocak ayında tespit edilmişti. Ortak Güvenlik Açığı Puanlama Sistemi’nde (CVSS), kritik olarak kabul edilen 9,8 puan ve CVE-2022-123XXX tanımlayıcısı verildi. Yazılım sağlayıcı, 2 Şubat'ta bu güvenlik açıkları için bir yama oluşturdu (sürüm 6.2.1-vr) ve aynı gün, Örnek Şirket de dahil olmak üzere, müşterilerine bir e-posta göndererek, kullanıcılara yamayı mümkün olan en kısa sürede uygulamalarını tavsiye etti.

4

4. Sonuç

Örnek Şirket’in, yamanın yayınlanması ile güvenlik açığının istismar edilmesi arasında, tam olarak 137 günü vardı. Olaya müdahale, veri ve sistem kurtarma maliyetleri, siber şantaj ve iş kesintisi kaybına ilişkin sigorta maddelerinin tümü, başlangıçta siber olaya yanıt olarak tetiklendi ve 137 gün boyunca, poliçe programında listelenen geçerli 'ihmal edilmiş yazılım olayı' limitlerine, aşımına ve koasüransa tabi tutuldu.

Chubb daha sonra Olay Müdahale Yöneticisi, BT adli tıp uzmanları, avukatlar ve halkla ilişkiler uzmanları, iş kesintisi kaybı, veri ve sistem kurtarma maliyetleri ve siber şantaj giderlerine yönelik olay müdahale maliyetlerini gözden geçirerek, talebi standart yöntemle düzenledi.

İhmal edilen yazılım güvenlik açıkları

- Bilinen güvenlik açığı, yama yok

1

1. Olay

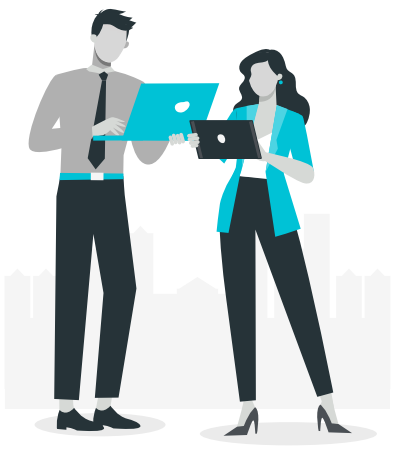
Bir hafta sonunda Örnek Şirket, bilgisayar sistemlerine ve sunucularına yetkisiz erişim tespit etti. Erişim, bilgisayar korsanlarının Örnek Şirket'in bilgisayar sistemlerine, sunucularına ve buralardaki verilere erişmesine olanak sağlayan, bilinen, ciddi ve yaygın bir güvenlik açığı yoluyla elde edilmişti. Bilgisayar korsanları hem sistemleri şifrelemiş hem de verileri dışarı sızdırmıştı.

2

2. Sorun

Örnek Şirket, sunucuları kapalı olduğu için müşterilerin siparişlerini işleme koyamıyor veya tamamlayamyordu. Çalışanlar, sunucuların kapalı kaldığı her 24 saat için, şirketin 750.000 € kâr kaybedeceğini tahmin ediyordu. Bilgisayar korsanı, şifre çözme anahtarlarını sağlamak ve sızdırılan verileri yayınlamamak için 2 milyon dolar fidye talep etti ve ödeme almadıkları takdirde, talebi düzenli aralıklarla artırma tehdidinde bulundu.

3



3. Çözüm

Örnek Şirket, olayın farkına varır varmaz durumu rapor etti ve hızla, ilk bulgulara dayanarak olayı değerlendirebilecek bir Olay Müdahale Yöneticisi görevlendirildi. Olay Müdahale Yöneticisi derhal, Örnek Şirket'e soruşturma ve kontrolü sağlamada yardımcı olması için, uzman bir adli BT şirketini görevlendirdi.

Olay müdahale ekibi de Örnek Şirket'e yardımcı oldu. Hızlı bir şekilde avukatlar, halkla ilişkiler personeli ve şantaj uzmanları ile görüştüler. Ekip daha sonra, yedeklerden geri yüklenebilecek sunucuların belirlenmesini içeren bir hafifletme stratejisi uyguladı.

Nihayetinde, BT ekibi ve şantaj uzmanlarının sızan verilerin hassas olmadığına karar vermesinin ardından, herhangi bir fidye ödenmedi. Sistemlerin, olaydan etkilenmeyen, güvenli bir şekilde ayrılmış yedeklemelerden büyük ölçüde geri yüklenebileceğini gördüler.

Olay müdahale ekibi, fidye yazılımının etkilenen sunuculardan kaldırılmasına ve bilinen güvenlik açığından yararlanılmasını önleyecek yama da dahil olmak üzere, sistemlerin geri yüklenmesine yardımcı oldu. Halkla ilişkiler ekibi, müşterilerle iletişim konusunda yardımcı oldu ve avukatlar, gerekli yasal ve düzenleyici kurumların bilgilendirilmesi konusunda Örnek Şirket'e destek oldu.

4

4. Sonuç

Sonuçta, operasyonlar tamamen normale döndü. BT adli tıp ekibi, olaydan 10 gün sonra bir rapor sundu. Raporda, erişimin elde edildiği yöntem, güvenlik açığı ile ilgili spesifik CVE ile yamaların kullanıma sunulduğu, ancak uygulanmadığı tarih de dahil olmak üzere, önerilen hafifletme yöntemleri yer alıyordu.

Olaya müdahales, veri ve sistem kurtarma maliyetleri, siber şantaj ve iş kesintisi kaybı sigorta maddelerinin tümü, siber olaya yanıt olarak başlangıçta tetiklendi. Ancak olay, bilinen bir güvenlik açığının istismar edilmesinden kaynaklanmıştı. Bu durum, olay sırasında bir yamanın mevcut olduğunu ancak uygulanmadığını ortaya koyan BT adli tıp raporu tarafından da doğrulandı. Rapor, bilgisayar korsanının sisteme tam olarak ne zaman erişim elde ettiğini ayrıntılı olarak açıkladı ve Örnek Şirket'in sistemlerinin yamasız kaldığı sürenin uzunluğuna dikkat çekti. Bu da ihmal edilen yazılım olayı limitleri kapsamında, doğru koasürans ve alt limitin uygulanmasını sağladı.