Geniş Çaplı Olay

Yaygın olarak kullanılan teknolojiye yönelik tek bir saldırı ve/veya bu teknolojinin arızalanması, sigorta sektörünün sigortalama kapasitesini aşan bir kümelenme riski yaratabilir. Chubb, poliçe sahiplerine teminat netliği ve piyasa istikrarı sağlamak amacıyla, bu tür Yaygın Olaylar için olumlu ve spesifik limitler, saklama payları (konservasyonlar) ve koasürans sağlıyor.r. Aşağıda, bazı varsayımsal geniş çaplı olay örnekleri yer alıyor.

- Küresel işletim sistemi siber saldırısı

1

1. Olay

Örnek Şirket'in 500 binden fazla bireysel müşterisi ve 5 bin ticari müşterisi vardır. Bir gün çalışanlar, popüler bir işletim sistemine dayanan iş istasyonlarına, kritik uygulamalara veya verilerine erişemediklerini fark ettiler. Neyse ki, BT ekibinde farklı bir işletim sistemi çalıştıran cihazları kullanarak erişim sağlayabilen birkaç kullanıcı vardı ve bu kullanıcılar sorunun ne olduğunu analiz ettiler. Yapılan ilk incelemede, sunucu işletim sisteminde birden fazla dahili sistemi ve müşteri hesap portallarını etkileyen kritik sorunlar olduğu görüldü.

2

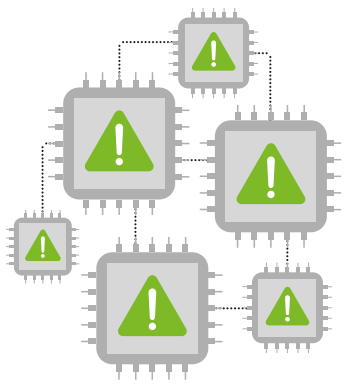
2. Sorun

Örnek Şirket, olayın farkına varır varmaz durumu rapor etti ve hızlı bir şekilde bir Olay Müdahale Yöneticisi (IRM) görevlendirdi. Olay Müdahale Yöneticisi, ilk bulgulara dayanarak olayı önceliklendirdi. IRM, Örnek Şirket'e soruşturmada yardımcı olması için uzman bir adli BT şirketini görevlendirdi. IRM, ayrıca avukatları ve halkla ilişkiler uzmanlarını da görevlendirdi.

Aynı gün medyada, birçok farklı sektörde, her ölçekten işletmenin siber saldırı kurbanı olduğuna ve sorunun yayıldığına dair çok sayıda haber yer aldı. Birçok rapora göre, tüm kurbanlar aynı sunucu işletim sistemini kullanıyordu. Ertesi gün devletin siber güvenlik kurumları resmi açıklamalar yayınladı., Saldırının, belirli bir işletim sistemindeki sıfır gün açığından faydalanarak gerçekleştirildiği, yaygın olarak kullanılan, halka açık bir bilgisayar ağı bağlantı noktası üzerinden yayıldığı belirtildi. Yazılım uygulamaları, işletim sistemine dayandığından, dünyanın dört bir yanında birçok işletmede uygulamaların işlevselliği, coğrafi konumları,, büyüklükleri veya faaliyet gösterdikleri sektörden bağımsız olarak ciddi şekilde etkilendi.

Olay müdahale ekibi, ayrıca bir hafifletme stratejisi ile destek verdi. Halkla ilişkiler ekibi, Örnek Şirket'in müşterilerini hizmet kesintisi ve bunun sebebi ilgili bilgilendirmek üzere çalışma yaptı. Hukuk danışmanları, ilgili yasal ve düzenleyici kurumların bilgilendirilmesine yardımcı oldu ve BT uzmanları, işletim sistemi sağlayıcısından ve güvenlik araştırmacılarından kurtarma tavsiyeleri beklerken, geçici çözüm olabilecek alternatif işletim sistemleri üzerinde çalıştı.

3



3. Çözüm

Sonraki birkaç gün boyunca güvenlik araştırmacıları, resmi siber güvenlik kurumları ve işletim sistemi geliştiricisi, saldırı ve güvenlik açığı ile ilgili bilgiler yayınladı. Ayrıca, olaydan etkilenen şirketler için tavsiyelerde bulundular ve henüz etkilenmemiş olsalar bile, tüm kullanıcılarının alması gereken önlemleri açıkladılar. Ulusal Standartlar ve Teknoloji Enstitüsü, güvenlik açığını, ciddi etki potansiyeli ve istismar edilebilirlik göz önüne alındığında, 10,0 taban puanına sahip bir Ortak Güvenlik Açığı ve Maruz Kalma (CVE) olarak listeledi. Bu, Ortak Güvenlik Açığı Puanlama Sistemi'nde (CVSS) yalnızca 'kritik' olaylara verilen en yüksek puandır. Raporlarda ayrıca saldırının, savunmasız açık bağlantı noktalarını arayan ve tüm pozitif eşleşmelerde işletim sistemi güvenlik açığından yararlanan gömülü bir araç üzerinden yayıldığına da ayrıntılarıyla yer verildi.

Bu, işletim sistemi geliştiricisi güvenlik açığını bulup bir yama oluşturmadan önce bilgisayar korsanları tarafından bilindiğinden ve istismar edildiğinden, bir sıfır gün güvenlik açığıydı. Yaygın olaydı, , çünkü tek bir eylem, Örnek Şirket'in sınırlı etki grubu dışındaki kuruluşları ve bireyleri de etkiliyordu. Sınırlı etki grubu, Örnek Şirket'in etkilenen işletim sistemini ve açık bağlantı noktalarını kullanması nedeniyle, bireysel ve ticari müşterilerini de içeriyor olabilirdi. Ancak uzmanlar raporlarında, bu güvenlik açığından Örnek Şirket ile hiçbir ilişkisi olmayan birçok başka kuruluşun da etkilendiğini ve dolayısıyla, bu tarafları sınırlı etki grubunun dışında bıraktığını vurguladı.

4

4. Sonuç

Olaya müdahale, veri ve sistem kurtarma maliyetleri ve iş kesintisi kaybı sigorta maddelerinin tümü, siber olaya yanıt olarak başlangıçta tetiklendi. Birkaç saat içinde bunun yaygın bir olay olduğuna işaret eden bilgilere ulaşıldığından, hasar talebi, poliçedeki yaygın olay bölümüne tabi oldu. Olay müdahalesi, veri ve sistem kurtarma maliyetleri ve iş kesintisi için sigorta sözleşmeleri kapsamındaki hasarlar, poliçede geçerli aşım ve koasürans uygulandıktan sonra, mevcut yaygın olay limitlerine kadar karşılandı.

Geniş Çaplı Olay

- Ortak yazılım çözümünde dünya genelinde kesinti

1

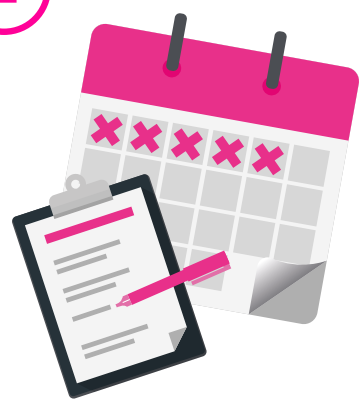
1. Olay

Örnek Şirket'in İngiltere, Fransa ve Almanya'da ofisleri bulunuyordu. Üretim ve satış yerleri, büyük bir yazılım sağlayıcısının bulut tabanlı bir Kurumsal Kaynak Planlama (ERP) çözümüne yönelik ortak bir aboneliğe dayanıyordu. Satış siparişlerinin işlenmesi, envanter yönetimi, üretim önceliklendirme, lojistik yönetimi ve bordro işlemleri ERP çözümü ile yapılıyordu.

İki hafta önce Örnek Şirket, sızma testi gerçekleştirdikten ve güncellemeden kaynaklanan herhangi bir performans sorunu olmayacağından emin olmak için, yeni sürümü bir test ortamında çalıştırdıktan sonra, ERP sistemini 2.3.2 sürümünden 3.0 sürümüne güncelledi.

Geçen hafta ERP sistemi çöktü ve Örnek Şirket'in erişimi kısıtlandı. Örnek Şirket, yazılım sağlayıcısının müşteri destek ekibi ile iletişime geçti ve Avrupa'daki birçok müşterinin kesintiden etkilendiğini öğrendi. Örnek Şirket ayrıca, bir Olay Müdahale Yöneticisi görevlendirmek ve Chubb'ın hasar departmanını olaydan haberdar etmek için Chubb Siber Olay Müdahale Merkezi ile de temasa geçti. İki saat içinde, yazılım sağlayıcısının web sitesinde, yaşanan sorunlarla ilgili özür mesajı yayınlandı. Üretim ortamlarındaki bir sistem açığını araştırdıklarını belirterek, daha fazla bilgi ve kurtarma önerisi için sayfanın düzenli aralıklarla tekrar bakılmasını tavsiye ettiler.

2



2. Sorun

Yazılım sağlayıcısı ertesi gün müşterilerine, olaydan etkilenip etkilenmediklerini kontrol etmek için nelere bakmaları gerektiğine dair bir açıklama ve bundan sonra ne yapmaları gerektiğini anlatan bir rehber içeren bir e-posta gönderdi. E-postada şu ifadeler yer alıyordu: "ERP 2.3 sürümünü kullanıyorsanız veya son üç hafta içinde 3.0 sürümüne güncellediyseniz ve erişilebilirlik sorunları yaşıyorsanız sorun, bulut hizmeti üretim sistemlerindeki kötü amaçlı faaliyetlerden kaynaklanmaktadır. Kurtarma girişimlerimiz devam etmektedir."

Örnek Şirket, ERP sistemini beş gün boyunca kullanamadı. Bu süre zarfında, siparişleri telefon ve e-posta yoluyla manuel olarak almaya başladılar. Üretim önemli ölçüde azaltılmış bir kapasite ile kısmen devam etti ve sipariş verilerine erişilemediğinden teslimatların durdurulması gerekti. Sistem nihayet yeniden kullanılabilir olduğunda siparişler, envanter, üretim durumu ve teslimatlar ile ilgili tüm geçmiş veriler silinmişti ve bunları geri getirme olanağı bulunmuyordu. Yazılım sağlayıcısı hem e-posta yoluyla gönderdiği hem web sitesinde yayınladığı mesajında, yıkıcı kötü amaçlı yazılımın, müşterilerin üretim verilerinin yanı sıra yedek kopyaları da bozduğunu doğruladı. Ayrıca, olayın Avrupa'da ve Kuzey Amerika'nın bazı bölgelerindeki 30 binden fazla ERP müşterisini etkilediği belirtildi.

3

3. Çözüm

Teminatın sınırlı etkili olay veya geniş çaplı olay bölümlerinin Örnek Şirket'in poliçesine uygulanıp uygulanmayacağını belirlemek için, bu olaydan kimlerin etkilendiğini ve neden etkilendiklerini değerlendirmemiz gerekiyordu. Yazılım sağlayıcısı tarafından yapılan açıklamalarda, etkilenen bulut ERP sürümlerini kullanan 30bin müşterinin, sağlayıcının üretim sistemlerindeki kötü amaçlı kod nedeniyle etkilendiği belirtildi. Diğer şirketler, Örnek Şirket ile olan ilişkileri nedeniyle değil, ERP sistemini seçmeleri nedeniyle etkilenmişti. Örnek Şirket müşteri olmasaydı bile, bu olaydan etkilenecekti.

4

4. Sonuç

Bu olayın Avrupa'daki müşterileri etkilediğine dair bilgi, kesintiden sonraki iki saat içinde Örnek Şirket'e gönderildi ve bu da olayın geniş çaplı olduğunun ilk göstergesi oldu. Bu nedenle, teminat altına alınan hasar tutarlarına geniş çaplı olay limitleri, aşım ve koasürans uygulandı. Buna koşullu iş kesintisi kaybı, manuel geçici çözümler ve veri kurtarma çabalarının maliyeti gibi veri ve sistem kurtarma maliyetleri, Olay Müdahale Yöneticileri maliyetleri ve siparişleri yeniden göndermesi veya geciken sevkiyatları yönetmesi gereken Örnek Şirket'in müşterileri ile iletişimi yöneten halkla ilişkiler ekibinin ve yapılan başka görevlendirmelerin maliyetleri de dahil edildi..