Vaka analizi

Penetrasyon testi sonuçlarına göre, Torvik Industries'de "The Wolf" tarafından gerçekleştirilen siber güvenlik ihlali HP yazıcılar tarafından durdurulabilirdi

Veri ihlaline dair resmi özet raporu

Sektör
Nakliye

Amaç
Ağda güvenlik açığının bulunduğu alanları analiz edip sorunları çözmek

Yaklaşım
Saldırıya uğranmasına neden olan güvenlik açıklarını bulmak için penetrasyon testi

Bulgular ve öneriler
- Kullanıcıları şüpheli e-postaları açıp ekleri basarken temkinli olmaları için eğitmek
- Tehdit algılama özellikli HP yazıcılarını dağıtmak
- Taşınan veya geçici konumlarda bulunan altyapı dahil olmak üzere tüm uç noktalarının güvenliğini yapılandırmak

İş farkı
Operasyonel kesintileri azaltıp markaya duyulan güveni artırmak için daha sıkı güvenlik önlemleri almak. Geçici konumlardaki ağ uç noktaların izlenmesine yönelik politikaları iyileştirmek.

Genel bakış

Torvik Industries*, her yıl 8 milyon konteynerin nakliyesini gerçekleştiriyor. 22.000 imalatçı ve toptancı için Torvik, ürünleriyle dünya çapındaki tüketiciler arasındaki en önemli bağ. Şirket varlıkları arasında tersaneler, gemiler, depolar ve Torvik'in geniş ağını destekleyen tüm teknoloji ekipmanları bulunuyor.

Şirket büyüdükçe, teknoloji altyapısı bu büyümeye uyum sağlamakta güçlük çekiyordu. BT güvenlik ekibi şirket sunucularını yapılandırırken, uydu şubeler veya geçici konumlarda bulunan bazı yazıcılar güvenlik için yönetime tabi tutulmuyordu.

23 Nisan 2018'de "The Wolf" olarak tanınan siber terörist, bilgisayarlardan vinçlere ve konteyner gemilerine kadar her yerde Torvik Industries'in faaliyetlerini kesintiye uğratmak için güvenli olmayan bir yazıcıyı kullandı. Şirketin güvenlik danışmanı, olayı analiz etmek için penetrasyon testi yönteminden yararlandı. Bunun sonucunda, güvenliğin artırılması ve çalışanların daha iyi eğitilmesi için öneriler sundu.

Ne oldu?

Torvik Industries yönetimi önemli noktalarda kontrolü elinde tutmaya alışkındı. Bu nedenle bilgisayar korsanlarının ağlarına ciddi bir şekilde sızıp şirketin gezer vinçlerini kapatabilmesi ve açık denizdeki gemilerin yönünü değiştirebilmesi onlar için beklenmedik bir durumdu.

The Wolf'un tek yapması gereken, bir şantiyedeki geniş format yazıcının güvenlik açığından yararlanmaktı. Ardından The Wolf, şirket ağına doğru ilerleyerek operasyon açısından önemli hedeflere sızabildi. Bu öncü nakliye şirketi bir anda büyük operasyonel kesintiler, uluslararası ölçekte ciddi denetimler ve binlerce öfkeli müşteriyle karşı karşıya kaldı.

Nasıl oldu?

Şirketin BT güvenlik ekibi, koruma altında olduklarını düşünüyordu. Teknik ve lojistik ekipler, olası güvenlik sorunları için küresel faaliyetleri durmadan izliyordu. Hatta yazıcı gibi uç noktalar için uygulanan güvenlik prosedürleri de mevcuttu. Ancak bir şey gözlerinden kaçmıştı: geçici olarak bir şantiyedeki römorka yerleştirilen geniş format yazıcının güvenlik yapılandırması.

Bilgisayar korsanının yazıcıya doğrudan ulaşmasına bile gerek yoktu. Geniş format belgeleri basmakla sorumlu Torvik çalışanına, PDF eki içeren bir e-posta göndermesi yeterliydi. PDF'te saldırı amaçlı gizli bir Postscript dosyası bulunuyordu. Bu dosya, PDF yazıcıya gönderildiğinde kendi kendini açıp çalıştırabiliyordu. Çalışanın belgeyi baskıya göndermesinin ardından kötü amaçlı yazılım, kendini yazıcıya yerleştirip daha sonra tüm ağa yayılmaya başladı. Zararsız gibi görünen bir e-posta ekine kötü amaçlı yazılım yerleştiren bilgisayar korsanı, şirket bilgisayarlarındaki kötü amaçlı yazılımdan koruma programını atlattı.

Geniş format yazıcıda tehdit algılama gibi güçlü yerleşik güvenlik özelliklerinin bulunmaması da ihlali mümkün kıldı. Şirket, portföydeki her bir yazıcının (uydu şubelere geçici olarak yerleştirilenler gibi) yapılandırmasını izleyip yönetmeyi de başaramamıştı.

İhlalin verdiği hasarın onarılması

Torvik Industries, kuruluş siber güvenliğinin kapsamlı analizi için öncü bir sızma testi firmasıyla anlaştı.

Penetrasyon testi ekibi, yerleşik güvenlik özelliklerine sahip HP yazıcıların kurulmasını önerdi. Bunlar arasında Güvenli Önyükleme ve ürün yazılımını beyaz listeye alma özellikli HP DesignJet serisi yazıcılar bulunuyordu. Bu özellikler sayesinde yazıcılar, kötü amaçlı kodları algılayıp kapanır ve ardından gerçek HP ürün yazılımının yeniden yüklenmesi için BT ekibini uyarır.

Penetrasyon testi ekibi, portföy genelinde güvenlik yönetimi yazılımı olan HP JetAdvantage Security Manager'ın Anında Açılan Güvenlik özelliğini kullanmalarını da önerdi. Bu özellik sayesinde, cihazlar ağa eklenir eklenmez güvenlik politikaları otomatik olarak uygulanır. HP Security Manager, uzak veya geçici konumlarda bulunanlar da dahil her HP yazıcısını kapsayan uyumluluk raporları da hazırlayabilir. Bu sayede portföyde güvenlik yapılandırmalarının korunduğu anlaşılabilir.

Güvenlik danışmanı, çalışanların şüpheli e-postaları tanıması ve bilinmeyen ekleri basmaktan kaçınması için bir eğitim programı hazırlanmasını da önerdi.

Sonuç

Torvik Industries'in faaliyetleri siber güvenlik ihlalinin sonuçlarından hâlâ etkileniyor. Şirket, başkanın alışılmadık görüşleri ve işlediği suçlar nedeniyle basında da geniş yer buluyor. Kuruluş, yönetimi yeniden şekillendirmenin yollarını ararken, siber güvenlik konusunda izlenecek yol açık: ava çıkan sıradaki kurtun saldırılarını önlemeye yardımcı olacak HP yazıcılarını ve HP çözümlerini tercih etmek.

**Torvik Industries, HP Studio'nun "THE WOLF: TRUE ALPHA" adlı filmindeki büyük siber saldırıda hedeflenen kurgusal bir şirkettir.*

HP çözümleri hakkında daha fazla bilgi için:
HP DesignJet: hp.com/go/designjetsecurity
Baskı güvenliği: hp.com/go/reinventsecurity

"The Wolf" filmlerini izlemek için şu adresi ziyaret edin:
hp.com/thewolf

Güncelleştirmeler için kaydolun
hp.com/go/getupdated

İş arkadaşlarınızla paylaşın

© Copyright 2018 HP Development Company, L.P. Bu belgede yer alan bilgiler önceden haber verilmeden değiştirilebilir. HP ürün ve hizmetlerine ilişkin yegane garantiler, bu ürün ve hizmetlerle birlikte verilen açık garanti bildirimlerinde belirtilmiştir. Buradaki hiçbir ifade ek garanti verilmesi olarak yorumlanmamalıdır. HP, bu belgedeki teknik hatalardan veya yazım hatalarından ya da eksikliklerden sorumlu tutulamaz.

4AA7-3562TRE, Ağustos 2018