Vaka analizi

Londra Havaalanı yıkıcı bir siber saldırının hedefi olduğunda, HP yazıcılar tehdidi algıladı

Veri ihlaline dair resmi özet raporu

Sektör
Havacılık

Amaç
Siber güvenlik uygulamalarındaki zayıf halkaları tespit etmek ve bunları güçlendirmeye odaklanmak

Yaklaşım
HP güvenlik uzmanlarının iş birliğiyle kapsamlı bir güvenlik planı geliştirildi

BT farkı
- IoT uç noktalarında güvenlik önlemleri alındı
- HP yazıcılarda yerleşik güvenlik özellikleri etkinleştirildi
- Ağ genelinde güvenlik izleme uygulamaları iyileştirildi

İş farkı
Kritik uluslararası altyapıyı korumak ve yolcu güvenliğini sağlamak için geliştirilmiş siber güvenlik uygulamaları iyileştirildi

Genel bakış

Londra Havaalanı*, her gün dünya genelinde 94 ülkeye seyahat eden 300.000'den fazla yolcuya hizmet veriyor. Havaalanında 300 şirketten yaklaşık 50.000 kişi çalışıyor. Bu nedenle havaalanı kalabalık bir şehri andırıyor.

Havaalanı büyüdükçe altyapısı da daha bağlantılı ve otomatik bir hâle geldi. HVAC sisteminden aydınlatma ve yazıcılara kadar tüm dahili sistem, artık havaalanı ağında yer alıyor. Baskı, tarama ve fotokopi işlemleri, havaalanı geneline yayılan ve 60'tan fazla çok fonksiyonlu HP yazıcı tarafından gerçekleştiriliyor.

23 Nisan 2018'de "The Wolf" adıyla bilinen siber terörist, ağa erişmek ve kötü amaçlı yazılımını yaymak için havaalanının bağlantılı aydınlatma sistemlerini kullandı. The Wolf, yeterli düzeyde korunmayan uç noktaları kötüye kullanmasıyla tanınıyor. Bu nedenle BT güvenlik uzmanları, kötü amaçlı yazılımın yayılmasını önlemek ve saldırıyı durdurmak için soruşturmanın bir parçası olarak HP Enterprise yazıcılara gelen tehdit verilerini inceledi. Şaşırtıcı bir şekilde veriler,, müdahalenin kaynağı konusunda The Wolf'tan ipuçları içeriyordu. Bu olaydan sonra Londra Havaalanı, uç nokta güvenliğini daha da artırmak için HP'yi tercih etti.

Ne oldu?

Büyük olasılıkla ağdaki kullanıcılara kimlik avı e-postası göndererek güvenlik açığı bulan The Wolf, kötü amaçlı yazılımla IoT aydınlatma sistemine sızabildi. Sonrasında kötü amaçlı yazılımını ağ geneline yayıp izlenmeyen diğer uç nokta cihazlarında kendine zemin hazırladı.

İzlenmeyen IoT cihazlarında varlığını

gizleyen The Wolf'un ekibi, büyük çaplı ve yıkıcı bir saldırı için çok sayıda başlangıç noktası geliştirirken ağ izleme sistemlerinin dikkatinden kaçabilirdi.

Havaalanı yönetimi, uçak ve yolcuların taşınması gibi kritik altyapı faaliyetlerini sürdürürken umutsuz bir şekilde çok sayıda sistemi kapatmaya çalışıyordu.

Saldırıya verilen karşılık

The Wolf, havaalanı ağına saldırmakla görevlendirilmişti. Havaalanının BT güvenlik ekibi, havaalanı ağının bilgisayar korsanlarına karşı iyi korunduğunu *düşünüyordu*. Ancak IoT cihazlarında gizli tehlikelerin farkında değillerdi.

Neyse ki havaalanında kullanılan HP

Enterprise yazıcılarda Bağlantı Denetçisi özelliği bulunuyordu. Bu özellik, bilgisayar korsanlarının kumanda ve denetim sunucularına doğru şüpheli "geri arama" denemelerinde bulunulduğunda, kötü amaçlı yazılımı durdurdu.

Aksiyonlar, yazıcıların sistem verilerinde yakalandı. Bir şeylerin yolunda gitmediğini fark eden BT ekibi, saldırı hakkında ayrıntılara ulaşmak için verilerini günlüklerini kontrol etti. Ancak kötü amaçlı yazılım ağa yayıldığından, vakit kaybetmemek gerekiyordu. BT güvenlik ekibi, yazıcının tehdit algılama sistem günlüklerini kendi güvenlik bilgileri ve olay izleme (SIEM) sistemlerine bağlamış olsaydı müdahale anında uyarı alabilirdi.

Her zamankinden daha sıkı güvenlik

İhlalin ardından BT ekibi, yönetilen baskı hizmeti sağlayıcıları ve HP Güvenlik Danışmanlarıyla birlikte güvenlik uygulamalarını gözden geçirdi.

Londra Havaalanı, HP Enterprise yazıcıları kurarak zaten doğru bir adım atmıştı. Yalnızca HP Enterprise yazıcılar ve çok fonksiyonlu yazıcılar, çalışma sırasında kötü amaçlı yazılımları algılayıp durdurmak ve sistemi yeniden başlamaya zorlamak için çalışma sırasında müdahale algılama ve HP Bağlantı Denetçisi özelliklerini sunar. Açılışta HP Sure Start, BIOS'u kontrol eder ve kodda açık varsa kendi kendine onarım gerçekleştirebilir. Aynı zamanda beyaz listeye alma özelliğiyle ürün yazılımı denetlenir.

Yönetilen baskı hizmeti sağlayıcısı, yazıcının yeniden başlatıldığı ve değiştirilen ayarların sıfırlandığı zamanlarda güvenlik ayarlarının otomatik olarak kontrol edilmesi için HP JetAdvantage Security Manager yazılımını dağıttı.

Havaalanının BT güvenlik ekibi de yazıcının sistem verilerini SIEM araçlarına bağladı. Diğer üreticilere ait yazıcıların aksine HP cihazları, birçok SIEM aracına tehdide özel veriler sağlayabilir. Bu sayede BT ekibi, olası güvenlik olaylarında gerçek zamanlı uyarılar alabilir. Bu sayede HP yazıcılar, ağı denetleyen son derece değerli cihazlara dönüşür.

Sonuç

Havaalanının HP Enterprise yazıcıları ve The Wolf'un geride bıraktığı ipuçları sayesinde güvenlik ekibi, saldırının yayılmasını yeterince kısa sürede engellemeyi başardı. Bunun sonucunda faaliyetlerin kesintiye uğramasının, basında olumsuz yer edinilmesinin, uygunsuzluktandoğan para cezalarının ve markanın göreceği zararın önüne geçildi.

Daha güçlü güvenlik uygulamalarını hayata geçirip HP yazıcıların yerleşik güvenlik özelliklerinden tam olarak yararlanan havaalanı, ağ genelinde güvenliği sıkılaştırdı.

**Londra Havaalanı, HP Studio'nun "THE WOLF: TRUE ALPHA" adlı filmindeki büyük siber saldırıda hedeflenen kurgusal bir kurumdur.*

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

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

Güncelleştirmeler için kaydolun
hp.com/go/getupdated

İş arkadaşlarınızla paylaşın

4AA7-3560TRE, Ağustos 2018