Vaka analizi

İsviçre Konferans Merkezi'ne yapılan AV saldırısı, HP bilgisayarların güvenlik özellikleriyle durdurulabilirdi

Veri ihlaline dair resmi özet raporu

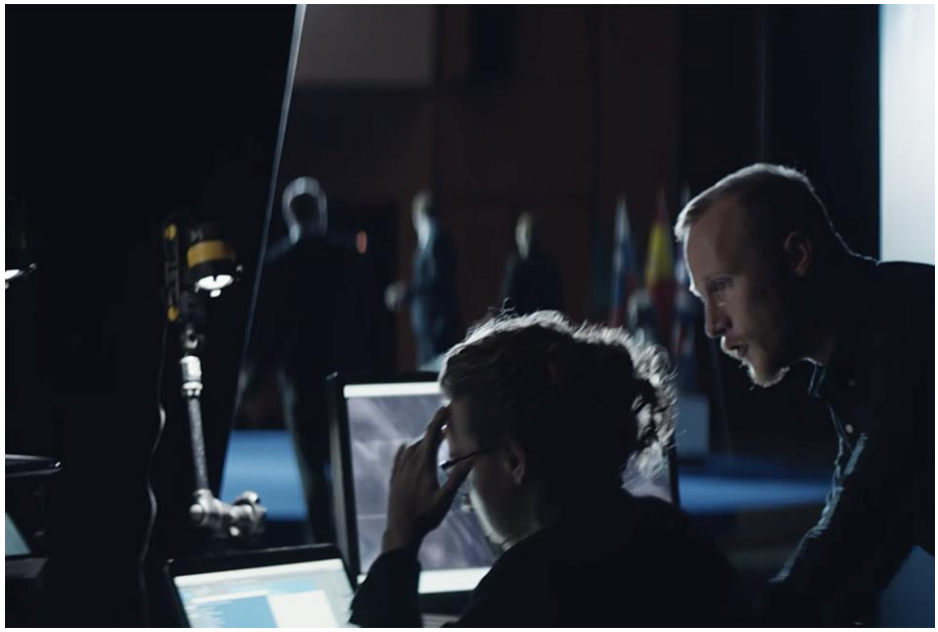
Sektör
Etkinlik merkezi

Amaç
Konferans merkezini ve hassas müşteri verilerini daha iyi korumak için güvenlik uygulamalarını denetlemek

Yaklaşım
Güvenlik uygulamalarını analiz etmek ve dikkat edilmesi gereken noktaları belirlemek için güvenlik danışmanıyla iş birliği yapıldı

BT farkı
- Portföy, kötü amaçlı yazılımlara karşı yerleşik koruma özelliklerine sahip HP Elite bilgisayarlarla geliştirildi
- Yetkisiz kullanımı önlemek için gereksiz bağlantı noktaları kapatıldı
- Bilgisayar portföyünün uzaktan yönetimi için HP Manageability Integration Kit eklentisi, Microsoft System Center Configuration Manager (SCCM) ile tümleştirildi

İş farkı
Tesisi ileri düzey saldırılara karşı daha iyi koruyup müşterilerin güvenini yeniden kazanmak için siber güvenlik önlemleri güncelleştirildi



Genel bakış

Cenevre yakınındaki İsviçre Konferans Merkezi*, her yıl 230'dan fazla etkinliğe ev sahipliği yapıyor. İş dünyasındaki konferanslar ve büyük ürün lansmanları için Avrupa'da tercih edilen nokta olan bu merkez, tüm dünyadan sektör liderlerine hizmet veriyor.

Merkezin yönetimi, müşterilere özenle seçilmiş bir ortamda istedikleri gibi özelleştirebilecekleri konferans deneyimi sunmak için teknoloji altyapısına büyük yatırımlar yaptı. Maalesef ilgili güvenlik iyileştirmeleri, bilgisayar portföyünü kapsamıyordu.

23 Nisan 2018'de kendisine "The Wolf" adını veren bir bilgisayar korsanı, çeşitli ülkelerden gelen izleyicilere yapılan üst düzey bir sunumu kesintiye uğratmak için konferans merkezindeki bir bilgisayara sızdı. İhlalin ardından İsviçre Konferans Merkezi, siber güvenlik açıklarını bulup onarmak için güvenlik danışmanlarına başvurdu.

Ne oldu?

Dünyanın başlıca kurumsal etkinlik mekanlarından olan İsviçre Konferans Merkezi, konuklar için muhteşem deneyimler sunma konusunda uzman. Ancak siber güvenlikte aynı başarı sergilenemedi. The Wolf, merkezdeki bilgisayarlardan birine kötü amaçlı yazılım yükleyip konuşmacının sunumunu kendi sunumuyla değiştirdi. Tesisin BT güvenlik ekibi, konferans salonunda yaşanan kaosun ortasında ağın kontrolünü geri kazanmak için mücadele verdi.

Ortaya çıkan zarar, tek bir sunumun mahvolmasıyla sınırlı kalmadı. İptal edilen rezervasyonlar nedeniyle yaşanan gelir kaybı şu anda tahmini olarak 3,2 milyon euro.

Nasıl oldu?

The Wolf'un tek yapması gereken, bir çalışanın e-postadaki zararlı bir bağlantıya tıklamasını veya masum görünen bir eki indirmesini sağlayıp korumasız bir bilgisayara sızmaktı. Bunun dışında, fiziksel olarak bilgisayara yakın olduğunda gözetimsiz bir USB bağlantı noktasına bir flash sürücü takabilirdi.

İsviçre Konferans Merkezi'nin bilgisayar portföyünde, kötü amaçlı yazılımı karantinaya alıp bu sızma girişimini engelleyecek temel koruma mekanizmaları yoktu. Anti virüs yazılımı yüklemiş *olsalar da*, bilgisayarların hiçbirinde donanım zorlamalı yerleşik güvenlik özellikleri bulunmuyordu.

Güvenliğin güçlendirilmesi

İsviçre Konferans Merkezi, güvenlik danışmanlarıyla birlikte mevcut siber güvenlik önlemlerinin kapsamlı bir denetimini gerçekleştirdi. Bu inceleme sonucunda tüm filo, kötü amaçlı yazılımlara karşı yerleşik korumaya sahip HP Elite bilgisayarlara yükseltildi. Bilgisayarlardaki koruma özellikleri arasında, açılış ve çalışma sırasında bozulmaları ya da BIOS saldırılarını otomatik olarak algılayıp durdurabilen ve onarabilen HP Sure Start Gen4 de bulunuyor.[1]

Yeni HP Elite bilgisayarlarda HP Sure Click, özelliği de bulunuyor. Her tarayıcı sekmesini veya indirilmiş PDF ya da Office belgesini bir mikro sanal makine (VM) içine alarak fiziksel olarak ayıran, böylece web tabanlı kötü amaçlı yazılımların veya e-posta eklerinin ağdaki bağlı diğer cihazlara yayılmasını önleyen HP Sure Click, daha gelişmiş koruma sağlamaktadır.[2]

BT ekibi artık bağlantı noktalarını ve çıkarılabilir ortam cihazlarını yönetmek için HP Device Access Manager'dan yararlanıyor. Aynı zamanda, filo genelinde güvenlik uygulamalarını ve BIOS yönetimini kolaylaştırmak amacıyla SCCM için HP Manageability Integration Kit kullanılıyor.[3]

Sonuç

Bu olay, İsviçre Konferans Merkezi'nin gelir kayıpları yaşamasına ve üst düzey müşterilerin markaya duyduğu güvenin zedelenmesine neden oldu. Ancak kapsamlı güvenlik önlemleri ve etkili yönetim çözümleriyle HP bilgisayarların dağıtımını gerçekleştiren merkez, artık siber güvenliği daha fazla ciddiye aldığını gösteriyor.

**İsviçre Konferans Merkezi, HP Studio'nun "THE WOLF: TRUE ALPHA" adlı filmindeki büyük siber saldırıda hedeflenen kurgusal bir işletmedir.*

HP çözümleri hakkında daha fazla bilgi için:

Bilgisayar güvenliği:
hp.com/go/computersecurity
Baskı güvenliği: hp.com/go/reinventsecurity

"The Wolf" filmlerini izlemek için şu adresi ziyaret edin:

hp.com/thewolf

[1] HP Sure Start Gen4, 8. nesil Intel® veya AMD işlemcilerle donatılmış HP Elite ve HP Pro 600 ürünlerinde sunulmaktadır.
[2] HP Sure Click, çoğu HP bilgisayarda sunulur ve Internet Explorer ile Chromium™ tarayıcıları destekler. Office veya Adobe Acrobat yüklü olduğunda, desteklenen ekler salt okunur moddaki Office (Word, Excel, PowerPoint) ve PDF dosyalarını içerir.
[3] HP Manageability Integration Kit önceden yüklenmemiştir. Eklentiye hp.com/go/clientmanagement adresinden ulaşabilirsiniz.

Güncelleştirmeler için kaydolun
hp.com/go/getupdated