CASE STUDY

Creating a Virtual Fort Knox

Although banks have taken cybersecurity seriously for years, their task keeps getting harder. As financial institutions increasingly embrace mobile apps and other digital tools, cyber thieves suddenly have a plethora of new targets. Ensuring resiliency and preventing an online heist can suddenly seem like plugging a leaky dike: In-house employees simply don't have enough fingers.

Trustwave®

Client Spotlight

With nearly $10 billion in assets and 800 employees, this Icelandic bank traces its roots back to 1930 and ranks as one of the country's largest financial institutions. After rising from the ashes of Iceland's 2009 financial collapse, the bank today serves more than 100,000 customers across 24 branches.

The Challenge

Like many financial institutions, this Trustwave customer regularly conducts penetration tests in order to determine its ability to withstand attacks and augment its small in-house security team. After turning to other firms in past years, the bank's security team needed a new expert who could bring fresh eyes and deeper knowledge to assess ever-proliferating threats.

"With Trustwave, there's a certain quality to the work and the communication that we don't always see with security partners. You don't get the feeling you're being sold something; you get the feeling you're collaborating to keep the bank safe."

– Chief Information Security Officer, major Icelandic bank

Industry Threat

Financial institutions, long the top target of cybercriminals, have been hit hard by the recent explosion in mobile banking. Banks and other entities saw their cybercrime costs skyrocket 40 percent between 2014 and 2017, to a shocking $18.3 million per firm, according to Accenture[1]—and that number continues to increase annually. Moreover, banks suffered twice the number of cyber attacks in 2017 as they did the year before, as cloud-based services, microservices, apps, edge computing and blockchain create new opportunities for criminals.

The Solution

The bank's security officer reached out to Trustwave SpiderLabs, an elite security team, to perform what's known as a red team assessment: A comprehensive, multi-layered attack simulation that tries to gain access to sensitive data in any way imaginable. While a typical penetration test might take a week or two, a red team engagement can take up to twice as long. That's because experts aren't just furtively testing for an organization's biggest network weaknesses. Instead, they're using extensive reconnaissance to find even obscure vulnerabilities and then simultaneously attacking each chink in the armor before leaving undetected.

In this red team event, Trustwave's ethical hackers first scanned the dark web and bought sensitive bank data that its leaders were unaware was for sale among criminals. Then, using the information gathered, the team executed a high-level attack on the institution's networks. Finally, Trustwave experts undertook an in-person attack that, while seemingly "low-tech," pointed out potentially devasting consequences of lax office security. After gaining physical access to the bank's headquarters and one of its branches by covertly following employees who swiped IDs, Trustwave's experts then infiltrated the office, taking sensitive information that was lying out in the open and adding spyware to unattended laptops.

"The big concern is not knowing what you don't know, and it's very hard to find in-house people with the necessary expertise. These exercises are always very eye-opening. Trustwave helps us find evolving vulnerabilities and helps us increase awareness among employees about possible threats."

– Chief Information Security Officer, major Icelandic bank

Trustwave®