Addressing Insider Threats, Cyber Attacks & Data Security

From iPhone to Drone, The Threat of Connected Devices in Your Branches

A new security consciousness has arisen for today's bank of a classic security threat. It has been a challenge for years to find, fingerprint, and analyze the wireless and wired devices connecting to the networks of both headquarters and branch offices. These devices come in all shapes and sizes, from phone to drone, and can be in the hands of malicious criminals or an unbeknownst gateway into your data via an employee or customer. Today's bank can be easily attacked via a rogue wireless/wired device connected to or unknowingly plugged into your network(s), an employee's misconfigured iPhone, an attached HP printer that was never inventoried, a high-flying wifi-enabled drone above your branch, or a high-end scanning device that is connected via non-SSL ports.

Traditional security solutions focus on building walls and filtering threats, but it has become obvious that is not enough; teams need proper visibility into all of these wireless/wired devices and how they change and behave over time.

As banks begin to deploy wireless/wired device threat detection it has become important to consider four key factors for file and data security:

Real-time Device Detection

Banks are in a unique situation; their distributed footprint opens them up to more threats, and real-time detection of all of the wired/wireless devices is critical. One recent development from cyber criminals has been to target Banks and small banks using devices like Raspberry Pis, connected for very short period of time to avoid detection by traditional scans and monitoring for siphoned data over time.

You can't protect from what you can't see, we all know that and plenty of vendors talk about it, A LOT. But it's true. Until you can actually see the devices, whether wired or wireless, cellular or Bluetooth, whether on or near your network, how can you possibly start to make decisions about your overall security?

Device Identification and Inventory

Let's face it: at your bank, many of the devices you see are trusted (at least for now). Therefore, the initial step is taking inventory of all the connected devices in your environment and fingerprinting them so you'll have a historical logging for future incident response if things change. You probably won't be shocked when you, like other banks, find an old Windows box connected to the network and running an unpatched legacy application in your environment.

Device Threat Alerts and Compliance Enforcement

Another recent threat seen at banks has been non-SSL ports open on high-end scanning devices, often used by your teams to scan privileged documents. Comprehensive visibility and real-time reporting about device behavior gives security teams the granular device intelligence needed to prioritize response for this type of vulnerability and enforce policy.

The time is now for banks to gain visibility into the wireless/wired device threat landscape and see all the things.

Paul Paget
CEO

Contact Info
www.pwnieexpress.com
(855) 793-1337

Paul Paget brings more than 30 years of leadership experience in the technology and information security markets to his roles as CEO of Pwnie Express and Executive Chairman of Savant Protection. Previously, he was CEO at Savant Protection, an innovator in infrastructure protection and industrial control systems and was sold to Digital Guardian, and served as CEO of Core Security Technologies, where he led the company's transformation into an automated penetration testing leader with more than 600 customers in 40 countries. He also held key executive positions at Baltimore Technologies, where he grew the Americas company 5x to a $30+ million dollar business, a board member of Nitro Security, which then sold to Intel/McAfee, and as VP of Sales and Marketing at CyberTrust. Paul's early career included management positions with Lotus Development and IBM. He is a graduate of Bowdoin College.