Q-Net Security Raises the Bar

on

Best Practices in Network Cybersecurity for the Financial Services Industry

Cyberattacks in the Financial Services industry are exploding

Pundits and reporters, from Accenture to ZDNet, all agree that those working in the Financial Industry can expect significant increases in cyberattacks this year. The criminals are getting better at being able to compromise existing systems while also increasing their ability to profit from these attacks. These attacks burden an already stressed system lacking sufficiently trained personnel to make timely changes to fundamentally insecure systems. Often these systems are on aging infrastructure which have an exploding number of insecure devices being connected and attacks include malware or its sibling, ransomware. Existing networks frequently have some malware in them, while new infections will enter through deficient defenses unable to adequately protect the exploding number of new connected devices. Overwhelmed networks and endpoints may react improperly to malicious activities such as distributed denial of service (DDoS); comprised processors and their kernels; outdated operating systems, and software. In addition to the network deficiencies, social engineering tactics are often employed to steal the very information used to protect these systems as they often rely on user managed security keys.

Almost daily news headlines highlight growing fraud

One need only look to this week's news headlines to understand how ubiquitous these attacks have become. Data breaches include Capital One, Sephora, and Pearson. A Man-in-the-Middle relay has attacked POS devices and caused kiosks and ATMs to spill their contents. Other headlines note "Russian Hackers are Infiltrating Companies via the Office Printer" and "New Intel Flaw Exposes Secrets on Windows Machines". According to Europol, in 2018 there was over $1 billion in losses attributed to the criminal gang "Lazarus" alone, and ATM fraud in the wild is costing billions of dollars each year!

Software solutions are insecure and need constant support

The ongoing fight to keep criminal activities in check requires a plethora of updates, patches, and additional monitoring solutions along with an army of highly trained professionals to watch and secure the infrastructure. But we are still losing many battles. While some of these attacks require physical access to the systems, most can be done through compromised networks. As such, typical cybersecurity solutions focus on securing the sub-network. Solutions are a multi-layered set of products that often begin with firewalls to keep bad actors out and good data in. Moving data outside of the firewall frequently employs VPNs for security while moving data within the designated sub-network is often done in the clear. Moving data between endpoint and a web browser will often employ TLS. For the times when endpoints become compromised or network security is thwarted, other solutions (SIEMs) look to monitor security events. Such systems need to be set up, monitored, updated, patched, malware signatures discovered, and keys managed. As an example of the effort required of cybersecurity staff, a Ponemon survey notes that almost 70% of the respondents rate key-management as "very painful". While the goal is network intrusion ***prevention***, the preponderance of network cybersecurity solutions provide

Solutions mainly focus on intrusion detection while prevention is needed

only network intrusion ***detection*** leaving it to the trained professionals and their advanced cybersecurity tools to try to re-secure the network and clean up the mess.

While these software solutions may be readily configurable, their management is cumbersome, often leading to misconfiguration that creates opportunities for mischief and criminal behavior. And without exception, all software solutions are not provably secure; in fact, history has demonstrated, as evidenced by the headlines contained here and reported in just the past several weeks, that such solutions continue to experience compromises and malicious attacks. Documented cases include a Cisco iOS issue that lays bare virtually every router and switch in the networking fabric; hardware issues like Spectre, Meltdown, and ZombieLoad may expose precious data, including usernames and passwords, to a crooks and scoundrels; software problems, including those affecting webservers and database managers, can be used to access sensitive data through SQL injection; and ubiquitous browsers have been shown to have security flaws, even when ostensibly secure data transfer using SSL/TLS (HTTPS) is employed.

Cybercrime exceeds $1.5 trillion in profits

The numbers are frightening. The FBI reports that thousands of ransomware attacks occur daily and more than 200,000 new malware signatures are seen each day. Billions of data records have been stolen averaging almost ten million per day. Reviewing DDoS attacks, 75% result from compromised routers with IP cameras adding another 15%. Research shows that half of all websites and 95% HTTPS servers are vulnerable while TLS compromises (Heartbleed and POODLE) increase that fraction to almost 100%! About one-third of the exploits use a Man-in-the-Middle. For data loss, over 90% start with phishing or spearphishing and 85% of the phishing attacks target the US. The number of ransomware attacks in the US is skyrocketing. To round out some of these troubling figures, there are now over 20 ATM and POS attack modalities in the wild with many beginning as a download in a compromised network. If we continue to rely on software solutions, we will continue losing battles and possibly end up losing the war.

QNS solutions are provably secure and provide quantum compute-resistant micro-segmentation

Q-Net Security (QNS) solutions are provably secure with a hardware-only (no software) approach to protect critical infrastructure and the networks that are essential to their operation. QNS delivers the strongest commercially available endpoint security solution and prioritizes network intrusion prevention making intrusion detection secondary if not superfluous. These products are engineered from immutable, purpose-built hardware, do not use any operating systems or vulnerable software, and can't be changed by malware or respond to it in any way. The QNS drop-in secure network overlay has attributes characterized as a distributed firewall together with sessionless VPN tunnels providing fine-grained network micro-segmentation. The QNS keys are generated using an industry-leading True Random Number Generator that can produce new keys as frequently as a million times per second.

The strongest network cybersecurity yet never needs patches

Should a Q-Net endpoint (ATM, server, IP camera, …) be compromised with malware (zero-day as manufactured, through a compromised network, or physically installed such as with a USB attached device), the attack surface will be limited, reducing the spread of infection. Since the network cannot be compromised, many redundant parts can be eliminated. In fact, based on the details made public, many of the headlines that we referenced above could have been prevented with a QNS implementation. This includes the two largest data breaches, Equifax and Capital One, each exceeding 100 million private customer records. While it was known how to ameliorate these issues with appropriate patches, the patches were not installed because of the inability to remain current with a system-wide patching routine. QNS devices never need to be updated or patched once deployed greatly reducing risk as well as operating costs. And with the strong microsegmentation provided by QNS solutions, gaining a username and password through phishing or other means is rendered virtually impossible. QNS delivers remarkably strong security and yet is easy to implement with unified endpoint management and no requirement for external key management. The QNS team has been careful to ensure that QNS devices can be placed in the field for years, if not decades, without needing any maintenance, even in a post-quantum world.

QNS devices are currently protecting regions of the national electrical grid, securing financial networks, including ATM networks, and providing factory-floor protection of Industrial Control Systems. These products are NIST FIPS 140-2 Level 2 certified and have all appropriate electrical certification.

Show me: A QNS POC can be set up in hours

A QNS POC asks for a *de minimis* time commitment from any Bank's Cybersecurity team. Implementation of QNS solutions are quite straightforward – drop-in with simple and centralized management that doesn't require individual devices to be configured. No advanced training is required, no changes are needed to the endpoints or the network, no regression testing is needed in heterogeneous environments, and no additional IP addresses are required to instantiate strong, secure networks. Consider new cybersecurity regulations for the financial industry (such as the NYDFS Cybersecurity Regulation). For publicly traded Financial Services companies, the CISO is required to attend each public board meeting. QNS has raised the bar for network cybersecurity and no longer can a CISO describe little action as the industry normal. There is no downside or internal political risk for giving Q-Net Security a try but the opposite … inaction may be dealt with severely and result in catastrophic consequences.

QNS is committed to protecting our customers and does not want them to become the next headline for having become a victim of a cyberattack. Schedule a Q-Net Overview Meeting or Conference Call by contacting Dr. Ronald Indeck at

rindeck@qnetsecurity.com or (314) 495-3539