LeNic Tech Talk

...where banking and technology connect!

June 2017

Don't be held hostage. Learn how the banking industry can defend against Ransomware

by Tom DeSot, EVP & CIO, Digital Defense

Ransomware attacks have been rising to fame this year through high-profile incidents at financial institutions, hospitals, law firms, retail organizations and even governments offices. The U,S, Federal Financial Institutions Examination Council stated early in 2016 that it is also seeing a concerning increase in the number and severity of these types of attacks on financial institutions and banks, involving extortion and cyber fraud.

Cyber fraud is the use of Internet services or software with internet access to deceive and defraud victims, both individuals as well as organizations, and with a motivation of financial gain. One example of cyber fraud is ransomware. Ransomware is a type of malicious software that restricts access to infected computer systems until the user pays a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files and display messages intended to coax the user into paying. Ransoms can range from $300-$50,000. In some cases, the criminal will threaten to destroy all data if the victim fails to meet demands or if the owner attempts to remove the malware without paying.

"Defenders must be diligent, continually updating systems training and retraining staff in order to attempt to stay ahead of attackers; no easy task"

While financial institutions are typically known for being on the forefront of information security due to compliance and regulations placed on them, they are certainly not immune to all types of cyberattacks. Most financial institutions strive to make sure that technologies are in place to quickly identify vulnerabilities and mitigate risks of a data breach. However, regulators and most security... [*Click **here** for full article.*]

Also in this issue

This Month's White Paper

Summaries Overleaf

Industry News

www.lenicgroup.com

How banks can cut security risks posed by email hoaxes

by Penny Crosman,
Editor at Large at American Banker

The recent news that two high-ranking banking executives were tricked into having inappropriate email conversations with a prankster who then posted them on Twitter was amusing — and surely embarrassing for the executives. It was also a lesson for anyone who is casual about using email and for any IT or security department that is not doing its utmost to ward off mischief and worse.

For those who may have missed it, Jes Staley, CEO of Barclays, fell for an email that looked like it came from Chairman John McFarlane. (The email address was... [*Click **here** for full article.*]

Data integrity breaches – the challenge facing banks

by Kevin Murphy,
President of ISACA's Scotland chapter

What type of organisation is likely to be targeted by data integrity breaches and how best can they detect and mitigate such attacks?

In the world of cyber security, we can argue that threat actors will largely stay the same: the insider, the criminal, the hacktivist and the hostile state. What is changing, however, is the methodology of that attack vector; specifically, the shift of focus from a customer to an organisation's data.

We know from Lloyd's of London that the cost of the financial world mitigating against cyber breaches is as much as $400bn a year, a figure that includes both preventative and remediation activities... [*Click **here** for full article.*]

Business White Paper

Hewlett Packard Enterprise

State of Security Operations

2017 report of capabilities and maturity of cyber defense organizations

Executive Summary

Organizations around the globe are investing heavily in cyber defense capabilities to protect their critical assets. Whether protecting brand, intellectual capital, and customer information or providing controls for critical infrastructure, the means for incident detection and response to protect organizational interests have common elements: people, processes, and technology.

The maturity of these elements varies greatly across organizations and industries, In this fourth annual State of Security Operations report, Hewlett Packard Enterprises provides updates to the current and emerging capabilities, best practices, and performance levels of security operations as learned from the assessment of organizations around the globe.

With over a decade of experience supplying the security... [*Click **here** for full white paper.*]

Digital Check Introduces SmartSource Adaptive 2.0 Multi-Function Scanner

Updated Device Brings Higher Speed to Mixed-Batch Check and Document Scanning

Digital Check Corp.'s new SmartSource Adaptive 2.0 scanner is now available for general purchase, delivering a significant performance boost for financial institutions and other businesses that need to scan checks and... [*Click **here** to learn more.*]

Google's Android Pay gets a hand from banks and PayPal

Banking Tech ... 18 April, 2017

Google is banking on mobile apps to boost its mobile wallet. The Android Pay parent has linked that service to a handful of banking apps, giving consumers the ability to add their cards more quickly to the mobile wallet.

Customers of Bank of America. Bank of New Zealand, Discover... [*Click **here** to learn more.*]