CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

Today's cyber-criminals are capable, opportunistic, and persistent, and data has become it's own currency in the underground, online communities where these criminals congregate.

Recently, we've seen evidence that low-level hackers may be gaining access using tried and true methods, such as phishing, social engineering, and leveraging easily exploitable vulnerabilities. Then, they provide this information to more advanced cyber-crime syndicates.

Security products, such as IDS/IPS, Next-Gen firewalls, and host-based endpoint protection systems, are still effective at preventing known threats using signatures, heuristics and behavioral analysis. However, more advanced threats, like polymorphic, in-memory malware, persistent root-kits, & Remote Access Trojans (RAT) deployed through the use of "crypters" and "packers"[1] can be next to impossible to detect and remediate.

Managed Security Services Providers (MSSP) can help by providing 24x7, real-time monitoring, but to keep costs down, MSSPs must hire entry-level analysts with little real-world experience. Furthermore, the trouble-tickets MSSPs generate must be investigated. Rules, whitelists, and blacklists must to be meticulously maintained to reduce false-positives and tune sensors. Unfortunately, in-house security teams face the same challenges.

Credit Union Security Managers must be able to predict all potential attack vectors and establish controls to reduce or eliminate exposure and provide for continued assurance that those controls remain effective. Today's threats are elastic and adaptive. Credit Unions must become elastic and adaptive as well.

The foundation of any effective information security strategy is a well-crafted policy. Policy must drive security, and security must drive compliance! Compliance is critical, but a narrow focus on compliance alone can provide a false sense of security. There remains a vast divide between compliance and security. *Compliance* should start with *security*; not the other way around.

Credit Unions must begin by assessing not only existing controls and protection methods. Your incident response team's ability to *identify* threats must be assessed as well. More than a Penetration Test, an assessment of your *threat identification capability* should be able evaluate and validate your controls using black-hat techniques and methodologies.

Next, Credit unions should consider segmenting existing flat networks into separate enclaves with limited *east-west* access. Some systems may even need to be air gapped! Impacts to business processes can be overcome by permitting access across enclaves by role-based exception. Such a redesign may be easier than you think to implement and manage, but segmentation can reduce exposure by limiting an attacker's access to the data in only one enclave.

Finally, honeypots & honey-nets have been around for a while, but recent advances in virtual technology, elastic computing, and sandboxing have vastly improved. These generation II & III honeypots can be leveraged to provide an early detection capability for new threats.

Advanced, adaptive honey-nets can also be developed to mirror your network while replacing real data with traceable data that may aid law enforcement in their efforts to track down cyber-criminals. Such a capability could be critical in turning the tide and striking a balance between defensive and offensive strategies.

Sources:
[1] http://www.virusradar.com/en/glossary/packer-crypter-protector

Russell "Rusty" Wilson
CIO

INGALLS INFORMATION SECURITY

Contact Info
www.iinfosec.com
Phone: (888) 860-0452

Russell "Rusty" Wilson is the Chief Information Officer of Ingalls Information Security, and has 19 years of experience in Information Technology, Cybersecurity, and Electronic Warfare & Signals Intelligence. He is a 16-year veteran of the Department of Defense (DOD), both Active Duty Army and Civil Service. He holds a Bachelor of Science degree in Network Design and Management and a Master of Science degree in Information Security and Assurance from Western Governor's University. Mr. Wilson is a Certified Ethical Hacker (CEHv8) and a Certified Hacking Forensic Investigator (CHFIv8). He maintains many other certifications including Security+, Project+, CCENT, ITILv3, GIAC G2700, MCSE+Security, and many others.