Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

JULY 2019

RSA® CONFERENCE HIGHLIGHTS: IMPROVING ACROSS THE BOARD

At the recent five-day RSA Conference of security professionals in San Francisco, two general themes materialized: (1) the need to focus on the improvement of technologies and forecasting and (2) understanding success. Within those themes, distinct trends and takeaways emerged as the focus for cybersecurity professionals.

Understand Technologies to Avoid Security Gaps

Speakers emphasized that security technologies are increasingly complex. This has led to gaps in security coverage, in part because employees do not fully understand the technologies. The complexity of technologies can also lead to misconfigured technology and security policy implementations across organizations.

For example, some organizations are not fully implementing two-factor authentication (2FA). The gap in usage is, in part, due to the need to explain why and how the technology functions in order to help users comprehend its importance.

DevSecOps: Integrate Security

Multiple sessions highlighted the need to adopt a revised view of the DevSecOps approach of developers and operations working together for a secure software development lifecycle. Previously, this approach has been more of a code scan after software is built and prior to production. With an integrated approach, development starts and continues within a secure environment.

Reverse Engineer to Evaluate Malware

In order to understand possible network and system vulnerabilities, including malware, the National Security Agency rolled out an open source, free reverse engineering tool called Ghidra designed to analyze malicious code and support greater threat intelligence.

Make the Most of Metrics to Forecast and Understand Risk

By using metrics, organizations can understand and forecast risk. In addition, when an organization defines its unique top risks, this knowledge can equate to greater success in thwarting and detecting the attacks.

Limit Risks by Employing Zero Trust

The need to trust systems in order for them to work was highlighted alongside the increasingly pervasive zero trust approach. Zero trust is an approach that inherently assumes all entities are untrustworthy until proven trustworthy. The assumption is malicious actions can occur at any time and organizations can combat these actions by performing ongoing evaluations and authentications as part of continuous analyses.

(continued)

Innovations in Cybersecurity: Duality and Axonious

Ten finalists vied for the prize of most innovative. Two technologies stood out among the others because they help solve complex common issues:

- **Duality**: maintains encrypted, private data, while still enabling collaboration
- **Axonious**: allows an organization to view and secure all of its IT assets

The Case for Integration

To avoid operating in silos that can lead to cybersecurity gaps, the concept of central control through a dashboard, orchestration system, or policy engine was explained. The concept does not require limiting suppliers, but is more focused on open APIs and the ability to connect data across technologies.

Focus on Education, Practice, and Collaboration

The human side of security was also discussed. From national defense to improving diversity within IT departments, there was a continued focus on cybersecurity education and training. In addition, experience, practice, and collaboration were also recognized as important to security improvement.

Source: Kerner, Sean Michael. *Top 10 Takeaways from RSA Conference 2019*, eSecurity Planet, March 11, 2019. https://www.esecurityplanet.com/network-security/top-takeaways-rsa-conference-2019.html.

SPEAR PHISHING FREQUENTLY TARGETS FINANCIAL DEPARTMENTS

Criminals continue to become more sophisticated in attacking organizations by taking phishing to the next level. While phishing makes use of fraudulent emails or messages—often executed broadly using botnets—to trick recipients into providing sensitive information or sending money, spear phishing tailors each message to the individual recipient. Individuals who can execute a financial transaction are frequently targeted, resulting in significant financial losses.

How It Works

- The criminal typically creates fake documents, including emails, invoices, or wire instructions
- Emails often appear to come from a higher level executive who can authorize wires or other electronic payments
- The messaging creates a sense of urgency to execute a transfer on behalf of a higher level employee

Email security, employee education, and dual control for authorizations can help prevent spear phishing attacks that result in financial and data losses.

Source: Olson, Scott. *The impact of spear phishing on organizations and how to combat this growing threat*, Help Net Security, March 11, 2019. https://www.helpnetsecurity.com/2019/03/11/spear-phishing-impact/.

UNDERSTANDING DIGITAL CERTIFICATES: HOW EXPIRATIONS IMPACT APPLICATIONS, SERVICES, AND THE BOTTOM LINE

When individuals log in to applications or services, they typically input usernames and some type of passwords or other authentications for authorized access. In order for machines to securely identify themselves to other applications or services, they use digital certificates. The complexity and interdependence of machines has increased digital certificate usage. This means that when digital certificate expirations occur, the reliability of networks and services can be degraded and it can be difficult to identify and fix the actual outages.

The majority of companies routinely experience outages, which significantly hamper vital processes required to doing business, thus affecting revenue. Organizations can minimize outages with certificate lifecycle visibility and automation.

Source: Help Net Security, *CIOs admit certificate-related outages routinely impact critical business applications and services*, Help Net Security, March 29, 2019. https://www.helpnetsecurity.com/2019/03/29/certificate-related-outages-harm/.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.

8913482-M-Online (07/19)