radware

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18

EXECUTIVE SUMMARY

Throughout 2017 mainstream headlines highlighted cyber-attacks and security threats that included possible interference in the U.S. presidential election, worldwide malware outbreaks and the Equifax data breach. These and other high-profile events spurred greater cyber-defense investment by everyone from nation states and global corporations to individuals purchasing anti-malware solutions for personal devices. Yet even as investments increase so do threats, hacks and vulnerabilities.

Understanding these complex and challenging dynamics is what drives Radware's *Global Application and Network Security Report*. This report brings together findings of a global industry survey, Radware's organic research, real attack data and customer stories to paint a picture of where we are and what security professionals can do.

The entire security community can benefit from this report, which highlights Radware's research and insights on:

- The threat landscape—the who, what and why of attackers
- Potential impact on your business, including associated costs of different cyber-attacks
- Preparedness levels by industry
- Experiences of organizations in your industry
- Emerging threats and how to protect against them
- Predictions for 2018

PUSHED TO THE LIMITS

The top driver of cyber-attacks is now cyber-crime. Attackers are motivated by financial gain and driven by the prosperity of cryptocurrencies Meanwhile, attacks are becoming more targeted. A determined enemy will take the time to learn the target by investing in reconnaissance, social engineering and specific tools.

Malware and bots and socially engineered threats emerged as the most common attack vectors. But organizations should not merely fear the threats in front of them. They should also fear what's lurking around the corner—including IoT botnets, Permanent Denial-of-Service (PDoS), SSL-based attacks and sophisticated injections of malware. Organizations can prepare by becoming familiar with new technologies such as IoT, blockchain and Function-as-a-Service (FaaS)/serverless computing.

Regulations continue to play an important role in raising the bar for security—providing guidelines and standards per industry or region. While many organizations are working to comply with security and privacy standards, they seem less concerned with compliance and certifications when evaluating security solutions. It turns out that some organizations are not familiar with all certifications and nearly one-third never ask vendors about them.

Massive global cyber-attacks in 2017 succeeded simply because of unpatched vulnerabilities. That represents a small and common human mistake with devastating impacts. Machine learning and artificial intelligence (AI) might seem like the logical solution. Twenty percent of organizations already rely on such solutions and another 28% plan to implement them in 2018. But they aren't fail-proof. Just consider the risks of AI poisoning, automated systems being thwarted and how such systems can go awry (e.g., Microsoft Tay and Facebook's chatbots).

Add it up and it's clear we are facing a precarious gap. Humans are reaching the edge of our collective ability to maintain control. Yet AI and machine learning still aren't sufficiently mature and can easily be tricked.

OTHER FINDINGS & HIGHLIGHTS

Ransom Motivated Every Other Attack

With the value of Bitcoin skyrocketing so did attacks motivated by ransom. Organizations cited ransom as the driver for half of all attacks, making it the top motivation and more prevalent than insider threats, hacktivism and competition to list a few. Globally 42% experienced ransomware attacks, a 40% increase from 2016.

Top Concern: Data Leakage

Data leakage/information loss emerged as the number-one security concern, cited by 28% of organizations globally. Service level degradation/outage was another top concern, cited by 23%.

DDoS on the Rise, Hitting Harder at the Application Layer

The prevalence of DDoS attacks grew 10%, hitting nearly two in five businesses. One in six suffered an attack by an IoT botnet and 68% of attacks resulted in a service degradation or complete outage. Both carry associated costs. 2017 also brought an increase in application-layer vs. network-layer attacks.

80% Aren't Tracking Costs

Eighty percent of organizations aren't calculating the cost of cyber-attacks. One in three still lack an emergency response plan even though cyber-attacks are becoming a near-daily fact of life. Alarmingly, following one in four attacks, a customer will leave or sue the attacked organization.

Security Still 'Cloudy'

Organizations cited security misconfigurations (26%) and application vulnerabilities (23%) as top risks in cloud environments. They also reported that 51% of cloud applications undergo changes weekly (a 16% increase compared to 2016). Frequent changes pose a visibility and control challenge to security professionals, especially when one-quarter of the applications are mission critical.

The most frequent security challenge when migrating applications to the cloud is control, governance and lack of visibility, indicated by 46% of organizations. Next are lack of expertise and know-how and additional complexity managing security policies. Interestingly, 51% of public cloud users also rely on cloud providers' security services and add them into the bundle even though these providers may not be security-focused companies.

Blocked Potential?

Blockchain is a hot technology topic, yet 36% of respondents admit they don't understand its mechanism. Only 10% think blockchain will improve information security.

Education Not Making the Grade

Education is the least-prepared vertical to face a different set of cyber-attacks. This marks the second year in a row that this sector has ranked lowest.

72% Unprepared for GDPR

Nearly three-quarters of organizations (72%) say they are not well prepared for the EU's General Data Protection Regulation (GDPR). Sixteen percent of those respondents do not even know what GDPR is.

Security teams can use findings and insights from Radware's annual *Global Application and Network Security Report* when analyzing the threat landscape and designing security strategies to protect their enterprises. As cyber attackers constantly evolve targets, techniques and attack vectors Radware also encourages organizations to stay ahead of the game by visiting its security resource center – DDoSWarriors.com.