Hewlett Packard Enterprise

Cyber Risk Report 2016 highlights

Information security: Detecting unknown threats has never been more important

The annual Cyber Risk Report from HPE Security Research helps you understand how hackers attack and where you are most vulnerable. This year's cyber security research report presents a broad perspective drawn from more than 3000 HPE and independent researchers, open source intelligence, and partners like ReversingLabs and Sonatype. Advanced data analysis provides compelling reasons to use security information and event management (SIEM) solutions to detect and resolve both known and unknown threats before the damage is done.

Attackers are broadening their attacks.

Malware research data:
- Attackers increasingly target applications.
- Malware targeting Linux increased 212%.
- An increasing percentage of new malware targets financial gain.

Attacks resulted in collateral damage:
- US Office of Personnel Management breach—stolen employee records exposed associates and families.
- VTech breach—exposed profiles and photos of more than 6 million children.

Breaches reached massive new scales.

Defenders continue to fall behind.

Almost half of large enterprises surveyed lack a formal threat intelligence and security operations center.

Spending focused on the network layer can leave other resources unguarded.

Many organizations surveyed fail to collect or process important security events.

72% of organizations surveyed fail to monitor internal applications for security events.

57% of organizations surveyed fail to monitor external-facing applications for security events.

Most Web and desktop apps contain vulnerabilities that can open the door to attackers.

35%
of non-mobile apps tested exhibited at least one critical- or high-severity vulnerability.

90%
of Web apps tested misused security features.

Lengthy remediation times leave companies vulnerable.

31%
of critical-severity application vulnerabilities took more than 60 days to remediate.

42%
of high-severity application vulnerabilities took more than 60 days to remediate.

Failure to apply patches increases the attack surface.

- The most exploited vulnerability in 2015 has been patched for 5 years.
- The top 10 exploited vulnerabilities are more than a year old.
- Almost half of exploited vulnerabilities are 5 or more years old.

Key takeaways for information security professionals:

- Breaches may result in collateral damage when personal data is compromised.
- The overall attack surface continues to grow.
- Financially motivated attacks on ATMs and the banking industry are on the rise.
- Unpatched software lets attackers exploit old vulnerabilities while finding new ones.
- Remediating vulnerabilities and deploying patched software take too long.

HPE Security recommendations:

Organizations need security that is **built in rather than bolted on**—where **analytics proactively detects and responds to threats** and regulatory and compliance solutions minimize damage in the wake of disaster.

Protect your organization with the HPE Security ArcSight comprehensive security information and event management (SIEM) solution that enables cost-effective compliance and provides advanced security analytics to identify threats and manage risks.

Enable your organization to fearlessly innovate.

Protect your business with HPE Security.

hpe.com/software/cyberrisk

4AA6-4619ENW, April 2016