Hewlett Packard Enterprise

CYBER RISK Report 2016

The annual Cyber Risk Report from HPE Security Research provides organizations with a better understanding of the threat landscape and supplies resources that can aid in minimizing security risk. This year's report features perspectives drawn from advanced data analysis and takes a focused look at multiple technologies, including open source, mobile, and the Internet of Things.

35%

Over one-third of the applications scanned – 35 percent – exhibited at least one critical- or high-severity vulnerability.

Nearly **86%** of enterprises surveyed state they are using IDS.

The use of open source components in applications has increased. **14%**

153%

Over 10,000 new threats were discovered daily on the Android platform, reaching a total year-over-year increase of 153%.

80%

Over 80% of open source and commercial applications suffer security feature vulnerabilities, with serious implications for management of private data.

With 95% of newly discovered malware samples and 42% of exploits targeting Windows, that OS remains the dominant platform for attack.

Mobile applications that suffer from internal system information leaks highlight the concern for storing business critical data on easily lost devices.

29% of all exploit samples discovered in 2015 continued to use a 2010 Stuxnet infection vector that has been patched twice.

The year of collateral damage

Data compromise is no longer just about getting payment card information. It's about getting information capable of changing someone's life forever.

Overreaching regulations push research underground

Various proposed regulations governing cybersecurity would push legitimate security research underground. These regulations should instead protect and encourage research that benefits everyone.

Moving from point fixes to broad impact solutions

2015 saw a shift by vendors toward developing defensive measures that prevent entire classes of attacks.

Political pressures attempt to decouple privacy and security efforts

Many lawmakers in the US, UK, and elsewhere claimed that security was only possible if fundamental rights of privacy and due process were abridged.

The industry didn't learn anything about patching in 2015

The #1 most exploited vulnerability in 2015 is over five years old, was the most exploited in 2014, and has been patched by the vendor...twice.

Attackers have shifted their efforts to directly attack applications

Applications are now seen as the easiest route by which attackers can access sensitive enterprise data.

The monetization of malware

ATM-related malware has become more common, making more money more quickly for cybercriminals.