Hewlett Packard Enterprise

SERVER MANAGEMENT AND SECURITY

TODAY'S EXISTING SECURITY THREATS

Security Today

Denial of Service (DOS):
Make crucial changes to the target's firmware that interfere with it's ability to perform key functions.

Distribution Denial of Service (DDoS):
Overwhelm the target with bogus requests for information or assistance from multiple sources, tying up resources and hindering its ability to respond to legitimate users.

Data Theft or Information Theft:
Malware or compromised code copied directly into the target's firmware renders it completely useless. Sometimes called "bricking" a server, i.e., rendering it as useful as a brick.

Permanent Denial of Service (PDoS):
Bricked or permanently disabled servers.

Ransomware:
Hostile software that invades a PC or server and locks it permanently, preventing legitimate users from accessing any content unless a ransom payment is made.

SECURITY ATTACK TRENDS

- **Hardware & firmware attacks**
- **Regulatory, GDPR, SEC**
- **Machine learning and AI**
- **Human element**
- **Pervasive ransomware**

COST OF CYBER CRIME AND THE RISK OF BUSINESS INNOVATION

Security Today

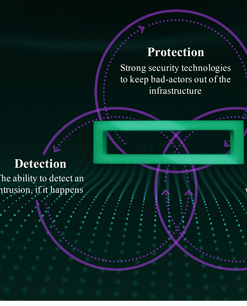
More innovative businesses risk higher losses
because their proprietary information is more valuable

Business disruption is the most significant
consequence of cyber crime

Advanced access management and encryption technologies
help reduce the cost of cyber crime and provide encryption at scale.

Persistent use of advanced security information and event management (SIEM) results in an average savings of nearly $3 million.

SECURITY REQUIRES DEFENSE IN DEPTH



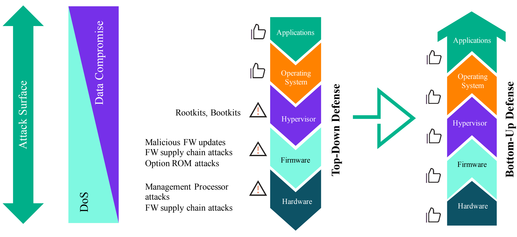
Protection
Strong security technologies to keep bad-actors out of the infrastructure

Detection
The ability to detect an intrusion, if it happens

Recovery
Recovering rapidly from a breach, without suffering the consequences of down-time or data loss

HPE SECURITY VISION: SERVER PLATFORM SECURITY

HPE servers comprehensive security approach protects key server infrastructure



HACKERS USE ARTIFICIAL INTELLIGENCE

Bypassing CAPTCHA	Improving Phishing	Evasive Malware
Using AI techniques researchers at Columbia were able to get by Google reCAPTCHA 98% of the time.	A reported 76% of organizations fell victim to phishing attacks in 2017. AI identifies valuable targets and quickly develop a profile of that target based on what they have tweeted in the past. Using this approach targets click on malicious links 30% of the time (compared to the 5-15% success rate of other automated approaches).	AI performs checks to identify hardware configurations and if a human is operating the machine DeepLocker's AI is trained to ensure that its payload only executes when it reaches a specific target, relying on three layers of concealment to prevent security tools from identifying the threat.

Source: Artificial Intelligence Part 2: Cyber Criminals Get Smart with AI, August 27, 2018, Stephen Helm

SECURITY TODAY - REAL WORLD EXAMPLES

Evolving Threats

Global Security Threats

Cyber crime will cost the world economy

$6 Trillion

by

2021*

Real World Examples

Large Oil Company
30,000
Systems Destroyed by Malware in Firmware

Large Credit Firm
$4B
Cost to Company

Cybercriminals try to corrupt a BIOS update…*

*Federal Bureau of Investigation, James Morrison, June 22, 2017

As security software becomes more prolific, hackers continue to make their way down the food chain to computer hardware where it is much more difficult to identify and remove.**

*Cyber security business report, October 19, 2017, by Steve Morgan
**New York Times, Technology Section, Jan 22, 2014, Nicole Perlroth

For more information on HPE Gen10 Servers, contact us today:

Summit Partners
http://gosummitpartners.com