State of Network Security

August 2014
Background and Methodology

• Wanted to explore the main challenges on managing network security and where companies are lacking in security products/practices.

• 205 completed interviews were collected via an online survey

• Qualified respondents were located in the United States and met the following criteria:
  - Work full time in a MIS/IS/IT/Networking/Technology-related job function in a company with:
    • 100+ employees
    • At least $1 million in annual revenue
  - Must make decisions or provide input into decisions made for technology solutions used within the organization

• Respondents were questioned on corporate IT security initiatives, specific concerns regarding network security and the nature of attacks and threats as well as their source.

• Field dates: June 30 – July 15, 2014
Demographics – IT Professionals

**Industry**

- Services: 48%
- Manufacturing: 16%
- Finance/Insurance/Real Estate: 12%
- Transportation/Communications/Utilities: 9%
- Public Administration: 5%
- Construction: 3%
- Retail: 3%
- Other: 2%

**Number of Employees**

- 10,000 or more: 21%
- 5,000-9,999: 10%
- 2,500-4,999: 16%
- 1,000-2,499: 19%
- 500-999: 19%
- 100-499: 15%

Average = 5,100 employees

**Role within Organization**

- Manager: 21%
- Director: 43%
- VP-Level: 35%

**Annual Revenue**

- $1M-$4.9M: 13%
- $5M-$9.9M: 15%
- $10M-$99M: 33%
- $100M+: 40%

Average = $79.5 million

**Annual Network Security Spend**

- <50K: 3%
- $51K-$200K: 27%
- >$200K-$1M: 32%
- >$1M-$5M: 21%
- >$5M: 17%

Average = $2.6 million

Total Respondents (n=205)

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Survey Highlights

Balancing Security Posture with Corporate Policy
Social media and non-productive employee web browsing are top types of abuse happening on corporate networks.
More than half of IT professionals are “very concerned” with file sharing.
Survey Highlights

Increasing Network Security Budget
Over 3 in 5 IT professionals expect both network security costs and budgets to *increase* over the next 12 months.
Firms that spend $500K or more annually on network security are also significantly more likely to have breach detection and compliance as a corporate initiative.

Top Security Initiative: Embracing cloud or virtualization
Survey Highlights

Network Security Attack Landscape
Nearly 3 in 4 IT professionals have experienced **phishing** within their organization. Those who spend more on security tend to experience more types of attacks.
Customer data is cited most often as the type of data attacked, followed by financial information.
• IT professionals are most concerned with **external threats** in regards to security.
• Data center and endpoint security comprise a second tier of concern.
• Although **2 in 5** are concerned with BYOD, it falls to the bottom of the list.
China is stated most often as a country of origin for attacks, followed by Russia and the USA.
Over 3 in 4 IT professionals experience untargeted spam in their organization once a week or more.
Over a third of IT professionals have recently seen more attacks/threats from user activity, while 2 in 5 state they have not seen a change. Those who spend more annually in network security have seen more attacks.
Of those who have recently seen more attacks stemming from user activity, around 7 out of 10 are a malware infected host, around 6 out of 10 are malicious communication with the command and control site and over half are taking advantage of software vulnerability.

Top threats relative to these new attacks are primarily within the data center, mobile, and branch networks.
• Nearly 3 in 5 IT professionals are concerned with **Application DDoS**.
• Brute force attacks tend to be more of a concern among companies with higher revenue or spend more on security.
• On the other hand, companies who spend less on security are not as concerned about DDoS.
Survey Highlights

Rising Network Security Concerns
Manageability rises to the top as a key concern for migrating to SDN, followed by being in the early stages of planning and an attacker compromising the SDN controller.
3 in 5 IT professionals use IPS or NGFW to identify their “patient zero.”
HP’s Recommendations to Increase Network Security Posture

• Layered security is still relevant, especially in advanced threat scenarios
  - Organizations need perimeter firewalls all the way to application security solutions
  - Companies are layering IPS, NGFW, Sandboxing and SIEM products
• With so many application vulnerabilities annually
  - Companies have to consider the need for zero-day coverage
  - Using application controls in NGFW and remediating software app vulnerabilities is key
• Ensure you are spending your large (and increasing) Network Security budget on the right things
  - How are you addressing command and control traffic?
  - Are you able to block unfiltered spam or phishing attacks?
Thank you