Tools, Techniques and Technologies for Protecting the Endpoint

Alan Zeichick
Principal Analyst
Camden Associates
alan@camdenassociates.com
@zeichick

Camden
<Camden Associates>

It is estimated that the recent **WannaCry ransomware** attack will likely cause more than **US$4 billion** in **economic damage**, according to *USA Today*

Camden
<Camden Associates>

The endpoint is under assault

- Intercepts from public WiFi
- Weak physical security (lost/stolen devices)
- Clear-text transmission of passwords
- Malware from many sources
  - Phishing emails
  - Bad ads from advertising networks
  - Malicious websites
  - DNS redirects
  - Self-propagating worms
- Employee training will not protect the endpoint

Camden
<Camden Associates>

Endpoints, circa 2014

- Traditionally focused on end-user devices:
  - Desktops in the office or at home
  - Laptops/notebooks at office, home, coffee shops
  - Mobile phones/tablets anywhere, on WiFi or cellular
  - WiFi/wired network printers and scanners
  - Can be inside the protected LAN or anywhere
- Endpoint protection efforts and tools were mainly focused on end-user devices
- That traditional focus is no longer sufficient!

Endpoints, circa 2017

- End-user devices, as before
- Servers
  - Web, database, SAN/NAS, application, identity
- Network infrastructure
  - Switches, routers, WiFi access points
- Cloud-based services
  - SaaS, PaaS/IaaS
- Industrial devices & IoT
  - Point of sale, HVAC, medical devices, wearables, automotive
- Virtual resources
  - Virtual machines, containers

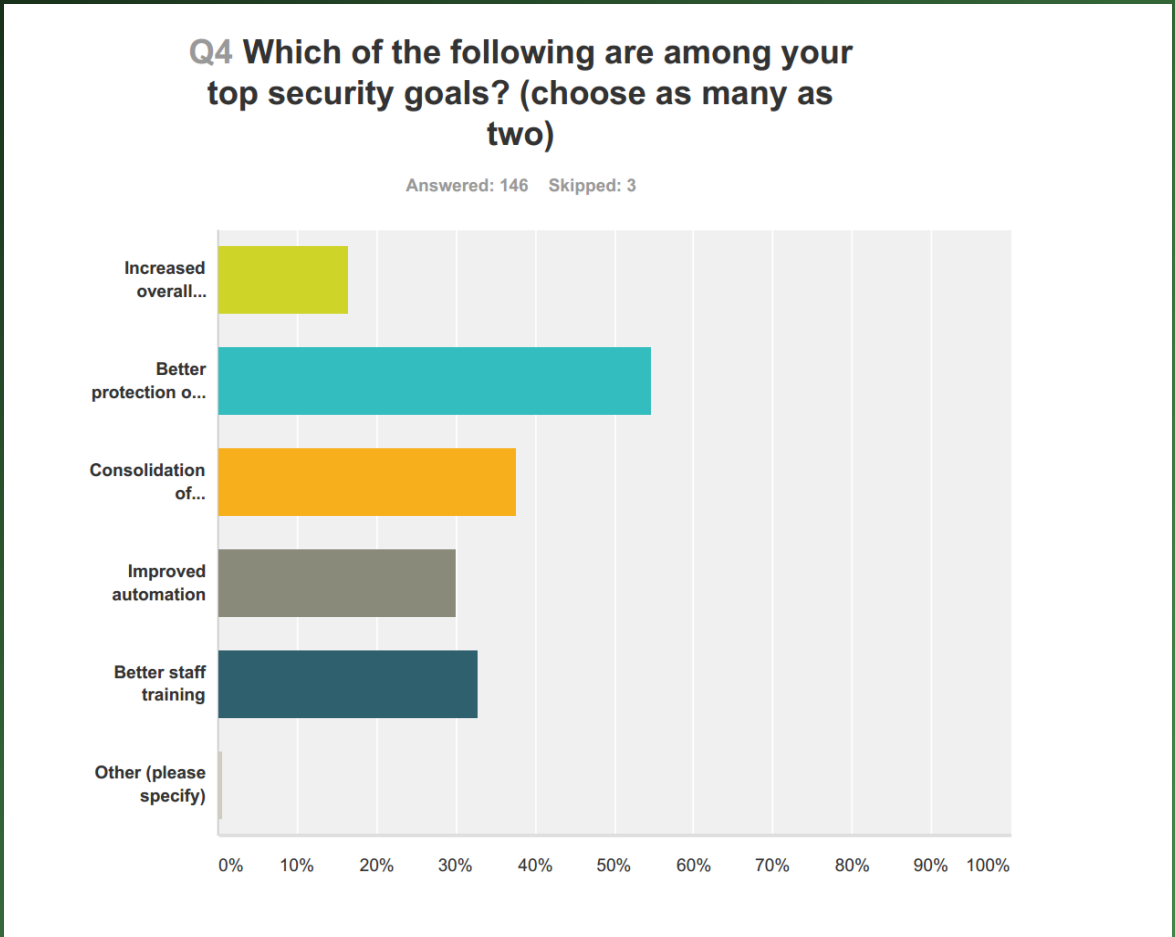
Protection is necessary

- Hackers can get in using many means
  - Malware, as mentioned before
  - Zero-day vulnerabilities
  - Unpatched operating systems (big for WannaCry)
  - Unpatched applications
  - Weak passwords
  - Flaws in Active Directory, other services
- Once the bad actor has a foothold, game over!

SysSecOps

- Systems Security Operations
  - Defined by Scott Raynovich in report due out tomorrow (Scott is now with Futuriom)
- SysSecOps is integration of systems monitoring and security tools
  - Gives IT managers are more holistic view of everything
- Needs to integrate many tools, technologies
  - AV, malware analysis, IDS, network monitoring, app performance monitoring (APM), cloud access service broker (CASB), systems and patch management, sec info and event management (SIEM), endpoint detection and response(EDR), etc.

Top security goals



Camden
<Camden Associates>

–Source: Scott Raynovich

And now, to our panel…

Camden

<Camden Associates>