Printers are Evil!

Why to segment printers, and how we did it

Ob: Disclaimer

While this is based on what has been, and continues to be, done to segment printers at my place of employment...

The views and opinions expressed here, or the fact that they are included here, do not necessarily reflect those of my employer

The Business Side

- Cost Per Page
- Shared Printers
- Document Security (Print Release?)
- Use a Print Server!
- Accountability… Accountability… Accountability

The Technical Side

- Printers are “soft” targets with *TONS* of vulnerabilities
  - Recent HP Fax problems
  - https://security.business.xerox.com/en-us/documents/bulletins/
  - https://www.cvedetails.com/vulnerability-list/vendor_id-2446/Canon.html
  - https://www.cvedetails.com/vulnerability-list/vendor_id-1287/Brother.html
- Printers aren’t just printers… copiers, fax, & email
- Nobody thinks about printers on their network
- How often are printers updated?

ACLS

Inbound - To the printers

- Print Server(s)
- Monitoring Server(s)
- Management host(s)

Outbound - From the printers

- NTP
- SMTP
- HTTP(s) to reporting server (PROXY)
- DHCP
- DNS
- LDAP
- SNMP

Pitfalls

- Fiery Engines
- Scan to Computer/Network Storage
- Cloud Services
- Printers being moved
- Other devices connecting to VLAN

- Open to SMTP
- LDAP access
- Local storage on device
- Lateral movement
- ACL ‘creep’
- ACL vs. Firewall

Tools We Use

- PaperCut - Print accountability & “Find-Me”
  - https://www.papercut.com/
- PacketFence - Port-Level Authentication
  - https://packetfence.org/
- Squid - Proxy
  - http://www.squid-cache.org/
- Nagios core- Monitoring & Alerting
  - https://www.nagios.org/

Questions?

Biography

Frank Barton is a systems administrator working in higher education where he manages a fleet of over 100 servers, both physical and virtual, windows and linux.

Frank holds his M.B.A. and B.S. in Computer Information Systems from Husson University, and his A.A.S. in Computer Systems Technology from Eastern Maine Community College. In addition to this, he also holds a current Security+ certification

He can be reached via email at FBarton@Gmail.com

He tweets @FBarton

He also blogs (infrequently) at https://experiencesofasysadmin.wordpress.com/