
# Covering Security Bases for Your Small Business (SMB)

Jason Dahl, Senior Security Engineer, Network Center INC.

# 1. What is the largest vulnerability on your network?

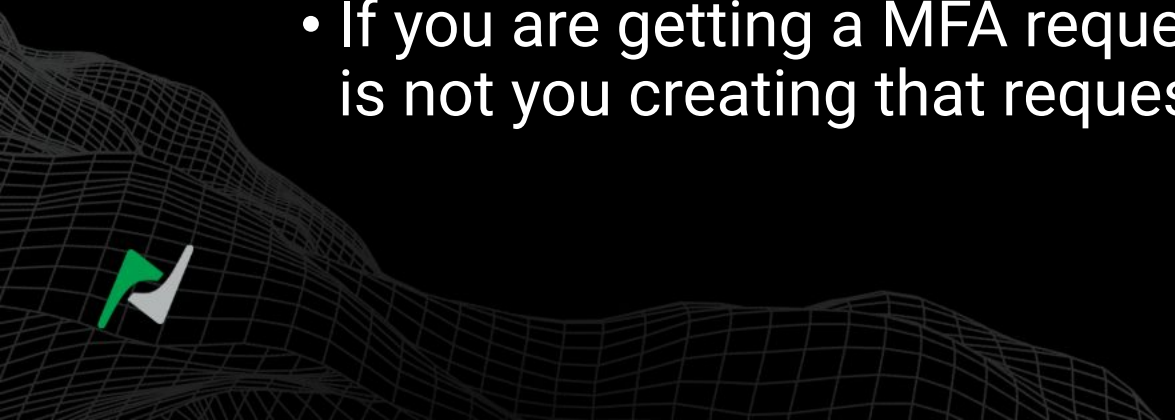
- Internal Users
  - Users unknowingly cause the majority of all cyber security incidents, yet we only train once a year or not at all.
    - Users need to be trained on how to spot a malicious URL, phishing email, or a possible malicious attachment. The users will always be your first line of defense against ransomware, stolen passwords or email take overs.
    - Training is vital to keep users properly educated on how to spot a malicious email or phone call also when they should get an alert and when to act. The training needs to be continuously evolving and digestible to keep up with current threats and trends.

# 1. What is the largest vulnerability on your network?

- Senior leadership, Human Resources, Accounting, and Information Technology are the biggest targets within your company. Each one of these groups hold resources attackers and hackers, love to steal, sell, and ransom.
  - Cost on the Black Market, Everything has a COST.
    - Credit Card – Premium Card with Big Balance - $250
    - Credit Card and Social Security Number - $5
    - Email Address – Gmail - $200 for 1,000
    - Online Bank Account – USA – 2% of Account Balance
    - Remote Administration Tool - $40
    - Login credentials for unhacked Windows servers for use with RDP - $20

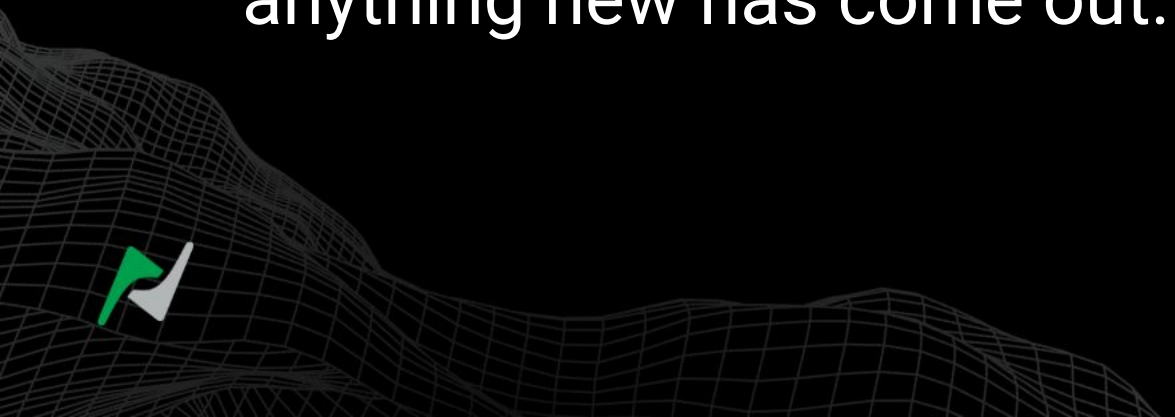
# 2. We use Multi-Factor Authentication everyday.

- What is Multi-Factor Authentication?
- Implementing MFA is vital for all organizations regardless of their size.
  - MFA is not a silver bullet; attackers can still access your account if your users are not aware why they are accepting a code or MFA pop-up.
    - Going forward, providers are working on different solutions, so users do not get MFA fatigue or accidentally allow access when someone else is making the request.
  - If you are getting a MFA request at midnight and you are sleeping, that is not you creating that request.



# 3. Keep all devices up to date and on current hardware.

- All devices, firewalls, switches, routers, APC power supplies, iLO devices, printers, and many other devices should be updated regularly. A large portion of these devices are overlooked because once they are setup, we make few changes.
- Making sure your VPN clients and software is also updated on regular schedule. Set up a calendar alert for a monthly or quarterly review of your current version and determine if anything new has come out.

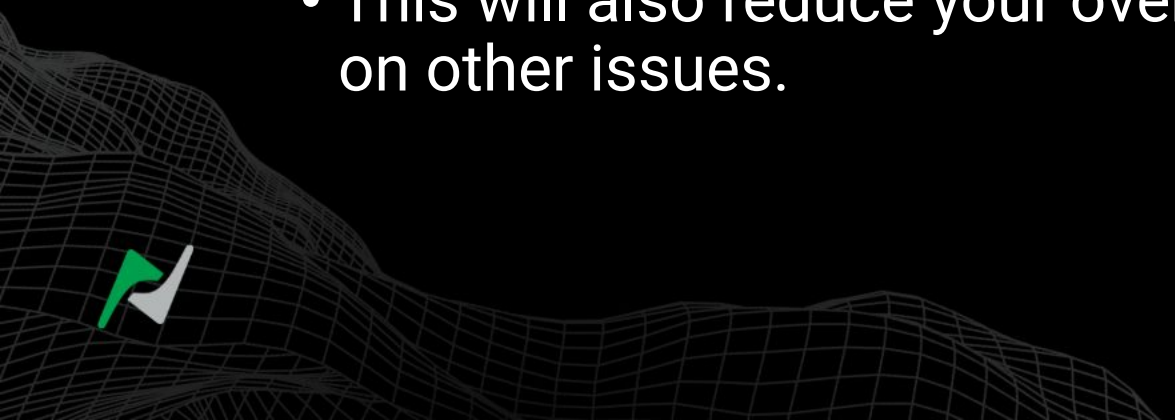


# 3. Keep all devices up to date and on current hardware.

- Include infrastructure devices in your 5-year budget to replace.
  - Technology and cybersecurity will always be changing, and these infrastructure devices need to be prioritized. These devices are normally forgotten about because we don’t administrator them every day.
- Know what type of device you have and sign up for alerts from that company.  Fortinet, Cisco, etc., all have alerts they send out when a critical security patches are needed.

# 4. Reduce software footprint on all devices

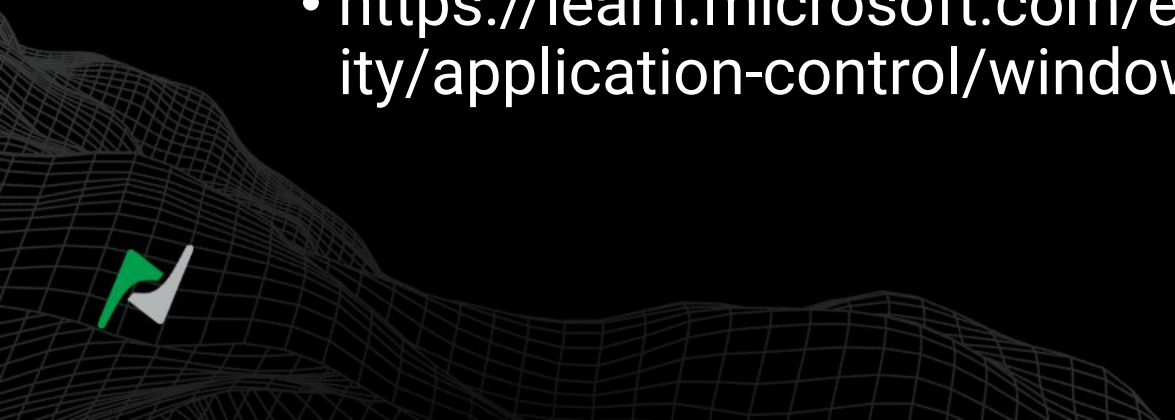
- This is about reducing your systems needing to be updated continuously and reducing security weaknesses.  As an example, select one browser (Chrome, Firefox, Edge, etc.), this will reduce the overall attack surface for those devices.
  - Reducing your attack surface makes your system as minimalistic as possible.  The fewer applications the few security threats.
- Don’t install productivity software on servers. (Term Server Exception)
  - This will also reduce your overall IT cost, having your technicians focus on other issues.



# 4. Reduce software footprint on all devices

- Implement Windows Defender Application Control (WDAC) which is built-in feature from Windows 10 and 11.
  - This is the most effective way I have seen a ransomware attack stopped. You do need to have it setup for strict control.

  - https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/



# 5. Develop a basic Incident Response Plan

- Knowing what it takes to run your day-to-day operations is vital, disasters happen all the time. Even if they are not IT related, we all have disasters that come up. All employees should be aware of where to find the plan and how to use it.
- Key areas to consider when developing your plan
  - Email
  - Phone System
  - File Shares
  - Backups
  - Emergency and key phone numbers
  - Organizational chart

# 6. Implement System Hardening guidance

- What is system hardening?
  - Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerabilities.
- Many different types of system hardening guidance available, operating systems, application, network, endpoint, and servers.
- Center for Internet Security (CIS), has a large selection of guides that are free for download.
  - CIS guidance should work to implement all Level 1 settings for the windows operating system.
  - Guides help you setup the Group Policy or Local Policy settings for the windows operating system.

# 7. Domain Name Service (DNS) ooo
# DO NOT use Google DNS servers.

- What is DNS?
  - All computers use numbers to communicate.  We have a difficult time remembering these long numbers, so DNS was invented.  This takes the number and assigns it to an easier to remember name.  “yahoo”
  - Almost all websites will have a name associated to it, “www.yahoo.com”.
  - DNS does a reverse lookup for a website.  The search starts at root [.], followed by the organizational grouping .com, .org, .gov; than it’s the organizations name, yahoo, google, microsoft; finally, the server website www, login.
  - The search would look like this .com.yahoo.www to the DNS server.

# 7. Domain Name Service (DNS) ooo
# DO NOT use Google DNS servers.

- How does moving to OpenDNS or a similar service help my organization overall?
  - Using a Private DNS server can help prevent employees from connecting to current or active malware attacks. These services monitor threat intelligent attacks and remove or block those URLs from getting accessed.
  - You can also get reports letting you know where employees are connecting too.  If you start to see uncommon URLs you can research and verify, they are legitimate sites.
- Google DNS is a great resource to test DNS, but attackers rely on the same common Public DNS.
  - Malware uses DNS a lot of the time, public DNS. Blocking would stop the attack.

NETWORKCENTER INCORPORATED

# Questions?

Network Center offers a Baseline Security Assessment.

Find out where you are to find out where you need to go!