Security for the "Have Nots"

Jake Williams
@MalwareJake
jake@malwarejake.com

Agenda

- "Haves" and "Have Nots"
- Best Practices and Resources
- Going Low Budget

$whoami

- Security researcher and risk management consultant
- IANS Faculty, former SANS Instructor
- Formally endorsed by Russian intelligence
- Digital terrorist, breaker of software, responder of incidents, reverser of malware, injector of code, spaces > tabs
- **Dislikes:** self-appointed “thought leaders,” snake oil AI grifters that are somehow more obnoxious than crypto bros, and anyone who **needlessly adds blockchain** to a software solution

Who Are We This Talk For?

- This talk is primarily aimed towards organizations that either have no dedicated security FTEs or are making their first dedicated security hire
- If this isn't you, but you're a consultant, this still matters to you
  - Please stop giving BAD ADVICE™ to your SMB (small-medium business) clients
- Even if you're a security architect at a Fortune 500, you might take something away from this, but the talk was **not written for you**…

Haves and Have Nots

- In cybersecurity, as in practically every walk of life, there are have and have nots
- To channel my inner Diddy - it's about all about those Benjamins baby…
- Let's talk about a real-world situation

Photo: Creative Commons

Be Clear About What's Achievable

- When working in SMB security, carefully evaluate what you can and can't do
- **When everything is a priority, nothing is…**
- You aren't trying to keep APTs out, you're trying to stop the most obvious of attacks
  - And recover from those you don't stop…

Best Practices Are Situational

- Best practices depend entirely on your situation
- When evaluating whether to apply a "best practice" make sure you understand how it applies to you…

Build or Buy?

- Many small businesses gravitate to build (or implement) open source for security tooling due to low budgets
- Build is almost always necessary for some orgs at some level, but be thoughtful about where skills and resources intersect
- There are 2080 work hours in a year – for everything you choose to do, you're actively choosing **not** to do something else
  - Was that something else higher priority?

Build vs Buy - Don't Forget About Maintenance

- Sure, you have the skills today for that solution
- **Key takeaway:** the fewer people you have, the more important every single one of them is
- Every staff turnover has a disproportionate impact relative to larger orgs

Your Threat Model…

IS YOUR THREAT MODEL

If these recommendations aren't for you, then they aren't for you.

PERIOD

Warning: Vendor Tears Ahead

Sorry vendors: most of your solutions are overly complex and too expensive for most SMBs

FCC SMB Cybersecurity Recommendations

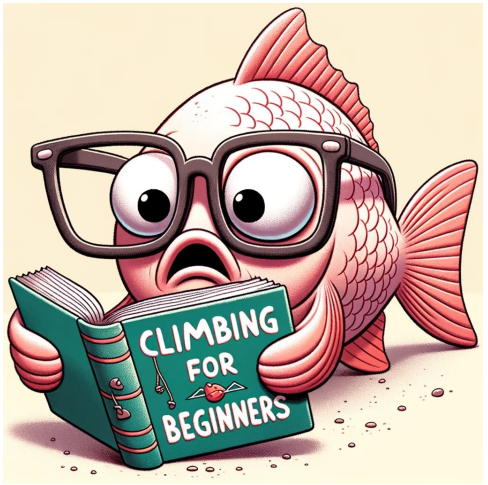
- Train employees in security principles
- Protect information, computers, and networks from cyber attacks
- Provide firewall security for your Internet connection
- Create a mobile device action plan
- Make backup copies of important business data and information
- Control physical access to your computers and create user accounts for each employee
- Secure your Wi-Fi networks
- Employ best practices on payment cards
- Limit employee access to data and information, limit authority to install software
- Passwords and authentication
- https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Kaspersky Cybersecurity Recommendations (1)

- Train your employees
- Carry out risk assessment
- Deploy antivirus software
- Keep software updated
- Back up your files regularly
- Encrypt key information
- Limit access to sensitive data
- Secure your Wi-Fi network
- Ensure a strong password policy
- https://usa.kaspersky.com/resource-center/preemptive-safety/**small-business-cyber-security**

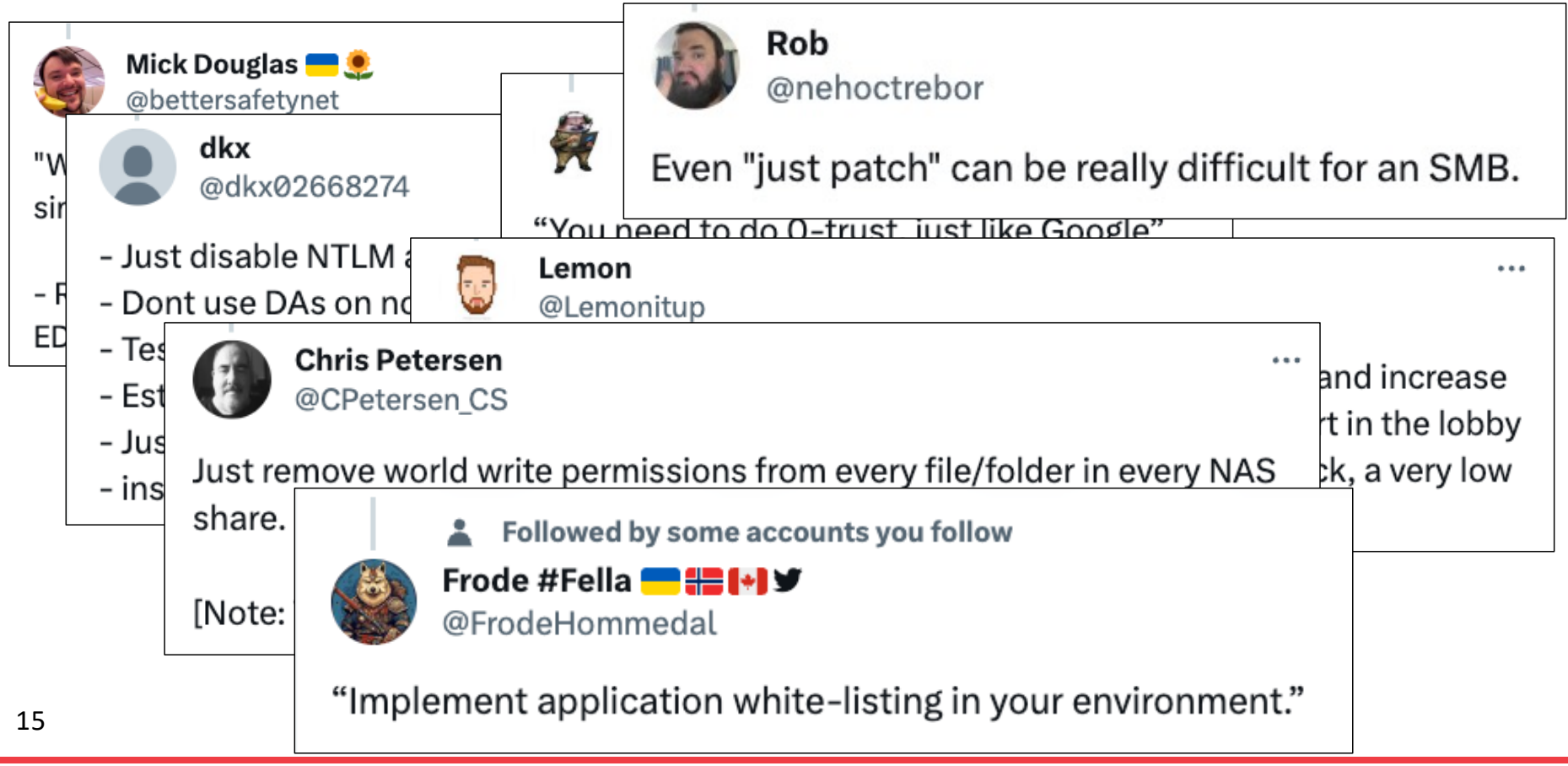
Kaspersky Cybersecurity Recommendations (2)

- Ensure a strong password policy
- Use password managers
- Use a firewall
- Use a Virtual Private Network (VPN)
- Guard against physical theft
- Don’t overlook mobile devices
- Ensure third parties who deal with you are also secure



I'm sorry, who TF exactly is this advice targeted to?
Are we **SERIOUSLY** telling small businesses to build a third-party risk program?

Bad Advice to SMBs – (Dis)Honor Roll



SMB Goals: Data > Prevention

- When you lack resources to stop the majority of attacks, focus on having the data for detection and investigation
- That data will help prioritize future security efforts when you have budget and time

Deploy an EDR Agent You Can Afford

That's it – that’s the slide

SMB/SME Recommendations – Email

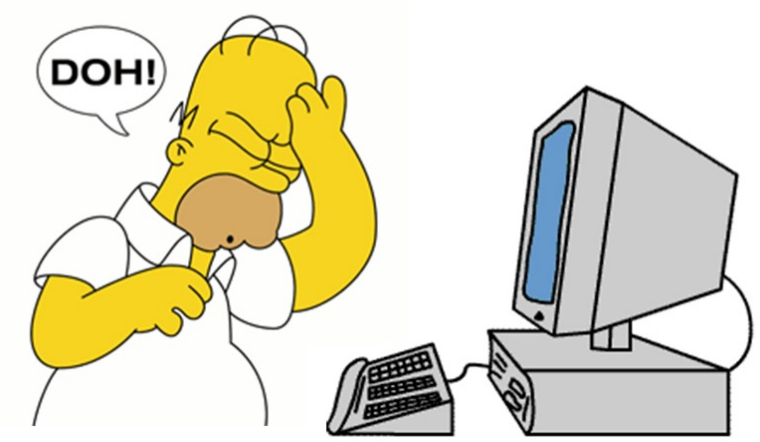
- Don't host your email locally
  - Microsoft has all but killed Exchange
  - Repeat after me: **Exchange on-prem is indefensible**
- If you're still running Exchange, call an IT MSP and have them transition you to M365 **today**
- I didn't say "do it yourself"
  - They do this all the time
  - There are few ways to do it right and **SO MANY** ways to get it wrong
  - The cost of getting it wrong is huge
  - Your time is more valuable

SMB/SME Recommendations – File Shares

- Don't host file shares locally
- Yes, the cost for on-prem file storage is cheaper on a per-GB basis
  - But you don't have time and resources to effectively manage a SAN or NAS
  - And it's increasing your attack surface…
- Online file storage (e.g., OneDrive, Dropbox, etc.):
  - Minimizes ransomware impact
  - May implement version control
  - Backups are included
  - Easier for users to self-service

SMB/SME Recommendations – DNS

- Use group policy or enterprise browser management to disable DoH
- DNS over HTTPS is great for privacy, but horrible for security monitoring
- You're not engineering for privacy, you're engineering for monitoring



SMB/SME Recommendations – Network Monitor

- Most firewall logs are not sufficient for incident investigations
  - Don't wait for an incident to find this out
- Security Onion is **trivial** to deploy
- It runs just fine on legacy (lifecycle replacement) server hardware for almost any SMB/SME sized network
  - Full disclosure: Security Onion isn't necessarily something I'd use in some very large security deployments, but that's not what we're talking about here…
  - You don't need to do any configuration, just let it run

SMB/SME Recommendations – Network Taps?

- Network taps are often expensive and out of the reach of most SME's
- Dualcomm has a 10G tap for **$699**
- $699 isn't nothing, but it's well within the reach of almost every business to enable full north/south monitoring

ETAP-XG

SMB/SME Recommendations – Event Logs

- Increase the size of your event logs with GPO
  - There's no reason for 20MB default sizes before event logs roll over
- Most SMBs can't operationalize a SIEM anyway
  - But as long as the logs haven't rolled over, they're available for investigations
- Consider deploying Sysmon with the Swift On Security template

SMB/SME Recommendations – Print Monitoring

- The Print Service/Operational log (if enabled) will log all print jobs, including those made to USB printers
- You get a full log of:
  - The user who printed the job
  - The filename printed
  - The printer it went to
  - The number of pages printed
- This is invaluable for investigations
  - Bonus – this catches print to PDF too ☺

Don't DIY Security Monitoring

Outsource this or be ***abundantly clear*** with stakeholders you're unlikely to catch the ***vast majority*** of intrusions

SMB/SME Recommendations – Disable USB Write

- You don't need fancy DLP software to get rid of the most common issue in SMB data loss:
  - Someone coming in with a 12TB "Best Buy Special" and walking out with all your data
- GPO settings on all modern versions of Windows facilitate blocking USB devices for read, write, and execute operations

SMB/SME Recommendations – Patching

- Patching is demonstrably difficult for even the most mature organizations
  - Patching 3rd party applications?
  - Forget about it
- Remote and hybrid workers complicate this even further…
- Invest in a patching solution like Automox or PDQ that just works
- This is an **easy** cost-justified buy over build decision

SMB/SME Recommendations – CSPM

- CloudSploit is a functional, open-source CSPM that is pretty low lift to get up and running to audit various public cloud providers
  - https://github.com/aquasecurity/cloudsploit
- But…

Should SMB's Be Using Cloud Infrastructure?

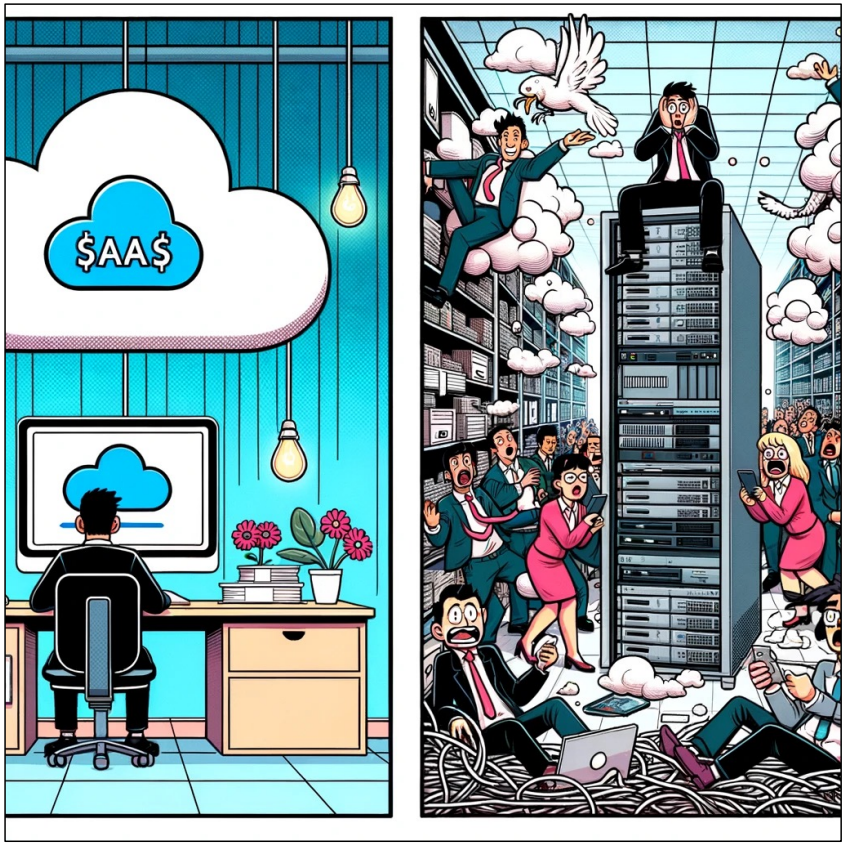
- Unpopular opinion: running infrastructure in a public cloud complicates security to an unacceptable level for most SMBs
- Like all advice, this is situational - evaluate your specific circumstances
- Most SMBs can achieve far better security redirecting resources to securing less complex VM deployments on-prem
- Complexity is the enemy of security

SMB/SME Recommendations – Offline Backups

- Offline backups are key for recovering from a ransomware attack
- An easy and cost-effective way to facilitate offline backups is to purchase multiple appropriately sized network attached storage devices and ensuring one is always offline
- Backups go to unit-A
  - A is operational
  - A syncs to B
  - B is taken offline and replaced with C
  - A syncs to C

SMB/SME Recommendations – Use SaaS

- Use SaaS wherever you can
- Just because you can implement something on prem, doesn't mean you should
- Remember: your time is valuable and you'll have to secure anything you're running on-prem
- SaaS only looks expensive to SMBs when they neglect to factor in labor and inevitable downtime



SMB/SME: Off Limits

- Solutions most SMB/SME's shouldn't waste their money on:
  - Managed "threat hunting"
  - CTI feeds
  - Phishing testing
  - Commercial security awareness training
    - Doubly so if it includes videos of Delta Force jumping out of vans…
  - Fancy "ransomware prevention" tools
  - Zero-trust solutions
  - AI-penetration testing
  - Commercial PAM solutions

Conclusions - Wrapping Up

- SMB security isn't about adapting best practices that work for big orgs
- Start with realistic security goals and adopt solutions that meet those goals
- When consulting with SMBs, meet them where they are, not where they'd be with infinite budget

Jake Williams

@MalwareJake

jake@malwarejake.com