

too
small
to
fail

Securing Small and Medium Businesses

@HomeBrewedSec
#SecuringSMB

Audience Participation

- I won't be having a Q&A time (*use the hashtag*)
 - Q&A *usually* isn't inclusive for speaker or participant
- If I use an acronym or mention a concept you don't understand:
 - Tweet me (*# or @ me*)
 - Heckle. Yell out "ELABORATE" or "EXPLAIN YOURSELF"

#SecuringSMB

Goals

- If you're at an SMB
 - Give you a starting point
 - Give you tools to convince management
- Everyone else
 - Convince you that SMBs are important, and securable

Why?

Why are SMBs Important?

How?

How do we secure SMBs?

#SecuringSMB



Why?

Why are SMBs important?

#SecuringSMB

Too Small to Fail

- 28.8 Million SMBs in the US
- SMBs represent 55% of all jobs in the US
- 65% of spear-phishing attempts are aimed at SMBs
- Target breach was result of a breach of a small HVAC vendor

Then why do we dismiss SMBs when it comes to InfoSec?

#SecuringSMB

How to Get Buy-In

- Regulatory Compliance and a prior breach are the major factors for security spending no matter the business size
- Appeal to owners' self-pride in **their** business, and risk to that pride from a breach
- Introduce Information Security as a sales / marketing tactic

Easier Ship to Turn

- SMBs often have less bureaucracy
- We often have direct access to decision makers, and personal buy-in from management
- Easier experimentation / piloting
- Smaller environment increases the ability to know where everything is and what it does



How?

How do we secure SMBs?

#SecuringSMB

Risk Management

- Risk Assessment and Threat Modeling is even more important in SMBs
- Understand the type of attacks and threats to expect
- Don't attempt to secure the same way a large enterprise would

Threat Modelling

- Know what you're protecting and know what you're protecting against
- Risk Assessment + Business Impact Assessment
 - Estimate what happens to the business if X happens, and the likelihood of X happening
- **Defender's Dilemma** (*traditionally*): An attacker only needs to exploit one weakness, a defender needs to protect all weaknesses
- **Attacker's Dilemma** (*homebrewedsec*): A defender needs to make it too expensive for an attacker to exploit a target given the value of that target

Hardening

- **Principal of Least Privilege:** An account shouldn't be able to access anything that account shouldn't have access to
- **Principal of Least Functionality:** A machine shouldn't be able to do anything that machine shouldn't be able to do
- Encrypt all the things & Patch all the things

Open Source Everything

(please don't)

- Consider your resources
- Do you really have time to manage Open Source software?
- You *might* not need a multimillion \$ SIEM
- Consider what resources and scenarios need to be monitored

#SecuringSMB

Transition Plan

- “Outgoing-sider threat”
- Maintain lists of passwords, accounts, keys, certificates, etc. distributed to who (especially IT and InfoSec)
- Higher priority in SMBs, as insider knowledge is consolidated
- Ensure CFAA warning is in exit interview / termination process

Backups!!!!!!!

- Backup your data
- Check your backup
- Test your backup
- Alert on your backup
- Check your alerts
- Resolve your alerts

tl;dr

- SMBs *are* important
- SMBs *are* targeted
- SMBs *are* similar in a lot of ways to enterprises
- Backup. Backup. Backup.
- Need to apply resource and risk assessment techniques even moreso than in enterprise environments

Appendix: Resources

- Background Image
 - <https://unsplash.com/photos/Z2EgLCJob40>
- Verizon 2018 DBIR
 - https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report_execsummary.pdf

too
small
to
fail

Securing Small and Medium Businesses

Slides

homebrewedsec.com/talks/

Questions

@HomeBrewedSec

#SecuringSMB