Ransomware-Proofing

May 21, 2021

LouMUG

About the Presenters

Rance Reinhardt

Mirazon

Communications for 5 years in the US Army

Network engineer with Mirazon for 6 years

Currently FortiNet, Ruckus, CWNA, MS Certified

Previously Cisco, CompTIA Certified

Previously DoD 8570.01-M IAM Level II

Kyle Haas

Mirazon

Systems engineer with Mirazon for 3 years

A+, Net+, MS-100

Let’s Get Started

Think about security within your IT realm in terms of layers:

- The Human Layer
- Hardware
- Software
- Network
- Response
- Recovery

How strong are you at each layer?

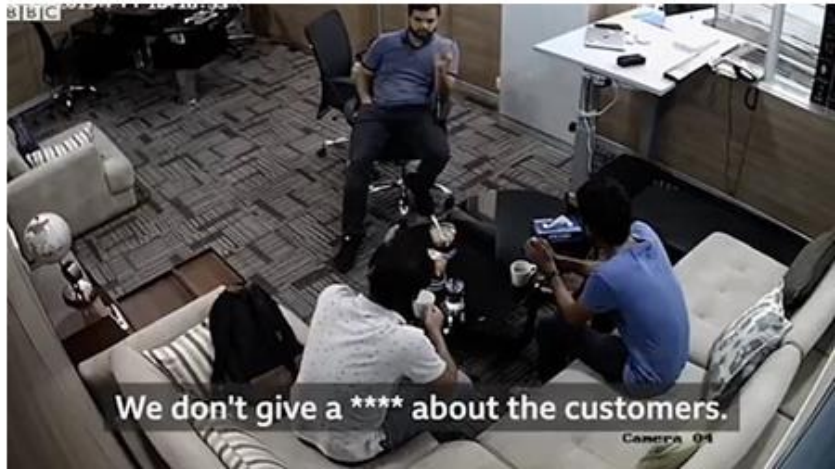
Do you have any significant weaknesses at any layer?

Introduction to Intrusion Methods

- What organizations are attacking you?
- What methods are being used to gain access?
- What are they targeting?
- What do you do about it?

Introduction to Intrusion Methods

- What organizations are attacking you?



The only safe computer in the known universe.

Introduction to Intrusion Methods

- What methods are being used to gain access?
  - The fancy hacker stuff.
    - Active Directory Enumeration
    - Man-In-The-Middle Attacks
    - Scams
  - Malware and Exploits
    - Unpatched firmware and software issues.
    - Software that creates a vulnerability.
  - Phishing
    - User training and policies – MFA!
    - Email filtering products.
  - Dark Web Information Brokers
    - Credentials compiled from leaks, previous hacks, etc.

Introduction to Intrusion Methods

- What are they targeting?
- Every person is vulnerable to being targeted.
- Published services to the internet.
- VPN access and remote connectivity.
- Email (Cloud and On-Prem)
  - Server vulnerabilities
- BACKUPS!

Introduction to Intrusion Methods

- What people are they targeting?

Most-Used Themes

1. New Microsoft Teams request
2. Coronavirus advisory alert and health warning
3. Office 365 password expiration notice
4. Deactivation of old OneDrive account
5. OneDrive shared contract notification
6. Starbucks bonus
7. World Health Organization coronavirus safety information
8. New voicemail message alert
9. Alert about large number of files deleted from OneDrive.
10. UPS shipping notice

Trickiest Themes

1. Free month of Netflix streaming for employees
2. Vacation contract rental
3. Starbucks pumpkin spice season
4. 2020 Summer Olympics advanced ticket sales
5. Overdue invoice reminder
6. Spotify password update prompt
7. Promissory note
8. Dress code violation
9. Coronavirus mask availability and payment plans for business.
10. Notice of moving violation

Introduction to Intrusion Methods

Why do users and even IT professionals fall victim?

- The attackers are organized.
- The attackers know our routines.
- The attackers know our products.
- The attackers operate much in the same way you do.

Introduction to Intrusion Methods

Remember the "Human Layer?"

- Educate your co-workers.
  - Show them how to identify spoofed email and scams.
- Be an advocate for secure policies.
  - MFA, complex passwords, etc.
- As an IT Admin, do not make your own life convenient at the expense of security. What happens if ***your*** credentials are stolen?

Hardening Systems

- Antivirus
- DNS Filtering
- Monitoring and Device Management
- Multi-Factor Authentication (MFA)
- Password Management Tools and Password Policy
- Email Filtering Services and Group Policy

Hardening Systems

- Antivirus
  - Definition Vs. Behavior-based Heuristics
  - Ransomware Variants

- DNS Filtering
  - Virtual/Hardware Appliances
    - WebTitan / Pi-Hole
  - Public DNS Servers with Filtering
    - Quad9 (9.9.9.9) / CloudFlare (1.1.1.2/1.1.1.3)

Hardening Systems

- Monitoring Endpoints
  - Cloud-Connected AV with Alerts
  - Endpoint Detection and Response (EDR)
  - Network Monitoring tools that integrate with other products

- Device Management – Staying Organized and Updated
  - Inventory Management
  - WSUS
  - O365 Device Policies – Conditional Access, etc.

Hardening Systems

- Multi-Factor Authentication - MFA
  - *Millions* of password-based attacks per day on Office365.
    - Microsoft says that a second authentication factor stops 99% of them.
  - MFA is not just for email and financial accounts! Fortitoken, etc.
  - Azure AD MFA

- Password Management Tools
  - LastPass, KeePass, etc.
  - Check your accounts on haveibeenpwned.com
  - https://www.security.org/how-secure-is-my-password/

Hardening Systems

- Email Filtering Services
  - Proofpoint, etc.
  - Exchange/Outlook Filters and Rules

- Group Policy and User Access
  - Password Policies
  - Script/Executable Policies (.vbs, .wsf, .exe)
  - Windows Firewall (WMI, RDP, etc.)
  - Limiting Logons (Log On To… In AD)
  - Clean up your security groups and permissions
  - Controlled Folder Access / OneDrive Redirection

Hardening Backups

- Veeam Backups
- Local Server Access Only (No Domain)
- Local Firewall
- Creating an Air Gap

Hardening Backups

- Why Veeam Backups?
  - Quick Differentials (Block-Level Tracking and Dedupe)
  - Simple restores – Baremetal OR Virtual
  - Supports essentially any backup target
  - Can be isolated without losing functionality
  - Health checks and alerts
  - Don't forget to backup your cloud data!

- Free trials are available… Do yourself a favor and try Veeam.

Hardening Backups

- Local Server Access Only
  - Disable/rename local admin or use unique local admin.
  - Do NOT join the backup server to your domain.
  - Do NOT allow or enable RDP.

- Local Firewall
  - Disable RDP, ICMP, etc. but open ports for Veeam. See full guide in link below.

More Info here!

Hardening Backups

- Air Gap
  - To make a logical barrier to your backup appliance.
    - Network Segmentation, etc.
  - Have a physical gap between you and copies of your backups.
    - Cloud repository
    - Cloud VM
    - Tape or External NAS/Storage location
  - If nothing else… Rotate some external USB drives--But be vigilant!

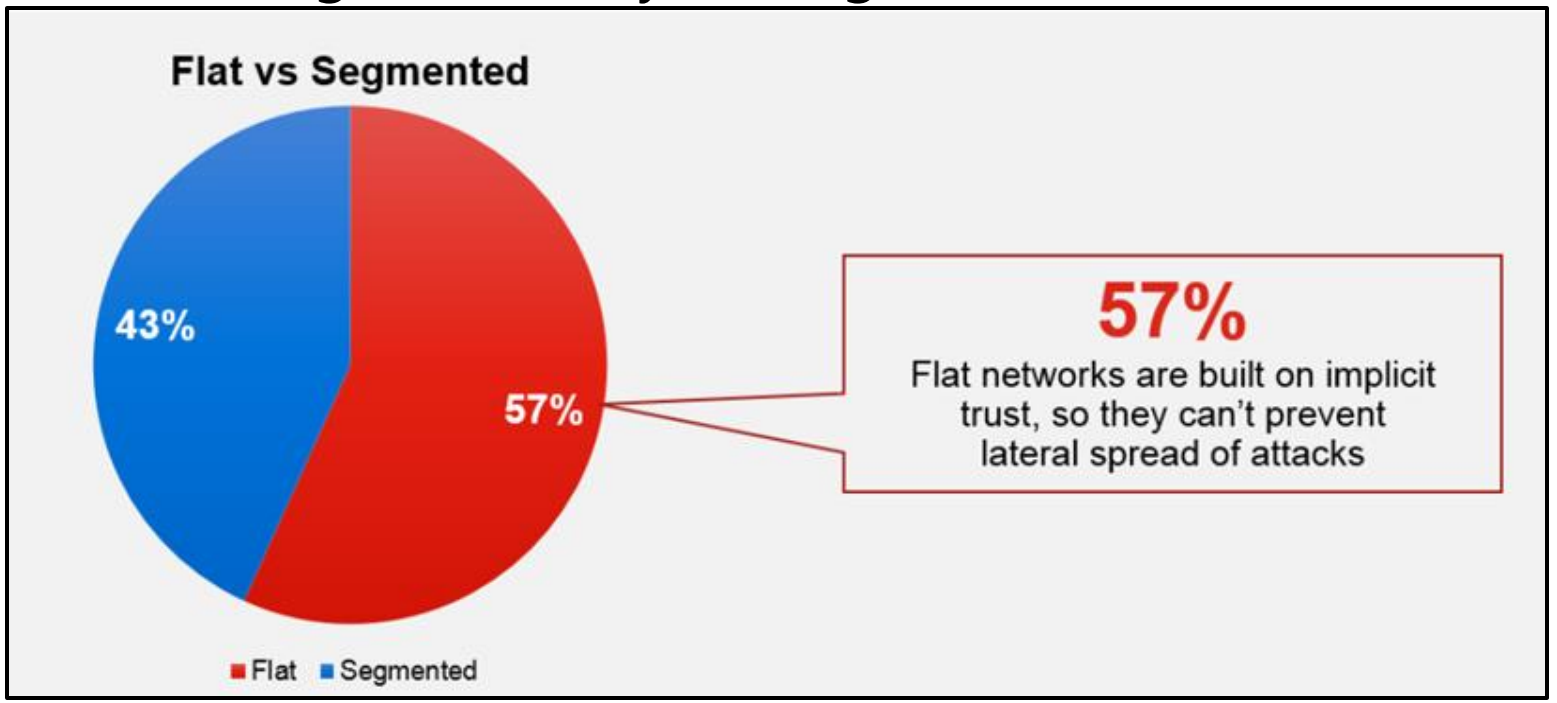
Hardening Networking

- Network Segmentation
- Only allow inbound services that are required.
- Only allow remote connectivity through an encrypted VPN.
  NO 3389 PORT FORWARDING!
- Network Access Control (NAC) and Behavior Monitoring

Hardening Networking

- Network Segmentation

Flat networks are bad.
Segmentation is good.
Regardless of your organization's size.



Hardening Networking

- Network Segmentation
  - Each type of device should be in its' own network.
    - VLANs are your friend.
    - Separates attack surfaces
    - Allows you to narrow internal services and mitigate intrusion spread.
  - Route your traffic through a "next generation" firewall.
    - Use a firewall as your organization's routing core.
    - Inspect traffic that passes between VLANs and run security profiles against it.
    - Allows for faster response in the event of an intrusion.
  - Air Gap your backups!
    - Narrow all traffic to only the services that move the backups.
    - Have only a single off net machine on a specific network that is used for backup management.
    - Use schedules to narrow the attack vector even more.

Hardening Networking

- Only allow inbound services that are required.
  - Narrow outbound services for:
    - Server infrastructure
      - Domain Controllers
      - Application Servers
      - Published Services
    - Vulnerable endpoints.
      - Legacy OSs
      - IoT
      - Manufacturing Controllers
    - Everyone?

Hardening Networking

- Only allow remote connectivity through an encrypted VPN.
  - NO 3389 PORT FORWARDING!
  - Full Tunnel or Split Tunnel?
  - IPSec or SSL?
  - Multifactor, Multifactor, Multifactor
  - VPN Management and Endpoint Compliance

Hardening Networking

- Network Access Control (NAC) and Behavior Monitoring
  - CyberHawk
  - FortiNAC
  - Impulse
- Onboarding, Authentication, and Wireless
  - CloudPath
  - RADIUS
  - Mobile Device Management (MDM)
  - Azure AD

Additional Resources

Jim Browning 4 part scam call center full take over.

https://www.youtube.com/watch?v=Ie71yVPh4uk

BBC Clip covering the above.

https://youtu.be/7rmvhwwiQAY?t=215

A bit of fun. (ScamBaiters)

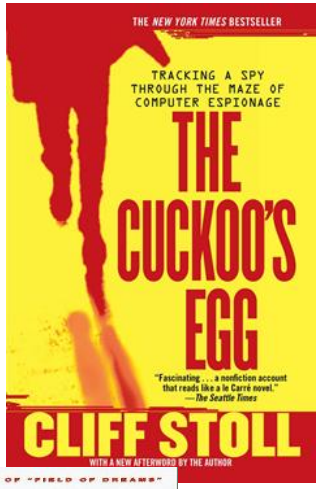
https://youtu.be/UmEKhOEnmpg?t=2110

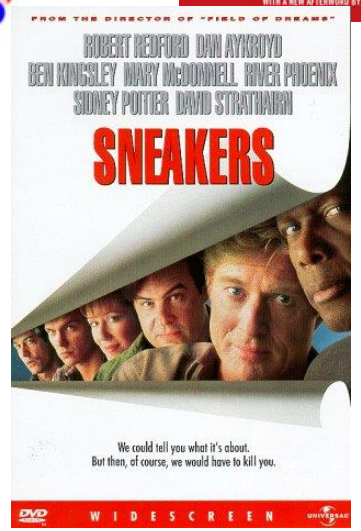
Sneakers Keypad Scene

https://www.youtube.com/watch?v=oG5vsPJ5Tos&t=11s

NCIS Not Hacking

https://www.youtube.com/watch?v=msX4oAXpvUE





Thanks! Q&A

Rance.Reinhardt@mirazon.com Kyle.Haas@mirazon.com

LouMUG