LEVEL UP

Chad Jackson

# How to be Secure

Cybersecurity

1

## Disclaimer

A Few Things First

**This presentation is for information only.**
Evaluate risks before acting based on ideas from this presentation.

**This presentation contains opinions of the presenters.**
Opinions may not reflect the opinions of Tandem.

**This presentation is proprietary.**
Unauthorized release of this information is prohibited.


2

# Chad Jackson

Technology Consultant
CoNetrix Technology

3

## Who Am I?

**...and why should you listen to me?**

- Texas Born and Raised
- Married with 3 Kids
- IT Professional for 11+ Years
  - With CoNetrix for ~8 years

4

# I have a passion for network and data security.

5

# I believe Data Privacy is a human right.

6

# As IT professionals, it is our job to ensure our customers' data remains private and secure.

7

## The problem is…

**Cyber Attack Statistics**

The ten ***most common*** types of cyber attacks:

1. Malware
2. Denial-of-Service (DoS)
3. Phishing
4. Spoofing
5. Identify-Based Attacks
6. Code Injection
7. Identity Based Attacks
8. Insider Threats
9. DNS Tunneling
10. IoT-Based Attacks

*https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/*

8

# The problem is…

**Cyber Attack Statistics**

Seventeen ***most common*** types of cyber attacks:

11. SQL Injection
12. Zero-Day Exploits
13. Password Compromise
14. Drive-by Download
15. Cross-site Scripting
16. Rootkits
17. Cryptojacking

*https://www.aura.com/learn/types-of-cyber-attacks*

9

# The problem is…

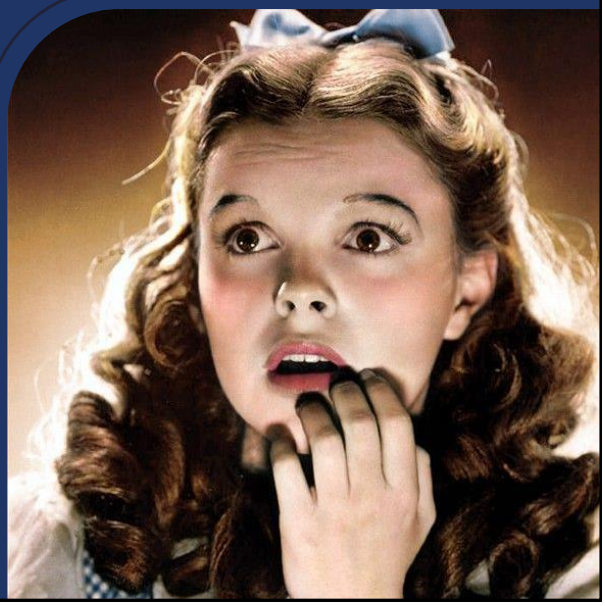
**Cyber Attack Statistics**

- "Average weekly cyber attacks per organization increased by 38% in 2022."
- "USA saw a 57% increase in overall cyber attacks in 2022…"
  - Finance/Banking saw a 52% increase

*https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks*

10

# Phishing & Ransomware & Lateral Movement Attacks… Oh my!



11

# How can you achieve bulletproof network security?

…you can’t.

12

# Questions?

13


14



15

What do Ogres, Onions, and Network Security have in common?

# Network Security is like an onion: it has layers!

16

LEVEL UP

Chad Jackson

# The Layered Approach to Network Security

Cybersecurity

17

## Agenda

**Here's the Plan**

- Identify Network Attack Surfaces
- Discuss Vulnerabilities
- Explore Solutions

18

# Attack Surfaces

1 Edge/Border

Servers 2

3 Workstations/Endpoints

Email 4

5 People

19

# Attack Surfaces

**And how to protect them…**

1

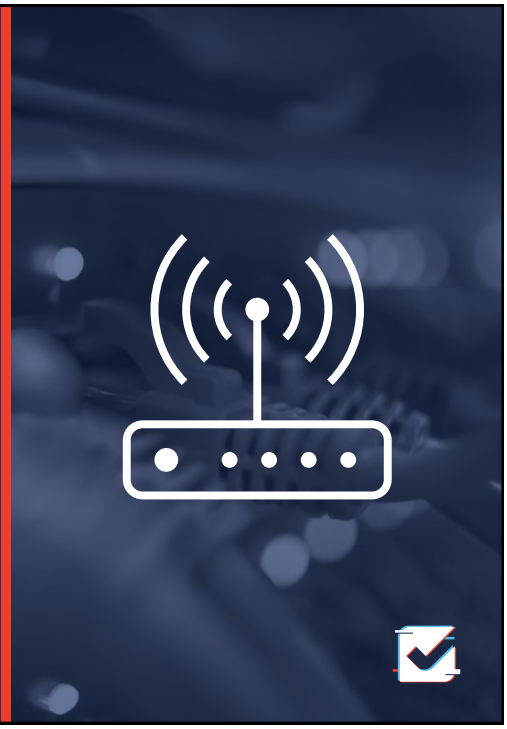
## Edge/ Border

20

# Edge/Border

**What is it/where is it?**

- The edge, or border of your network/domain.
- The device your internet plugs into:
  - Firewall
  - UTM Device
  - Router
- Remote offices (more on this later…)



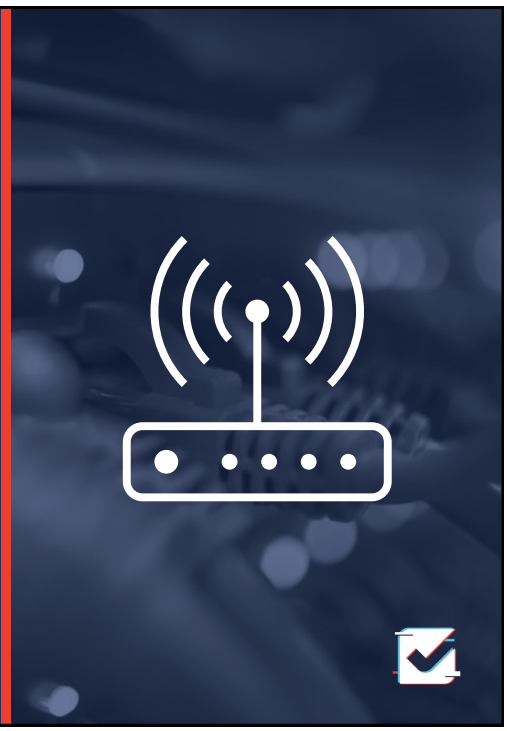
21

# Edge/Border

**Vulnerabilities**

A few examples:

- DoS Attacks
- Outdated firmware/software
- Zero-day/Emerging Threats
- Insider Threats



22

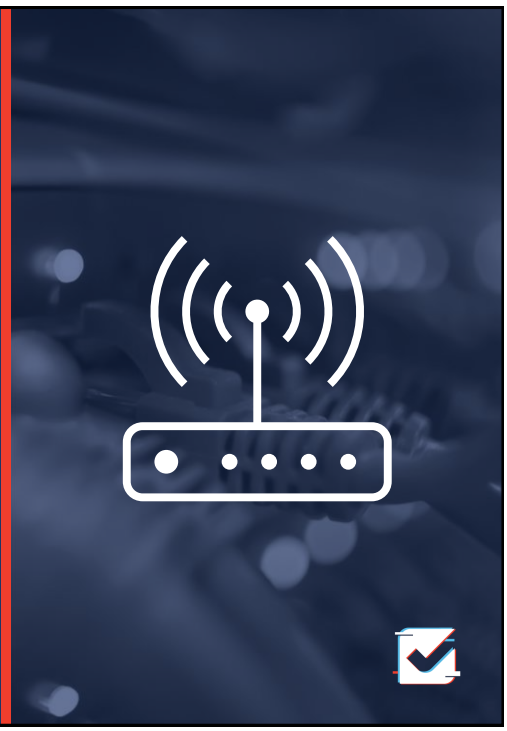
# A router with an access list is not adequate protection.

23

## Edge/Border

**Solutions**

- Unified Threat Management (UTM)/ Next-Gen Firewall (NGFW)
  - Firewall
  - Web Filter
  - IDS/IPS
  - SSL/SSH Inspection
  - Deep Packet Inspection
  - Malware Detection
- Multi-Factor Authentication (MFA) for logins.
- Log Auditing (SIEM/SOC)
  - Integration with Threat Intelligence Services.



24

# Attack Surfaces

**And how to protect them…**

**2**

## Servers

25

# Servers

**What is it/where is it?**

- The castle keep/the engine room.
- Types of servers:
  - Domain Controller
  - File Server
  - Application Server
  - Print Server
  - Web Server

26

# Servers

**Vulnerabilities**

A few examples:

- Ransomware
- Lateral Movement Attacks
- Zero-Day
- SQL Injection
- Insider Threats

27

# Servers

**Solutions**

- Antivirus with Endpoint Detection & Response (EDR)
  - MDR = Managed Detection and Response
  - XDR = EDR + SIEM/SOC (basically)
- Server Hardening
  - Simplified, secure configurations
  - Access Reviews
- Patch Management
- MFA for Logons
- Log Auditing (SIEM/SOC)
- Network Segmentation (vLAN)

28

# Attack Surfaces

**And how to protect them…**

**3**

## Workstations / Endpoints

29

# Workstations/Endpoints

**What is it/where is it?**

- The lobby floor
- The executive suites
- Airports
- Conferences/trade-shows
- Starbucks
- …everywhere

30

Vulnerabilities

## Workstations are the most numerous type of device on your network; therefore, this is your most vulnerable attack surface.

31

## Workstations/Endpoints

Vulnerabilities

A few examples:

- Phishing
- Malware/Ransomware
- Lateral Movement Attacks
- Out of date/unused software
- Malicious USB Devices
- Snooping
- Loss/Theft

32

# Workstations/Endpoints

**Solutions**

- Antivirus with Endpoint Detection & Response (EDR)
- Access Reviews
  - Eliminate Local Admin Privileges
- Patch Management
- Network Segmentation (vLAN)
- VPN Connections when Remote
- USB Device Control
- Disk Encryption*
- MFA for Logons*

33

# Attack Surfaces

**And how to protect them…**

**4**

**Email**

34

# Email

**What is it/where is it?**

- Servers:
  - On-premise
  - In the cloud – ex: Microsoft 365
- Clients:
  - Workstations/endpoints
  - Mobile devices
  - …Starbucks

35

# Email

**Vulnerabilities**

A few examples:

- Phishing (all forms)
- Malware/Ransomware
- Insider Threats
- Salespeople

36

# Email

**Solutions**

- Content Filter
- Encryption
- Data Loss Prevention (DLP)
- Mobile Application Management (MAM)
- MFA for Logons
  - Cybersecurity Insurance Requirement
- Social Engineering/
  Security Awareness Training

37

# Attack Surfaces

**And how to protect them…**

**5**

**People**

38

# People

**What is it/where is it?**

- The lobby floor
- The executive suites
- Sporting events
- Concerts
- Cabo
- Starbucks!

39

# People

**Vulnerabilities**

- Phishing
- Insider Threats
- Identity-Based Attacks
- Password Compromise

40

# People

**Solutions**

- Password Hygiene
- MFA
- Access Reviews
- Social Engineering/ Security Awareness Training

41

**A quick comment from Allen Iverson:**

# “We talking ‘bout [Security Awareness Training]???”

42



43

What do Ogres, Onions, and Network Security have in common?

# Network Security is like an onion: it has layers!

44

# Recap

**Attack Surfaces**

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Border/ Edge | Servers | Workstations / Endpoints | Email | People |

45

# Network Security is best accomplished through a layered approach.

46

LEVEL UP

Chad Jackson

# How to be Secure

Cybersecurity

47