SANS | CYBERSECURITY LEADERSHIP

The SANS Institute

Crucial Cyber Hygiene Defenses for 2023

Why is this a presentation in 2023?

- Organizations still are not consistently implementing basic defenses

- Researchers want to debate sexy topics:
  - Artificial Intelligence / ChatGPT
  - Threat Actor Attribution / Emulation
  - Objective / Quantitative Risk Models

- The cybersecurity industry has a core incentive / motivation problem

- Attendees need a clear strategy for defense that actually stops attacks

What Threats is This Based Upon?

- We're assuming the goal is to prevent loss of C-I-A
- We're assuming organizations are not special snowflakes
- The research presented in here is the cumulative result of feedback provided by:
  - The Verizon Data Breach Report
  - Multiple Vendor Threat Reports
  - The Collective Threat Taxonomy
  - MITRE ATT&CK
  - Feedback from Pen Testers & Incident Response Teams

Specific Threats We Are Addressing in 2023

- Lack of Operational Awareness (Inventory)
- Email Phishing
- Credential Theft from Endpoints
- Credential Re-Use / Credential Spraying
- Lateral Movement from Endpoints
- Application Abuse Due to Component Vulnerabilities
- Application Abuse Due to Coding Vulnerabilities

Who Says This is True?

Cybersecurity Hygiene Guides

- UK GCHQ
- Australian Cyber Security Centre
- Canadian Centre for Cybersecurity
- US National Security Agency
- The SANS Institute
- Collective Risk Project
- Center for Internet Security

Regulators / Standards Bodies

- National Institute for Standards in Technology (NIST)
- International Organization for Standardization (ISO)
- Cybersecurity & Infrastructure Security Agency (CISA)
- PCI, FFIEC, NERC, FCA, CMS…
- So many more…

Cyber Hygiene vs Legislative / Insurance Models

- Cybersecurity Hygiene Models ≠ Legislative or Insurance Models

- **Cybersecurity Hygiene Models** =

  Defensive controls meant to ensure business goals are achieved.

- **Legislative / Insurance Models** =

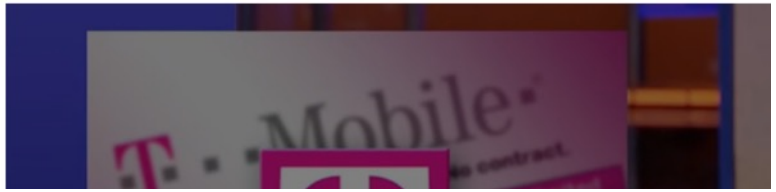
  Defensive controls meant to show an organization has implemented enough defenses to show they are not negligent

- Different standards are written for different reasons, know the difference when choosing which to implement

T-Mobile breached by hacker customers impacted

The company went through extensive cybersecurity m

By Luke Barr
January 20, 2023, 3:57 AM



Twitter hacked, 200 million user email addresses leaked, researcher says

By Raphael Satter

Atlassian and Envoy briefly blame each other for data breach

Carly Page, Zack Whittaker / 6:50 AM CST • February 17, 2023

December 22, 2022 | By Karim Toubba

Notice of Recent Security Incident

Update as of Thursday, December 22, 2022

To Our LastPass Community,

We recently notified you that an unauthorized party gained access to a third-party cloud-based storage service, which LastPass uses to store archived backups of our production data. In keeping with our commitment to transparency, we want to provide you with an update regarding our ongoing investigation.

Endpoint / Server Safeguards

2022 Common Wisdom:

- Asset Inventory
- OS Patch Management
- Vulnerability Scanning

2023 Cyber Hygiene:

- Application Control
- Multi-Factor Authentication
- Third-Party Patch Management
- Vulnerability Remediation

Network Safeguards

2022 Common Wisdom:

- Perimeter Firewalls
- Remote VPN Access for Management
- VLANs for Performance

2023 Cyber Hygiene:

- Host Based Firewalls
- Host Based Agents for Management
- Campus Networks are ISPs
- VLANs for Access Control
- Campus Network VLAN Privatization

SaaS / Cloud Safeguards

2022 Common Wisdom:

- Cloud App Inventory
- Cloud Access Security Brokers

2023 Cyber Hygiene:

- Multi-Factor Authentication
- Cloud Service Provider Account Inventory
- Cloud Service Provider Configuration Management
- SaaS / Cloud Logging

DevOps Safeguards

2023 Cyber Hygiene:

- Cloud First Architectures
- Software Bill of Materials (SBOM)
- Code Scanning in CI/CD Pipelines
- SLAs for Vulnerability Remediation

What Defenses Were Left Out (on Purpose)?

- Eventually there are other defenses to consider, but not today

- There are a number of defenses we left out, on purpose:
  - Automated threat emulation
  - Adversary deception technologies
  - Data loss prevention
  - Internet of Things
  - Passwordless authentication

Cybersecurity Hygiene – A Sustainable Plan

- Once you have the basics in place, there are other cybersecurity standards to consider that will give a broader perspective

- Other standards to consider include:
  - Collective Controls Catalog
  - NIST 800-171 / 172
  - NIST Cybersecurity Framework
  - ISO 27002:2022
  - Center for Internet Security Controls

SANS | CYBERSECURITY LEADERSHIP

General inquiries: info@sans.org
Registration: registration @sans.org
Tuition: tuition@sans.org
Press: press@sans.org
(301) 654 – SANS (7267)

Contacts and Resources

AUTHOR

James Tarala

James.tarala@enclavesecurity.com

@isaudit

SANS Leadership Resources

https://www.sans.org/cybersecurity-leadership/

@secleadership