Infinite Improbability

Plan for the Worst
and
Prepare for the Unknown

AVERTIUM

Infinite Improbabilities… Finite Probabilities…

Conversation Topics

- Understanding Knowns/Unknowns
- Plan for the worst and try to Prepare for everything else
- The Holistic Approach
- Weaving Security into Culture
- Getting that ever-elusive “Buy-In”

AVERTIUM

It’s important to know what you know…

Things we should know…

- Published Vulnerabilities
- Common Vulnerabilities and Exposures (CVEs)
- Publicized Threats
- Classic Security Concepts
- Tested Security Frameworks
- The occasionally paranoid (but correct) Security Professional

Things we often think we know…

- Day 0 Vulnerabilities
- Interaction Vulnerabilities
- Stealth Threats in the Wild
- Classic Security vs. Bleeding Edge Technology
- Buzz Words… AI, Machine Learning, Containerization, IoT, Quantum Computing…

And more important to know what you don’t!

AVERTIUM

A little explanation…

Most of us know basic security principles and "good" security practices.

- Passwords (bear with me)
- Knowledge Sharing/Training
- Compartmentalization
- Principle of Least Privilege (PoLP)
- NIST, CIS CSC 20, OWASP, STIG, ISO/IEC, NERC, DoCRA, IASME, Cobit, ASD, NZISM, PCI-DSS…

But many of us don't really understand the impact of changing technology.

- Cloud-Based Services
- Intelligence-driven programs
- Cross-bred architectures
- Complacency
- My house knows everything about me… then talks to my phone behind my back.

Any fool can know. The point is to understand. ~Albert Einstein

Plan for the worst…

Ensure we utilize well established Security Concepts

- Layered Security
- System Hardening
- Secure Coding Practices
- Backups… Backups… Backups…

  (a hard drive hidden at your house doesn't count)
- Principle of Least Privilege
- Encryption
- Pass Phrases (not passwords…)
- Multifactor Authentication

  (This doesn't include captchas and honestly… not security questions)

It may not be cool, but how often do we fail to use many of these?

AVERTIUM

Try and Prepare for Unknowns.

Think outside the box, be creative, and challenge paradigms:

- Dynamic Training (role-specific)
  - Administrative
  - Compliance
  - Technical
- Understand New technologies
  - Software Defined Architecture
  - Cloud Based Services
  - Quantum Computing
  - Blockchain
  - Containers
- Cross-Discipline Positioning
- Programmers/Security
  - Devs/Sysadmins

AVERTIUM

A “Holistic” Approach to Security

ho·lis·tic

/hōˈlistik/

adjective

Characterized by comprehension of the parts of something as intimately interconnected and explicable only by reference to the whole.

AVERTIUM

A “Holistic” Approach to Security

Security isn’t just software and hardware.

- People
- Lifestyle
- Culture
- Perception
- A different way of thinking…

AVERTIUM

Security shouldn’t be an afterthought or chore

- Make Security Fun (I know making things fun is a trope…)
  - No “Death by PowerPoint”
  - Use Games
  - Create Incentives
  - Applaud wins… Use losses as learning points, not career enders.
- Everyone is in charge of Security (not one unlucky person).
- Security should improve Productivity not impede it.
- Make it real… Not just something you have to do at work.

AVERTIUM

That's great but… How do I convince my boss?

- **Security Metrics aren't just good for Monitoring.**
  - Metrics can provide valuable insight to prioritizing tasks, monitoring productivity, and minimizing resource waste.
  - (This means you can make more money)
- **Security Tools aren't just good for Protection and Detection.**
  - Tools can do many other tasks like traffic shaping for network resources, prioritizing applications, and minimizing resource hungry services.
  - (This means you can make more money)
- **Security Training isn't just good for the Company.**
  - Training can also help employees in their personal life. This can reduce stress, improve quality of life, and thus make the employ more productive.
  - (This means you can make more money)

AVERTIUM

If that doesn't work… Hit 'em with the mad math skills.

- Stop thinking ROI and start thinking ALE (mmmmmmm… Ale)
  - Annualized loss expectancy – Calculate the cost of a security incident in both tangibles (time & money), and intangibles (reputation & competitive advantage).
  - ALE = (Number of incidents per year) x (Potential Loss per Incident)

- Add in The Exposure Factor (EF) and Single Loss Expectancy (SLE)
  - EF= (The profit an asset provides) x (The amount of time that asset is unavailable)
  - SLE= EF x (Asset Value)

- Incidents can also be referred to as Annualized Rate of Occurrence (ARO)
  - Soooooo… SLE x ARO = ALE (I say again, mmmmmm… Ale)

AVERTIUM