



CyberSecurity Webcademy:
Securing Your Environment

Agenda



Introductions



Summary of Session 1: The Basics



Keeping Cybercriminals Out

Presenters



Justin Krentz – Account
Executive in Pennsylvania



Tyler Lewan – Account
Executive in Colorado

Summary of Session #1: The Basics

- Security Assessment**
- Staff**
- Spam Email**
- Passwords**



Risk #1: Holey Moley You Need to Patch



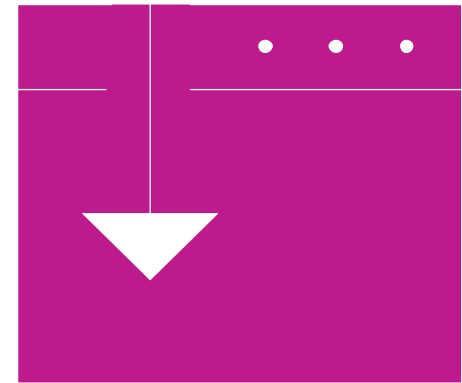
Ignoring update notifications

- Puts your device and your company's data at risk
- Constant new ways of compromising security
- Operating on legacy platforms

Prevention #1: Computer Updates

Keep Microsoft products updated

- Sooner you update - sooner your more secure
- Look for a “critical update” service



Advantages #1: Computer Updates

- Repairs newly discovered security holes
- Add new features
- Help protect your data



Risk #2: Fire in the Hole



- Threats to personal devices and networks are changing every day
- Traditional firewalls are static
- Left vulnerable by outdated security technology

Prevention #2: Next Generation Firewall

Includes standard firewall capabilities PLUS

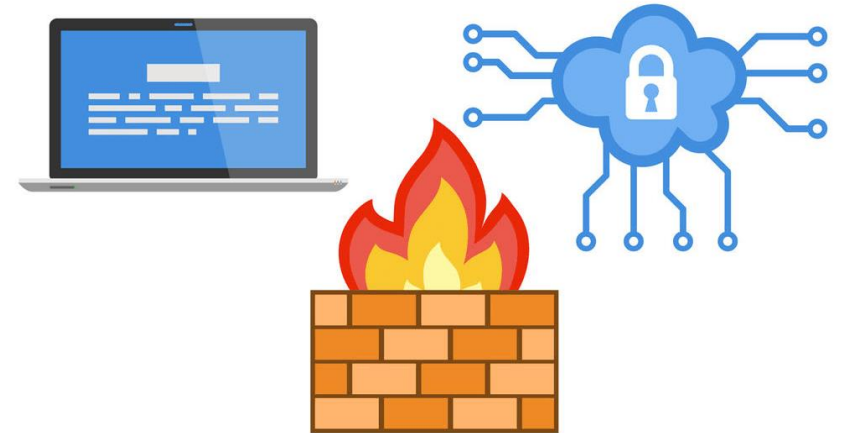
- Integrated intrusion prevention
- Application awareness and control
- Threat intelligence sources
- Upgrade paths
- Address evolving security threats



Advantages #2: Firewalls

- Can be a low-cost option
- Protects from a broader range of threats
- Automation and product integrations*

* will address this later in session



Risk #3: “Ghosts” in the Machines”



- More working from home means more laptops
- Sensitive files open to every employee
- Files can easily be stolen
- Can be sued if PII is leaked or shared

Source: varonis.com/2019-data-risk-report

Prevention #3: Encryption

- Encrypt files at rest and in motion
- Cloud encryption keeps sensitive data in a read-only
- Automatic email systems or included in Office 365



Advantages #3 - Encryption

Cybercriminal gets through

- Your firewall
- Your laptop is stolen
- Password guessed

Your data will still be protected



Vertical  Solutions

Risk #4: Who's Knocking at Your Backdoor?

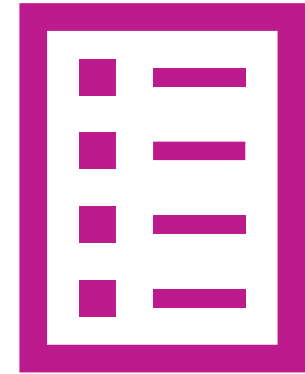


How fast can you detect?

- Layered security means more systems
- Impossible to monitor and analyze all logs
- Many alerts go completely uninvestigated

Prevention #4: Log Management

- SIEN -uses big data engines to review **all** event and security logs from **all** covered devices
- Looks at network behavior as well as user behavior
- Tracks and investigates what's happened
- Clear picture of potential cybersecurity issues across the entire network



Advantages #4: Log Management


- Detection of unnoticed incidents
- Monitoring and reporting necessary to meet mandates
- More intelligence around malicious activity



- 9/30 - Making it Harder for CyberCriminals
- 10/ 7 - Being Prepared for an Incident

Cyber Attack!

16 Ways to Protect Your Business From a

| | | |
|---|--|--|
|  <p>Security Assessment It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?</p> |  <p>Security Awareness Train your users- often! Teach them about data security, email attacks, and your policies and procedures.</p> |  <p>Spam Email Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks.</p> |
|  <p>Passwords Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, or set user screen timeouts.</p> |  <p>Computer Updates Keep Microsoft products updated for better security. Look for a "critical update" service via automation to protect from attacks.</p> |  <p>Log Management SIEM, Security Incident & Event Management uses big data engines to review all event and security logs from all covered devices.</p> |
|  <p>Firewall Turn on intrusion detection and intrusion prevention features. Send the log files to a managed SIEM.</p> |  <p>Encryption Whenever possible, the goal is to encrypt files at rest, in motion, and especially on laptops.</p> |  <p>Advanced Endpoint Detection Protects your computers data from malware, viruses, and cyber attacks through fileless and script based threats.</p> |
|  <p>Multi-Factor Authentication Adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.</p> |  <p>Web Gateway Security Network security is a race against time. Cloud based security detects web and web threats as they emerge, and blocks them on your network within seconds.</p> |  <p>Dark Web Research Knowing in real time what passwords, accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.</p> |
|  <p>Security Expertise Work with IT professionals who understand the framework for managing today's security threats.</p> |  <p>Backup Backup local and to the cloud. Have an offline backup for each month of the year. Test your backups often.</p> |  <p>Response Plan Having a well prepared incident response plan to follow ensures that you can respond quickly.</p> |
|  <p>Cyber Insurance If all else fails protect your practice with cyber damage and recovery policies.</p> | | |

Thank you!

Justin Krentz:

Jkrentz@verticalsol.com

724-493-0933

Tyler Lewan:

tlewan@verticalsol.com

847-987-9606



Vertical  **Solutions**
an R.L. Nelson & Associates Company