Securing the Enterprise

Cyber Security Myths& Reality

"What cyber criminals are planning for 2019
(plus 5 crime-stopping essentials)"

BELARC

Topics

- Example breach
  - US Office of Personnel Management (OPM)
- Some cyber security myths, and the reality
- Recommendation and Way Forward

Belarc company

- Over 1,700 customers world wide
  - AIG Asia, Catholic Relief, Federal Aviation Administration, NASA, Travelers India, US Air Force, US Army, US BLM, US Navy
  - Many long term >10 years
  - Located in 42 countries
- Eight US and Worldwide Patents
- Proven technology and products
  - 20 years, certified on US DoD networks: NIPRNet, SIPRNet, JWICS

Example breach - US OPM

- US OPM – US Office of Personnel Management
- Impact
  - 20 million security clearance records leaked
  - 4 million personnel records
  - 5 million fingerprint records
  - US personnel were withdrawn from foreign stations

Example breach – US OPM

- How did it happen?
  - Attackers used known vulnerabilities
    - End user devices and contractor web server
  - Elevated privileges and gained access to databases
  - Ex-filtrated data using official appearing domains
    - opmlearning.org and wdc-news-post.com

OPM breach analysis

- Why was this not stopped or detected by Einstein (IDS/IPS)
  - Needed specific malware signature files to detect
  - Traffic from malware was encrypted
  - Domains were not on prohibited list
- Why was this not stopped by endpoint protection?
  - AV signatures did not detect malware
  - Firewalls allowed https (SSL) traffic
- What about encrypting the database?
  - Attackers had authorized user privileges

OPM breach lessons learned

- What would have stopped the breach?
  - Installing software updates on all end-user devices and servers
  - Limiting user privileges
  - Enabling two-factor authentication
- “No US Federal government breach over the past few years has relied on a zero-day exploit” – Curt Dukes, NSA IAD
  - Why are we so focused on stopping zero-days?

Myth: prioritize securing high value assets

- Reality: The initial breach is often on **devices with no direct access** to high value data.
- Attackers **escalate privileges** or find admin accounts to allow access to high value data
- Only patching the high value servers, encrypting data or DLP would have little impact on these attacks.

Myth: latest end point protection (EPP) will stop breaches

- Myth: The latest EPP with behavioral analysis, AI machine learning, and application containment will stop breaches.
- Maybe but this still needs to be proven.
- Reality: Very few breaches use zero-day vulnerabilities.

Myth: IDS/IPS will stop most attacks

- Reality: IDS/IPS is dependent on up to date signatures to ID attacks
- What if the attack uses encryption? Fakes network address?
- Will AI machine learning detect breaches in large networks?

Myth: Focus on critical vulnerabilities

- Reality: Maybe a good place to start, but majority of breaches use non-critical vulnerabilities.
  - Attackers look at CVSS scores too.

Myth: Focus on recent vulnerabilities

- Reality: 92% of vulnerabilities used are > 1 year old
- Median age was 6 years.
  - Based on number of CVEs successfully exploited by date published.
  - 2016 Verizon DBIR

Myth: Why focus on isolated networks

- For example industrial control systems, SIPRNet
- Reality: Often not as isolated as expected
  - SCADA systems, VPN connections, USB storage devices

Myth: End users are the weakest link

- Yes, they click on anything, but it would not matter, if:
  - Their computers were patched and applications updated.
  - They did not have admin privileges.
  - They used two-factor authentication

Belarc Recommendations

- Build cyber security process on proven standards
- Center for Internet Security (CIS) Top 5 controls: (out of 20)
  - Identify authorized and unauthorized **devices**
  - Identify authorized and unauthorized **software**
  - Controlled use of **admin privileges**
  - Continuous **vulnerability assessment** & remediation
  - **Secure configurations** for all devices
- **Top 5 will reduce risk of breach by 85%**
  - All 20 by 94%

Way forward

- First put in place people, process and technology to continuously implement CIS top 5 controls
  - Next CIS top 20 controls
- Later look at new wiz-bang technologies

How Belarc can help

- Continuously, automatically monitor CIS top 5 controls
  - Enterprise wide
  - Single automated system vs. many distributed tools and manual efforts.
  - Allows all required parties to have access to necessary data
- Proven technology with thousands of customers
  - US DoD, Federal Government, Commercial, 42 countries

Contact and Questions?

Contact us for a live demo, in house trial or other information.

Belarc, Inc.
Andrew Ridgers
aridgers@belarc.com,
01749 689213
http://www.belarc.com/CIS