Legal Informatics, Privacy and Cyber Crime

Part 5: Discussion on Policies

Etalle

2018
About this part of the course

• Topic: Problems and countermeasures

• Underlying Material: Book, chapter 8
Chapter 8: Problems and Countermeasures

Wrong myths to be discussed – one by one

• Deployment of Secure Sockets Layer (SSL) prevents you from all types of attacks
• Implementation of firewall as a network perimeter defense makes the environment bulletproof.
• Deployment of an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) protects malicious code from entering my network.
• Custom encryption provides similar strength as standardized cryptographic algorithms.
• Usage of Two-factor Authentication (TFA) protects from all types of fraudulent activities.
• Deployment of security policies eradicates the risks
• Anti-virus (AV) engines provide robust protection.
• Malware is distributed primarily through shady and rogue web sites such as torrents and warez
• Email filtering mechanisms only allow secure and verified attachments to be delivered with emails.
• Malware infections are specific to certain operating systems.
• Mobile devices are completely secure.
• Virtualization technologies are untouched by malware.
Technical Countermeasures: make it Resilient

Strong Response Plan + End System Security = **Resilience**

You need to monitor what you have, and to be able to react. Everything you install has monitoring costs, if you want to keep it secure. Keeping things patched is the least, but it is not sufficient.

Monitor    Respond
User Security (commented book statements)

• “Users should be somewhat paranoid in their surfing habits on the Internet. It is highly advised that users should not click tempting links about which they are not sure of”
  • OK

• Users should practice safe computing principles such as
  • “implementing strong and complex passwords”
    • OK-ish
  • “avoiding usage of same passwords at different web sites”
    • Yes, at least to some extent
  • “changing passwords at regular time intervals”
    • NOOOOOO
Passwords better be usable

- Changing password and special characters mess up with usability
User Security II (commented book statements)

• “Users should use VMs for dedicated surfing or visiting untrusted web sites”
  – A good suggestion, but who is going to do this?
• “Users should not supply their personal and critical information on web sites (Phishing webpages) or to individuals (rogue phone calls) that are not obviously legitimate”
  – Obvious
• “Organizations should provide regular training to users”
  – Obvious, but who does?
• “Users should not use their personal USB devices”
  – Detail….
Network Security (commented book statements)

- Here (like elsewhere) the book is just puts all countermeasures in a list, without ranking them.
- Fact is, countermeasures have (running) costs, and every organization needs to find a suitable cost/benefit
  - “Organization should deploy robust network perimeter security defenses such as IPS and IDS, email filtering solutions, and firewalls to restrict the entry of malicious code in the internal network. Organizations should install robust Domain Name System (DNS)”
    - Banks Have this
  - “Implementation of Honeynet is also an effective strategy to understand the nature of malware”
    - I am not sure I agree. Not even Banks have this (yet), it is coming up, very expensive
Network Security II (commented book statements)

• “Strong traffic monitoring solutions should be deployed on the edges of the networks”
  – Yes, and for critical companies (utilities, manufacturing, smart buildings), etc also **INTERNAL monitoring** should be in place.

• “Security Information and Event Management (SIEM) solutions help administrators detect anomalous events occurring in the network”
  – Having a SIEM is a good idea, if you have the resources for it, it is a heavyweight monitoring solutions. Banks and large enterprises have it. With the SIEM goes also the following

• “Administrators should analyze server logs on a regular basis to find traces of attacks or malicious traffic”
  – Yes
Network security III (commented book statements)

• “Sensitive data flowing to and from the network should be properly encrypted”
  – Agree with the “to and from” the network, inside the network is a different sot

• “Use HTTPS with good certificates”
  – No brainer. Cheap too

• “Enterprise networks should be properly segregated”
  – Very important, and if you ask me first thing to do, together with Setting up good policies
And the administrators should think security

- Administrators should follow the best secure device configuration practices such as configuring strong and complex passwords for network devices such as routers, printers, and switches, using Simple Network Management Protocol (SNMP) strings that cannot be guessed, avoiding the use of clear text protocols, disabling unrequired services, deploying least privilege principles for restricting access to resources, configuring software installation and device change management policy, and out-of-band management features.
QUESTIONS?