csm-ace 2017
9th CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

In conjunction with

nice
NATIONAL INNOVATION AND CREATIVE ECONOMY EXPO'17

#cyberreadiness
Securing Digital Economy

9 – 16 October 2017 | The Royale Chulan Kuala Lumpur

Defense-in Depth

Richard LaMagna CPP CISM

NW3C- LaMagna and Associates, LLC

Rich@lamagnaandassociates.com

10 October 2017

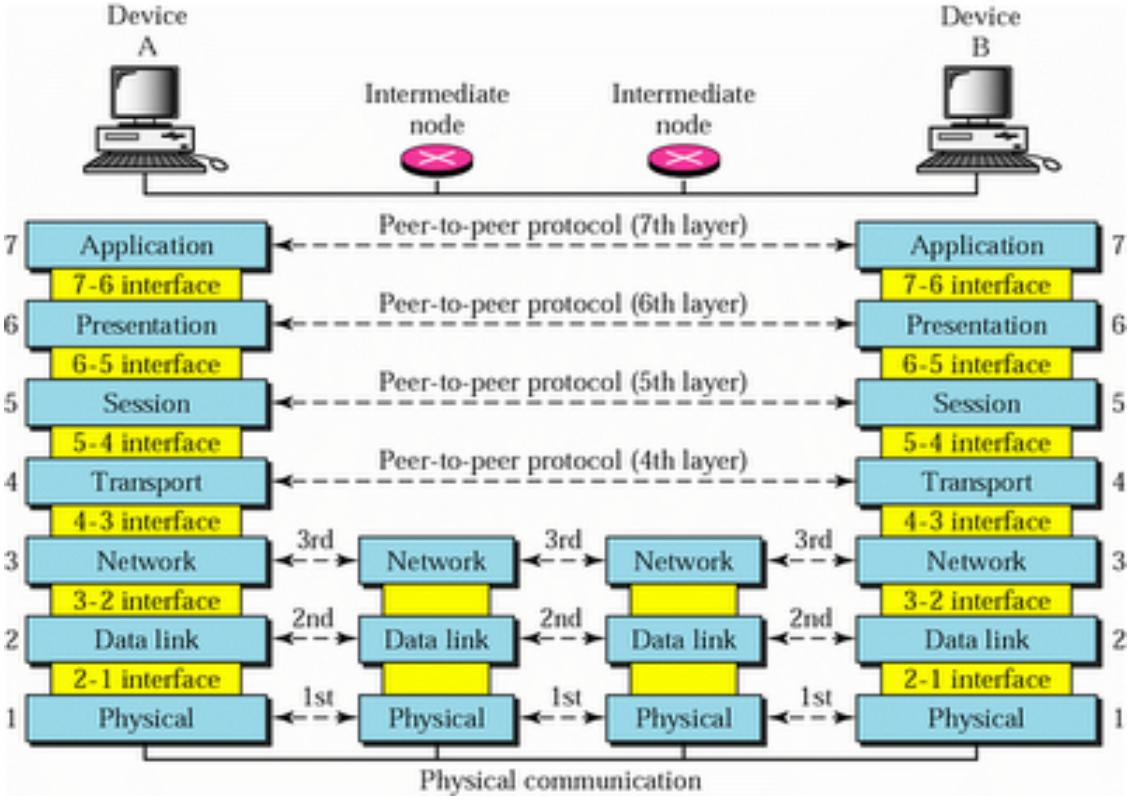
Defense In Depth

- The concept of defense in depth is to manage all kinds of risk with diverse defensive strategies; physical security is essential

- If one layer of defense fails, another layer of defense will hopefully prevent a full breach: e.g. perimeter fence and motion detection sensors, security cameras.

- Defense in depth is especially effective when each layer works in concert with the others.

Open Source Interconnection (OSI) Model



Defense in Depth

- Must use multiple security products that complement one another
- Failure in one does not result in total insecurity
- This includes firewalls, an intrusion detection system (IDS) and strong authentication on important servers
- Encryption is also an added layer of security

Defense In Depth Strategy

- People, process and technology at core of defense–in-depth strategy
- First step of a defense-in-depth strategy to protect against network breaches is to establish proper access control systems
- Check whether users have correct device identities (software, hardware, network etc.) and user IDs (credentials)
- Access should be role-based and given on need-to-know basis; updated regularly
- If a breach occurs using stolen user credentials, the organization must be able to immediately deny access caused by detection of breach via centrally managed VPN or deny remote access rights

Defense In Depth Strategy

- Layering security defenses in an application decreases chance of a successful cyber attack but does not assure 100% security

- Redundant security measures force an attacker to circumvent each measure to gain access to digital protected data

- Example: the use of a packet-filtering router in conjunction with an application layer gateway (ALG) and an intrusion detection system (IDS) combine to make it harder to attack the system

- Adding strong password controls, two-factor authentication and user security awareness training improves the system's security profile even more

Defense In Depth Strategy Components

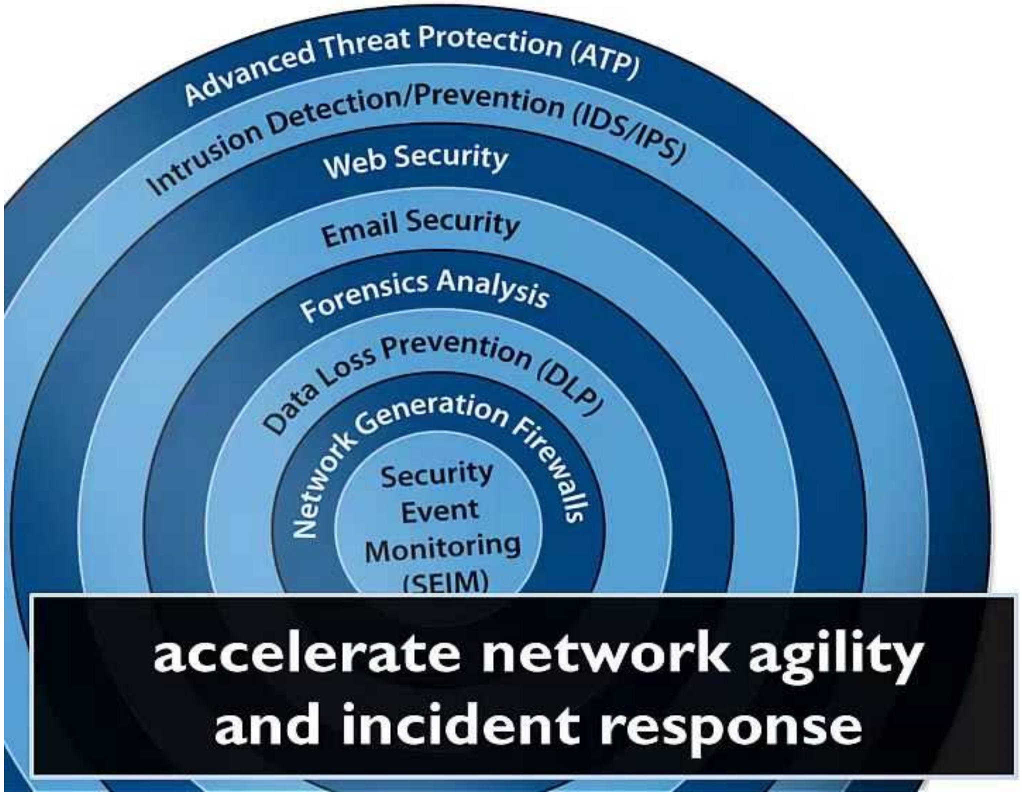
- Backup all critical data regularly-the only real defense against a ransomware attack

- Perimeter protection is critical to operations but doesn't protect from insider threats

- No clear separation between inside and outside of enterprise perimeter; corporate data and applications often reside in the cloud

- Must have an architecture that protects users, applications and assets wherever they reside in the enterprise perimeter; they must hold up against long-term complex attacks like advanced persistent threats (APTs)

Network Defense-in-Depth


Advanced Threat Protection (ATP)
Intrusion Detection/Prevention (IDS/IPS)
Web Security
Email Security
Forensics Analysis
Data Loss Prevention (DLP)
Network Generation Firewalls
Security Event Monitoring (SEIM)

accelerate network agility and incident response

Network Security in Layers

1. **Advanced Threat Protection (ATP)**
   e.g. FireEye, Cisco/Ironport
2. **Intrusion Detection/Prevention (IDS/IPS)**
   e.g. Sourcefire, McAfee
3. **Web Security**
   e.g. Imperva, Fortinet,
4. **Email Security**
   e.g. Bluecoat, Trustwave
5. **Forensics Analysis**
   e.g. RSA/NetWitness, Solera
6. **Data Loss Prevention (DLP)**
   e.g. Websense, TrendMicro
7. **Network Generation Firewalls**
   e.g. Palo Alto Networks, Checkpoint
8. **Security Event Monitoring (SEIM)**
   e.g. HP/Arcsight, IBM/Q1Labs

Seamless Integration of Components

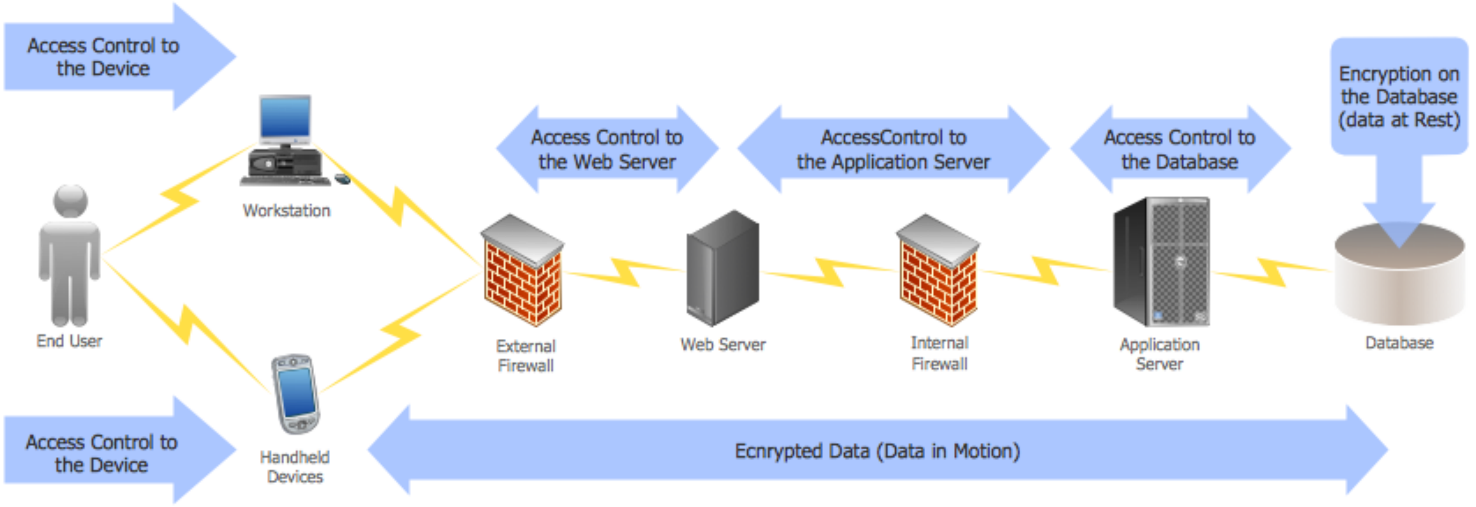
- The best defense against security attacks of all kinds is a detailed picture of how applications work together across the IT architecture

- It presumes collaboration among IT and application owners, designers and developers

- Once IT Ops has a complete picture of application stack, they can take measures to prevent and recover from ransomware attacks and other threats as they appear in the data center

- Network and security components must be able to communicate; if an attacker penetrates one system, others can respond immediately to take preventative measures.

Computer Security Model Shows D-in-D



Access Control to the Device

Workstation

End User

Access Control to the Device

Handheld Devices

Access Control to the Web Server

External Firewall

Web Server

AccessControl to the Application Server

Internal Firewall

Access Control to the Database

Application Server

Encryption on the Database (data at Rest)

Database

Ecnrypted Data (Data in Motion)

Hardware and Software Components

- Data loss prevention (DLP) products and applications are available as hardware appliances, software apps and cloud-based services

- They monitor structured and unstructured data to ensure that only authorized individuals have access to this information--there are many DLP product vendors

- Secure web gateways (SWG) are available as hardware appliances, software and cloud-based services; they monitor traffic to protect against the introduction of malware to the network.

- Security analytics products aim to detect security events as they occur, preferably in real time.

Risk Assessment Questions

- Does the IT operations team have recovery and restore plan? Is critical data backed up?

- Is there an incident response team?

- Is there a complete inventory of all of the organization's assets (devices and software) that connect to the network?

- Have the most critical data repositories been identified and prioritized? (Don't try to protect everything equally).

- Is there an up-to-date log of software updates and security patches?

- What are the password policies, and are they strictly enforced?

Best Practices

- Deploy patch updates for operating systems and all software
- Conduct continuous monitoring of network to detect anomalies and risks
- Conduct penetration testing to identify vulnerabilities on your network
- Raise user awareness, adopt and enforce strict password policies and two-factor authentication; train employees to avoid opening email attachments or links from unknown sources
- Maintain up-to-date antivirus and security software
- Restrict user permissions to the principle of least privilege and need to know

Resources

- Center for Information Security Critical Controls-https://www.sans.org/critical-security-controls

- Network Perimeter Security in a Perimeterless World ,Tech Target, Security School by Johna Til Johnson, Nemerles Research, http://searchsecurity.techtarget.com/tip/Ensuring-network-perimeter-security-in-a-perimeterless-age

- Have backups ready for ransomware recovery – – not the ransom by Brian Kirsch, tech target-**http://tinyurl.com/yc59mycz**

- Defense in Depth https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

- Understanding Layered Security and Defense in Depth: http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/

- Six Strategies for Defense- in- Depth: http://www.opus1.com/www/whitepapers/defense-in-depth.pdf