Introduction to Cyber Security

Joachim Mammele

ICCM Europe

01.02.2022

https://security-companion.net/

Overview

- Definition
- Client-PCs
- Servers
- Vulnerability Scans
- Pentests

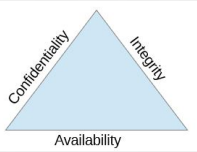
Definition Cyber Security

- Efforts to protect data and information from unauthorized access, modification, publishing or deletion

CIA Triad

Describes the 3 most important goals

- Confidentiality
  - No authorized access
- Integrity
  - No authorized modification
- Availability
  - Systems can be used at all time



The AAA of Security

- Authentication
  - Verifying that a person is really the one it pretends to be
- Authorization
  - Verifying if a person is allowed to access certain files or areas of a building
- Accounting
  - Logging of activities and user data (eg. IP-addresses)

Possible countermeasures

- Not a single action is sufficient against attacks but a combination of many different ones (Defense in Depth)
- On-going cat and mouse game between IT-staff/police and hackers
- Groups of attackers are not only encrypting data but also exfiltrate it. If the vicitims don‘t pay then attackers threat to make the personal data public

- In general: A complete protection is never possible. It is only possible to make life harder to attackers so that they go somewhere else („don‘t be the low hanging fruit“)
- Please verify for each of the following suggestions if and how they can be applied to your organization

Strategic countermeasures

Create a Disaster Recovery Plan

- What is the most valuable data?
- Which data should never be released to public?
- Make a plan about how to act in case of an incident (hacker attack, ransomware etc.)
- Print the plan to prevent its encryption

Client-PCs

- Protect BIOS with a password
- Define order of boot-devices in BIOS
- Activate UEFI/ SecureBoot
- Activate hard drive encryption (BitLocker)
  - test first if it makes computer slower
- Deactivate USB-drives/sticks (difficult to exlude sticks that act as keyboard), see eg. video and Attiny payloads
- Configuration via Group Policies

- Regularly install Windows-Updates (eg. using WSUS)
- Inventory of clients to always have an up-to-date overview of Windows patches, installed software, drivers, etc. → Example: https://www.opsi.org
- Install third-party software via software depot and keep it up-to-date (https://fogproject.org/)
- Create black/white lists of third-party software
- Policy: What is the user (not) allowed to do?
- Use Windows protection functions like Defender (prevents encryption of files)

- Browser as a special gateway
  - Protect against execution of scripts with plugins like uMatrix,NoScript or uBlock Origin
  - Introduce blacklists via proxy

Network

- Disable unnecessary/unencrypted ports through firewall, use encrypted ports instead (e.g. HTTPS instead of HTTP, SSH instead of Telnet)
- Prevent connections between clients (e.g. desktop PCs)
- Separate areas (IT, HR, management) by VLANs
- Printer firmware is very rarely updated
  → Printer in own VLAN, allow traffic only from outside into VLAN but not from printer VLAN to outside

- Never share RDP directly to outside but only via VPN
- Always change default user/password combinations
- Use a firewall (OPNsense, pfSense etc.), configure implicit deny

Wi-Fi

- Only WPA2 or WPA3 (no WPA or WEP)
- If possible use WPA2 with Enterprise Mode
- Disable WPS function (button on router)
- Put Wi-Fi traffic in own VLAN

- Check Wi-Fi coverage
  - Is Wi-Fi really necessary in the parking lot?
- Hackers could easily carry out attacks from the parking lot using directional antennas, e.g. to guess the password (password spraying).
  - Possibly use other antenna shapes than standard omni antennas to avoid radiation into certain areas (outside)
- Activate wireless isolation
  - Allow clients only access to the Internet and not to other clients or servers in the network

Wi-Fi usage on the go

Risks:

- Traffic in open Wi-Fis can be listened to by anyone with AccessPoints in MonitoredMode
  - use only with VPN or better avoid it
- Fake APs with same SSID as legitimate AP but with higher transmission strength
  - Clients connect to fake AP instead of real AP

- Computers often automatically connect to open W-LANs that have an SSID that you were already connected to before
- Choose cable over Wi-Fi / deactivate Wi-Fi where possible

Wi-Fi - MAC filtering

- Offers only limited protection as the MAC address of a client can easily be changed to gain access (MAC spoofing).
- But can be an effective protection together with other measures

Smartphones

Ban "Bring Your Own Device" within your organization or

- Do not allow jailbroken/custom ROM devices
- Allow devices only if they contain only apps from official app stores
- Possibly: mobile device management allows centralized control of devices
- Establish rules for Bring Your Own Device / Choose Your Own Device
- Limit access rights of smartphones by putting devices in own VLAN

Backups

- 3-2-1 system (original counts, 2 in house, one out of house)
- Keep backups offline to avoid encryption by Trojans
- Use pull instead of push strategy (avoid write permissions of source computer to backup server)

Active Directory

- Central point of a network
- Always create regular backups of the AD
- Make clients replaceable
  - Store data only centrally on server
  - Enable folder redirection on clients
- Do not install software directly on clients but only use centralized management

- Install Windows via PXE on clients
  - Integrate additional programs into images using Windows Deployment Services
- In case of encryption or Trojan attack, rebuild server and clients and import AD backup into server
- If only a partial re-setup of IT systems is performed, there is a risk of a new infestation
- Practice recovery regularly in test environment

Passwords

- Set up password policy (at least 8 characters with at least one lower case letter, upper case letter and special characters)
- Otherwise risk of brute force attacks

password lists

- example: Password list
- Use passwords only 1 time, for each account a different one
- Password manager Bitwarden or Keepass (in combination

Create security awareness

- Question: Do your colleagues know what to do if
  - USB stick is found in parking lot
  - An unknown person wants to get into the building or follows an employee to get into the building

- Recognize false package messengers, do not let them enter the building unobserved
- Avoid group photos with badges on social media
- Do not leave hard drives and USB sticks on the desk, always lock them away
- Lock server cabinets

Train security awareness

- Do not open unknown attachments or better intercept them through email firewall (example Proxmox Mail Gateway)
- Only allow newer, macro-free Office documents (docx, pptx etc.) through to the employee, no doc, docm, ppt etc.
- Disable macros or allow only signed macros
- Open alternatively with LibreOffice

- Check e-mail security with test mails
  - Verifying that not possible to open .doc-files
  - Verifying that Javascripts is disabled in mails
  - Verifying that mails are checked for viruses using the EICAR test file
- Train awareness using phishing campaigns (gofish, KingFisher)

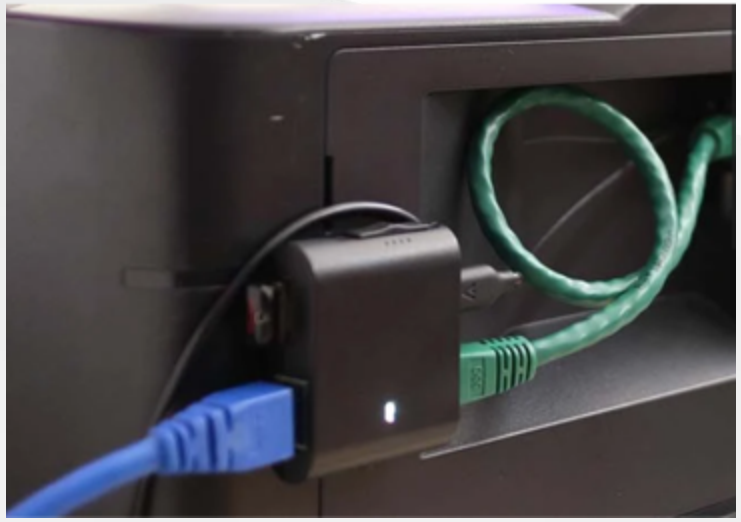
Suspicious files

- Check with virus scanners
  - Virustotal
  - heise desinfec't
- In test VM: Ensure version of host virtualization software is up-to date to avoid malware breaking out of VM
- Tool-supported real-time testing or testing in a laboratory environment
  - https://cuckoosandbox.org/ or https://www.cuckoo.ee
  - https://any.run/

General measures

- Check computer regularly for unknown "USB sticks" and "intermediate plugs" between monitor and computer
  - Rubber Ducky and Bash Bunny execute arbitrary scripts on computers, intercept login data or intercept network traffic
  - VideoGhost regularly creates screen screenshots

- check publicly accessible devices and printers for intermediary devices
- PacketSquirrel allows, among other things:
  - Recording of routed network traffic
  - DNS spoofing (intercepting DNS requests and redirecting them to own IP address)



- Disconnect unused network sockets at the patch panel
  - Shark Jack (battery-powered mini-computer) allows e.g. scanning of the network with nmap

Vulnerability scanning

- Automated scanning of servers/clients using tools (nikto, OpenVAS, nessus)
- Relatively inexpensive as scanning can be done in-house
- Detect only a small part of vulnerabilities
- Sometimes detect false positives
- Require expertise to evaluate results

Possible tools, caution: tools can have a negative impact on website performance
→ better run in test or staging environment and also only with prior permission:

- Nmap: scan machines for open ports and used protocols and versions.
- Nessus: free for up to 16 machines
- OpenVAS: open source but sometimes complex setup
- Nikto: Scan of web applications

- Special CMS scanners (WPScan, joomscan, CMSScan)
- HTTP(S) headers: Securityheaders.io or https://observatory.mozilla.org/
- SSL Check: https://www.ssllabs.com/ssltest/
- Scanning platform: https://hackertarget.com/

Pentesting

- Manual detection of vulnerabilities
- Relatively expensive since expert knowledge is required
- Enables finding of gaps that cannot be found automatically (Example: Web application: Is there a way that a normal user can see admin fields that are not intended for him?)

Pentesting - categories

1. External network pentesting

- Examines publicly accessible web sites, VPN servers, mail servers etc. for vulnerabilities

2. Internal network pentesting

- Checks how the internal network can be attacked (for example, simulates malicious behavior of an employee)

3. Social engineering tests

- How susceptible are own employees to reveal information via email or phone (phising, CEO spoofing)

4. Physical penetration testing

- Attempt to penetrate the building in the form of package deliverer etc.; plugging in malicious USB sticks to e.g. check if IT team detects them

5. Wireless penetration testing

- Checking if available Wi-Fis are state of the art (especially regarding encryption)

6. Application penetration testing

- Checking self-written software, apps etc. for vulnerabilities (using OWASP WSTG or MSTG Testing Guide)

BugBounty programs

- Offering a program to allow security professionals to scan your website for vulnerabilities
- Usually financial rewarded, but there are also programs without payment
- Examples: OpenBugBounty, Intigriti, Yeswehack

Possible further measures

- Software Firewall (NextGen)
  - Enables e.g. deep package inspection (Is the traffic on port 80 really HTTP traffic or maybe outgoing ssh traffic to a command&control server?)
- Intrusion Detection System/ Honeypot
  - Cost/benefit ratio must be weighed

- Security Information and Event Management (SIEM) (eg. ELK-Stack)
  - Is there a increased number of failed login attempts?
  - Are there logins at unusual times of the day?
- Security Onion
  - Linux distribution for threat hunting, enterprise security monitoring and log management
- OpenCVE
  - Offers a dashboard for all CVE entries
  - Offers filters and sets alarms if new CVEs are published for products used by an organization

Sources and further information

- Book: Hacking & Security by Michael Kofler et al.
- Heise special c't Security
- Training material CompTIA Security+ Professor Messer
- https://hak5.org
- Tool overview: https://inventory.rawsec.ml/tools.html

Questions?