HanseSecure

Exploit Hunter

IHK Webinar
IT-Sicherheit im Homeoffice

Inhaltsverzeichnis

1. Wer

2. Einführung

3. Praxis

1. Wer

Wer

- 21 CYBERSECURITY TWITTER ACCOUNTS YOU SHOULD BE FOLLOWING
  (https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/)

"Florian is a redteamer, pentester and exploit hunter, as well prolific tweeter and blogger. @HanseSecure is one of the best sources for tweets and retweets of technical write-ups, links to scripts, plug-ins, exploit kits and other new tools, along with how-to's and tips for anyone interested in redteaming and pentesting."

- Modern red teaming: 21 resources for your security team
  (https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)

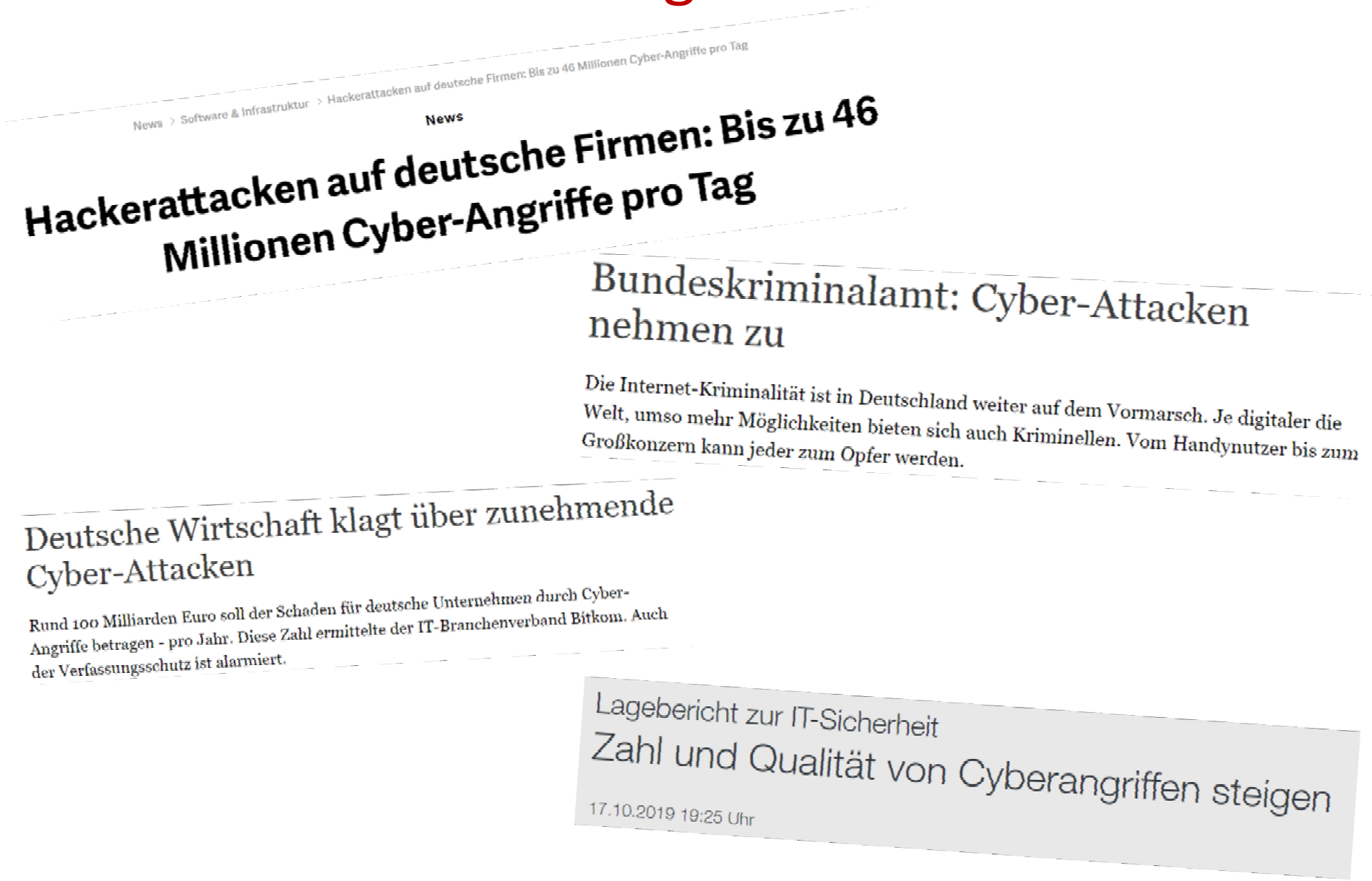
"Hansemann is an ethical hacker and penetration tester. His tweets and blog focus on tools and techniques of interest to red team members. For example, he covers Tokenvator—a tool to elevate privilege with Windows tokens—and how to write a payload for process injection in Windows."

Wer

- Intel Vulnerability
  (https://hansesecure.de/2019/05/intel-unquoted-service-path/)
- Microsoft SmartScreen Bypass
  (https://hansesecure.de/2019/05/smartscreen-bypass/)
- Disclosure CVE-2018-7272
  OpenAM Unauthorized Access
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7272)
- Disclosure CVE-2018-16231
  Remote DoS in Personal FTP-Server
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16231)
- Update CVE-2009-1437
  Remote Code Execution in Coolplayer
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1437)

2. Einführung

Einführung



News > Software & Infrastruktur > Hackerattacken auf deutsche Firmen: Bis zu 46 Millionen Cyber-Angriffe pro Tag

News

Hackerattacken auf deutsche Firmen: Bis zu 46 Millionen Cyber-Angriffe pro Tag

Bundeskriminalamt: Cyber-Attacken nehmen zu

Die Internet-Kriminalität ist in Deutschland weiter auf dem Vormarsch. Je digitaler die Welt, umso mehr Möglichkeiten bieten sich auch Kriminellen. Vom Handynutzer bis zum Großkonzern kann jeder zum Opfer werden.

Deutsche Wirtschaft klagt über zunehmende Cyber-Attacken

Rund 100 Milliarden Euro soll der Schaden für deutsche Unternehmen durch Cyber-Angriffe betragen - pro Jahr. Diese Zahl ermittelte der IT-Branchenverband Bitkom. Auch der Verfassungsschutz ist alarmiert.

Lagebericht zur IT-Sicherheit

Zahl und Qualität von Cyberangriffen steigen

17.10.2019 19:25 Uhr

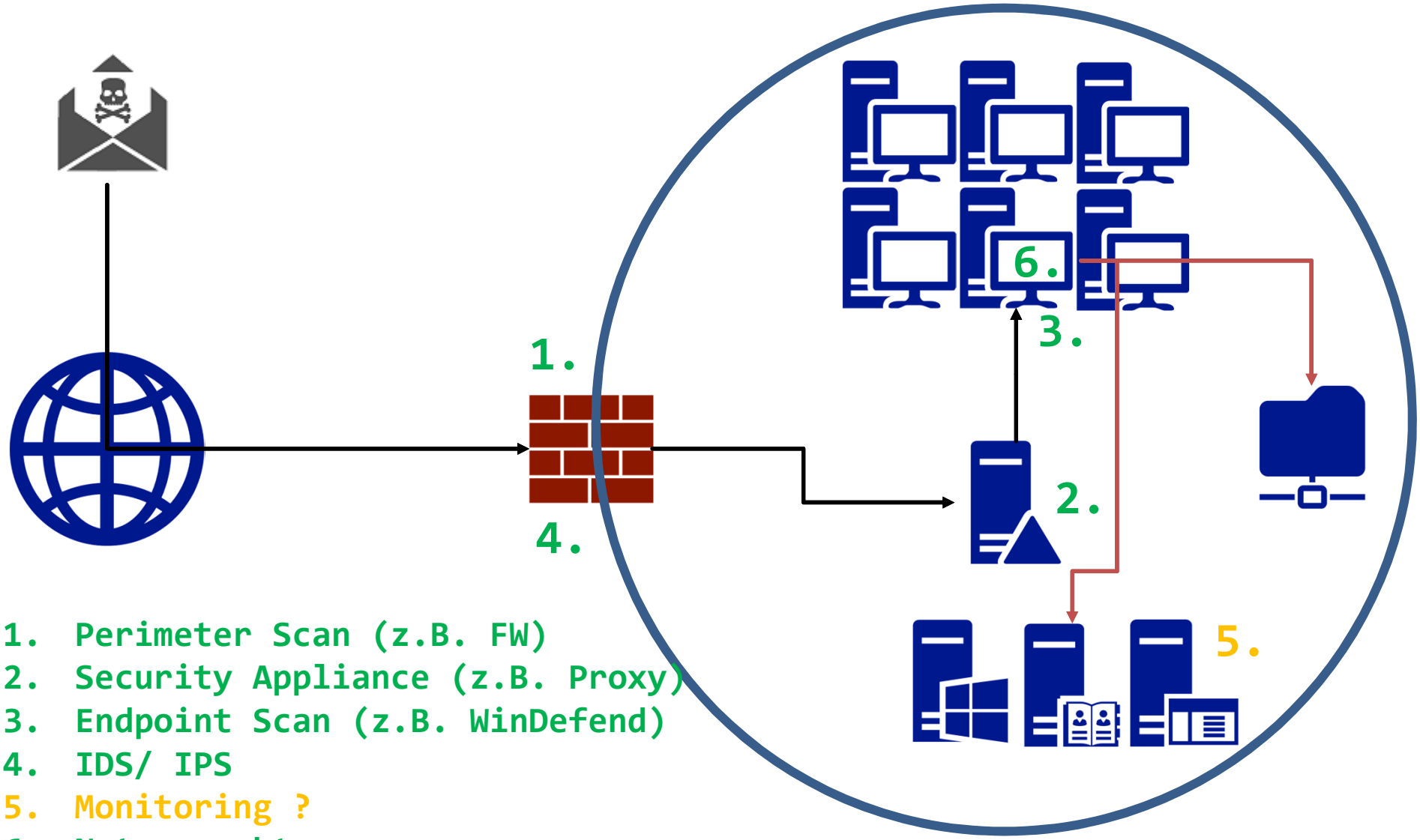
Einführung

Einführung

- Arbeit im Geschäft
- Home Office
- Home Office mit privater IT

Einführung

Arbeit im Geschäft

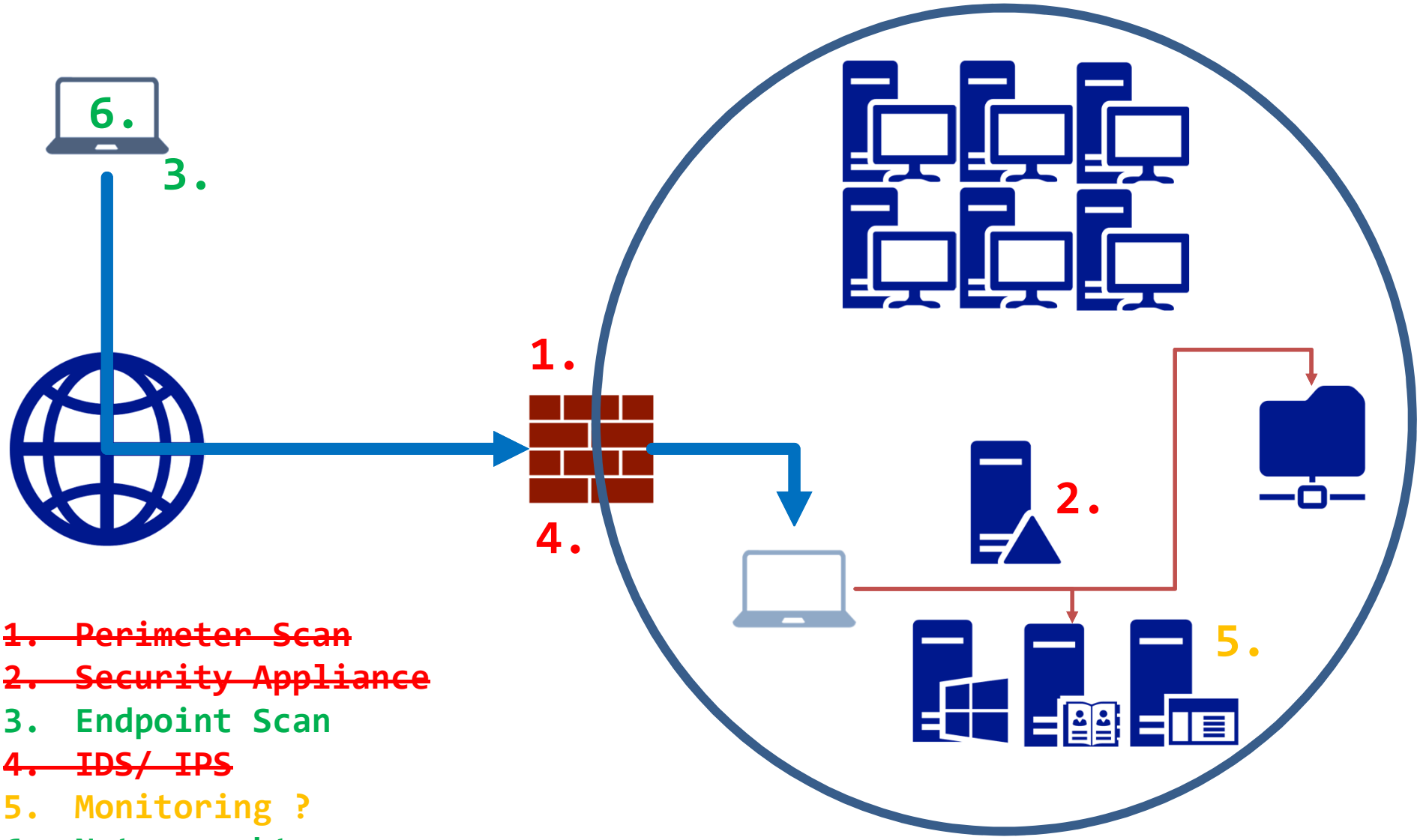


1. Perimeter Scan (z.B. FW)
2. Security Appliance (z.B. Proxy)
3. Endpoint Scan (z.B. WinDefend)
4. IDS/ IPS
5. Monitoring ?
6. Nutzerrechte

@CyberWarship

Einführung

Home Office



~~1. Perimeter Scan~~
~~2. Security Appliance~~
3. Endpoint Scan
~~4. IDS/ IPS~~
5. Monitoring ?
6. Nutzerrechte

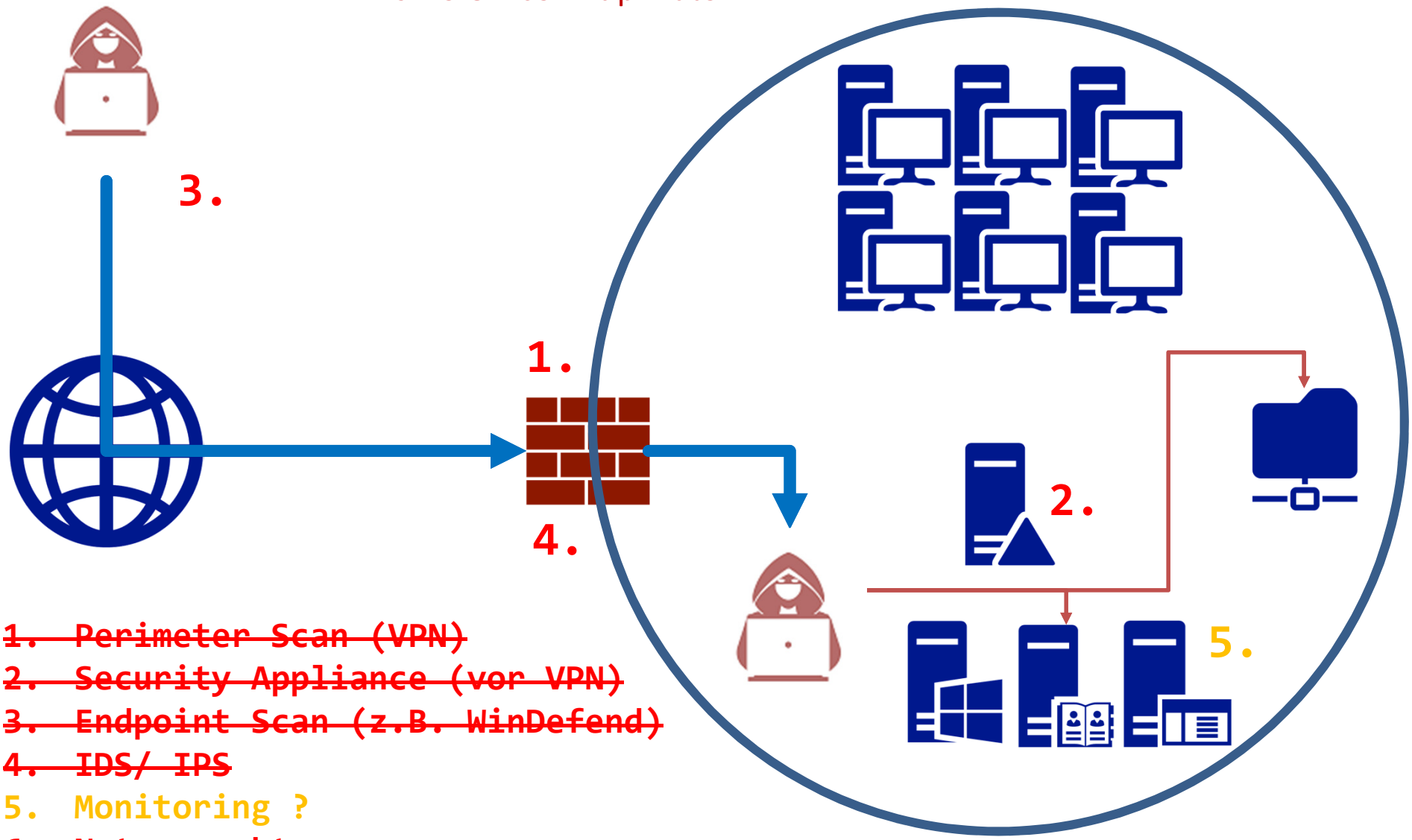
@CyberWarship

HanseSecure

Einführung

Einführung

Home Office mit privater IT



~~1. Perimeter Scan (VPN)~~
~~2. Security Appliance (vor VPN)~~
~~3. Endpoint Scan (z.B. WinDefend)~~
~~4. IDS/ IPS~~
5. Monitoring ?
~~6. Nutzerrechte~~

@CyberWarship

Einführung

Einführung

Fragen?

3. Praxis

Praxis

Pre Breach (vor dem Hack)

Angriffsvektoren

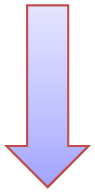
- Phishing Mails
- Wechseldatenträger
- Kompromittierter Client
- Geleakte Passwörter
- Drive-by-Downloads
- Reguläre Downloads

Praxis

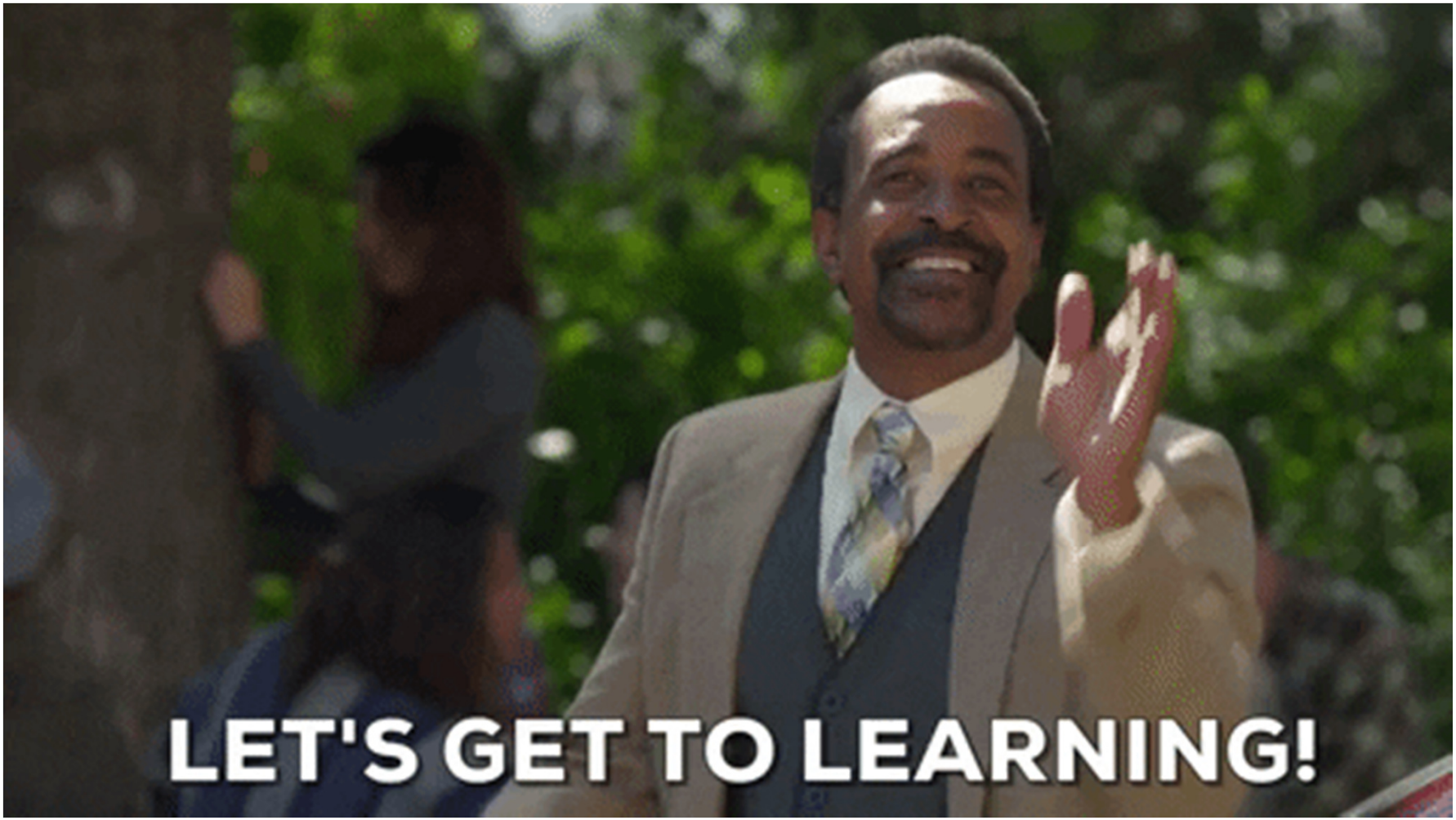
Praxis

Post Breach (nach dem Hack)

- **Alle Möglichkeiten des kompromittierten Nutzers**
- Zugriffe auf Netzlaufwerke
- Emails Lesen & Schreiben
- Zugriff auf interne Systeme
- Auf dem System gespeicherte Zugangsdaten
- **Suche nach Schwachstellen im internen Netz**



Praxis



Praxis

Quick Wins

Private IT grundsätzlich als kompromittiert betrachten	Dienstliche IT mit einheitlichen Konfigurationen verwenden
Festplattenverschlüsselung (z.B. Bitlocker)	Auswirkung von Verlust oder Diebstahl mindern Optimal wenn zusätzlich PreBoot
Passwortmanager	Verhindern von einfachen bzw. mehrfach verwendeten Passwörtern
Notwendigkeit VPN prüfen	Umfassender interner Netzzugriff vs. Kollaboration Software
2-Faktor Authentifizierung	Mindestens Dienste wie VPN oder Webmailer mit 2FA schützen

Praxis

Quick Wins

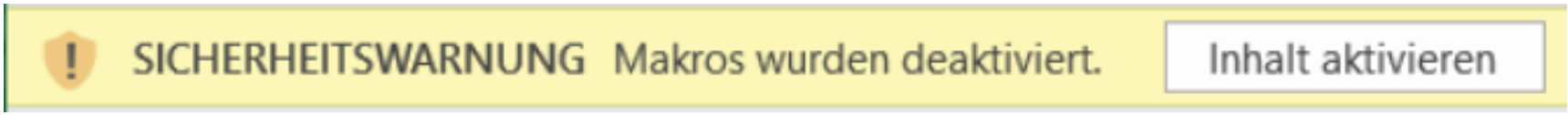
Einsichtnahme durch Dritte	Verdunkelungsfolie gegen Blicke im Cafè oder in der Bahn
Wechseldatenträger	Notwendig? Wenn ja Schnittstellenmanagement
Getrennte Benutzer Konten	Wenn Admin Account kompromittiert war, hilft nur Neuinstallation
VPN sollte in DMZ münden	Kein sofortige Vollzugriff auf das interne Netzwerk
Monitoring	Verbindungspunkte (VPN-Gateway, Terminalserver, etc.) verstärkt überwachen

Praxis

Quick Wins

Office Macros einschränken

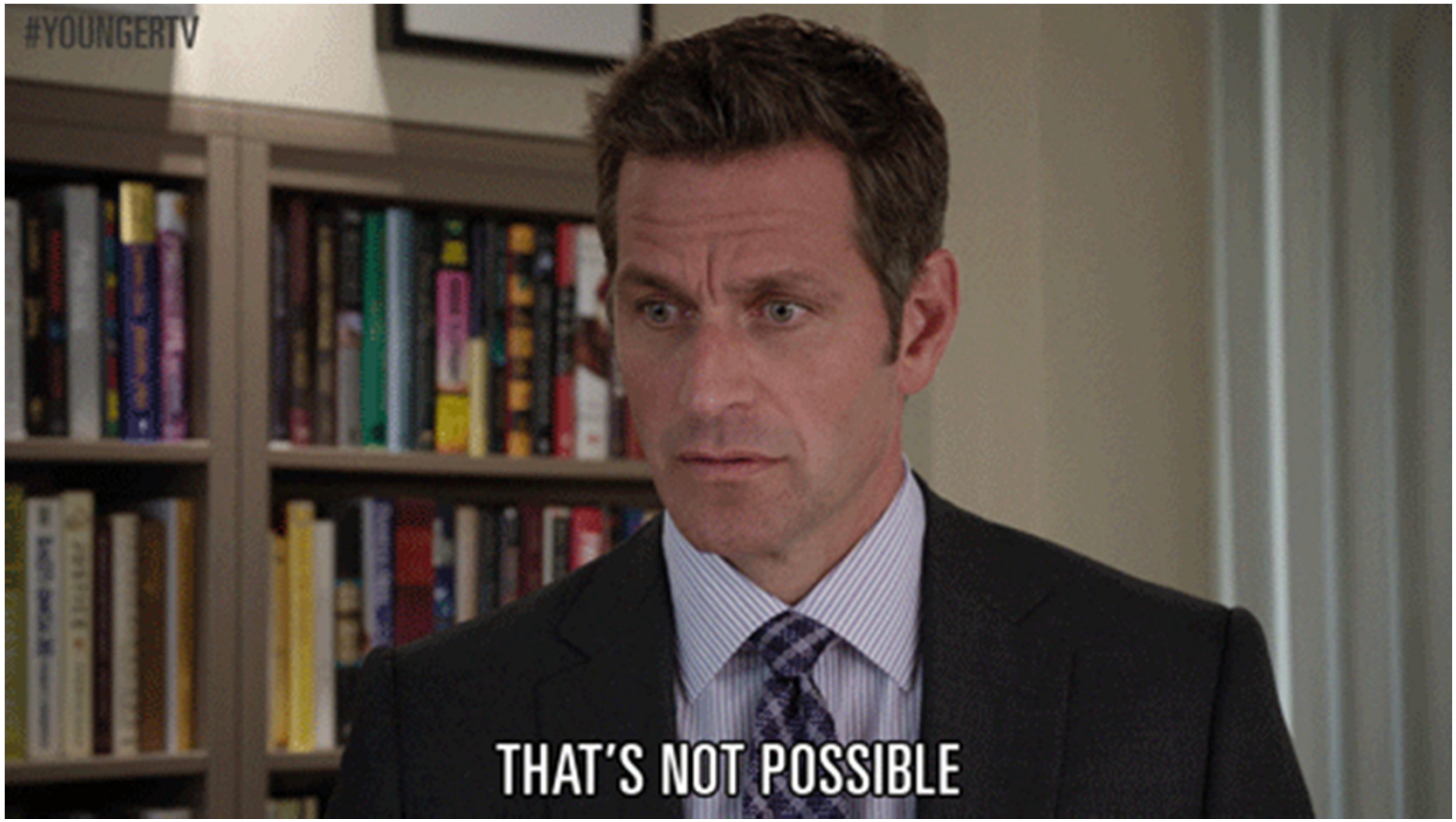
- Phishing-Emails sind das meist verwendete Einfallstor der Hacker
- Virenscanner schützen nicht ausreichend
- Ein sehr **großer Teil** der Phishing-Angriffe **verwendet Macros**
- **Viele** Unternehmen benötigen **keine Macros**
- Die gänzliche Deaktivierung von Macros wird über GPO gesteuert = extrem trivial!
- Wenn Macros benötigt werden, sollte Macro Signing verwendet werden.



Praxis

Private IT grundsätzlich als kompromittiert betrachten

Dienstliche IT mit einheitlichen Konfigurationen verwenden



Praxis

Idee für **private IT**

Betriebssystem von externen Medium

Bereitstellung einer externen Festplatte oder USB-Stick mit einem vorkonfiguierten Betriebssystem. Dieses könnte automatisch eine VPN + RDP Session zu Ihren Terminalservern herstellen. Die Nutzer könnten sich dann anschließend mit 2FA und dem jeweiligen Passwort anmelden (Useability ;-).

Der wesentliche Vorteil hierbei wäre, dass von den möglicherweise (äußerst wahrscheinlich) kompromittierten privaten Systemen die Festplatte nicht genutzt wird, welche meist die entsprechenden Schadcode-Routinen enthält.

Praxis

Quick Wins

- Private IT grundsätzlich als kompromittiert betrachten
- Passwortmanager
- Office Macros einschränken
- Wechseldatenträger
- Festplattenverschlüsselung mit Pre-Boot (z.B. Bitlocker)
- Einsichtnahme durch Dritte
- 2-Faktor Authentifizierung
- VPN sollte in DMZ münden
- Monitoring
- Getrennte Benutzer Konten
- Notwendigkeit VPN prüfen
- OS von externen Medium

Praxis

Fragen?

HanseSecure

Exploit Hunter

Danke für Ihre Zeit!

Florian Hansemann

Mobil: +49 (0) 176 6138 7300
Twitter: @CyberWarship
Mail: info@hansesecure.de