cirosec

ISMS-LEAD-AUDITOREN
ANGRIFFE
AUDITS
RUSION-PREVENTION
SECURITY
WLAN
SICHERHEITSANALYSEN
SICHERHEITSMANAGEMENT
IT-GRUNDSCHUTZ
DATA LOSS PREVENTION
PENETRATIONSTEST
IT-FORENSIK
MOBILE/WIRELESS SICHERHEIT
SICHERHEIT SENSIBLER DATEN
APPLIKATIONS-SICHERHEIT
NETZWERKSICHERHEIT
INTERNET SICHERHEIT

APTs, gezielte Angriffe, Malwareschutz

Advanced Persistent Threats (APTs)

- Typische Definition
  - Meist individuelle Malware, umgeht AV etc.
  - Gezielte Angriffe von Profis / Kriminellen bis zu State-Sponsored
- Führt zu
  - Klassisches AV, IDS/IPS, Firewalls etc. bieten kaum Schutz
  - Zahlreiche neue Produkte drängen auf den Markt
- Typische Diskussion
  - Fähigkeiten zur Erkennung und Reaktion werden immer wichtiger
    - Technisch wie personell
  - Ist Prävention am Ende?

Beispiele für APTs und die Angreifer

cirosec

- Mandiant APT1 Report
  - Abteilung 61398 des chinesischen Militärs
  - Gebäude mit 12 Stockwerken in Shanghai
    - vermutete 1.000 Mitarbeiter
  - Eigene Malware, Tools etc.
  - Durchschnittliche Dauer einer Kompromittierung 1 Jahr, oft auch mehrere Jahre
- HB Gary Federal (Anonymous)
  - Einbruch über SQL Injection in ein CMS
  - Extraktion von Benutzernamen und Hashes
    - Passwort-Cracking
  - SSH-Zugang zu Support-Server, wiederverwendete Passwörter …
  - Veröffentlichung der Mail-Datenbank von HB Gary im Internet

opsony

- George Hotz („geohot“) zeigte, wie man Herstellerbeschränkungen auf der PS3 umgehen kann
- Sony hat ihn daraufhin gerichtlich verfolgt
- Anonymous rief zur Vergeltungsaktion auf
  - Zahlreiche Hacks auf Sony, PSN etc.

Modernes Phishing: Beispiel Amazon

cirosec

Persönliche Anrede

Von: Amazon <bestellung@amazon.de>
Datum: 13. Februar 2014 07:13:35 MEZ
An:
Betreff: Ihre Bestellung | #028-1808834-83847533

amazon.de

Sehr geehrte/r Diana Biehler!

Vielen Dank für Ihre Bestellung!

Möchten Sie Ihre Bestellung ändern oder stornie
Wenn Sie Ihre Bestellung ändern oder stornieren mö

http:/www.mca.hr/cgi/
76EB2B198B2EBA05A2734C67512FF060049
9E2AF16C237CFF30122DDD51BD136
Klicken, um Link zu folgen

Bestellungsübersicht:
Einzelheiten zum Versand : Bestellung wird in ei

Bestellnummer:	028-1808834-83847533
Versand:	Premiumversand
Artikel:	EUR 799,00
Verpackung & Versand:	EUR 0,00

Gesamtbetrag:	**EUR 799,00**

Lieferung voraussichtlich: 09.Februar.2014 **zwischen** 10-15 Uhr.

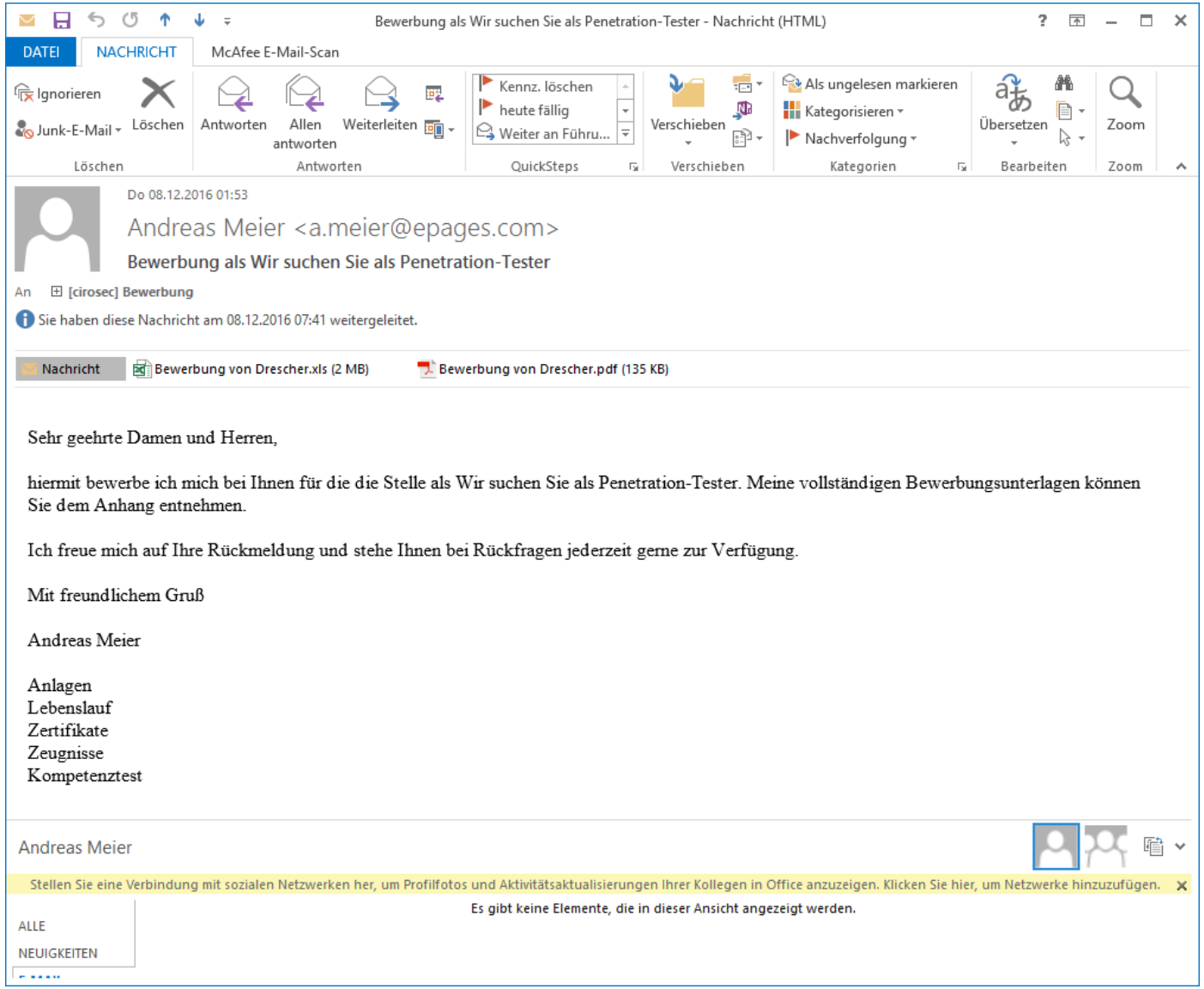
1 Apple iPhone 5S 64GB Schwarz
Smartphone; EUR 799,00
Auf Lager.
Verkauf durch: Amazon | Smartphone

Sie benötigen Hilfe beim Prüfen und ändern Ihrer Bestellungen?
Umfassende Informationen darüber, wie Sie Ihre Bestellungen aufrufen, prüfen und verwalten können, finden Sie auf unseren Hilfeseiten unter www.amazon

Wir weisen darauf hin, dass Verkäufer moeglicherweise zusätzliche Informationen wie beispielsweise die USt-Identifikationsnummer oder USt-Schluessel anfra

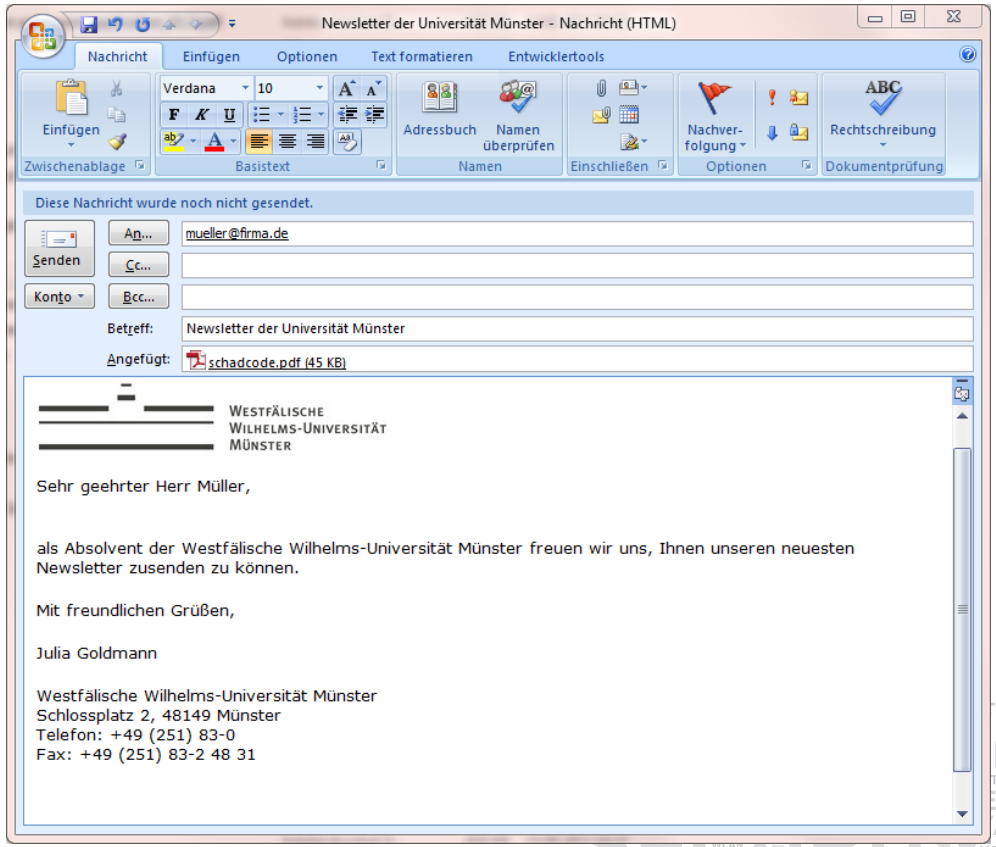
Bitte beachten Sie: Diese E-Mail dient lediglich der Bestätigung des Einganges Ihrer Bestellung und stellt noch keine Annahme Ihres Angebotes auf Abschluss e zu Stande, wenn wir Ihre Bestellung annehmen, indem wir Ihnen eine E-Mail mit der Benachrichtigung zusenden, dass der Artikel an Sie abgeschickt wurde. D

Goldeneye im Dezember 2016



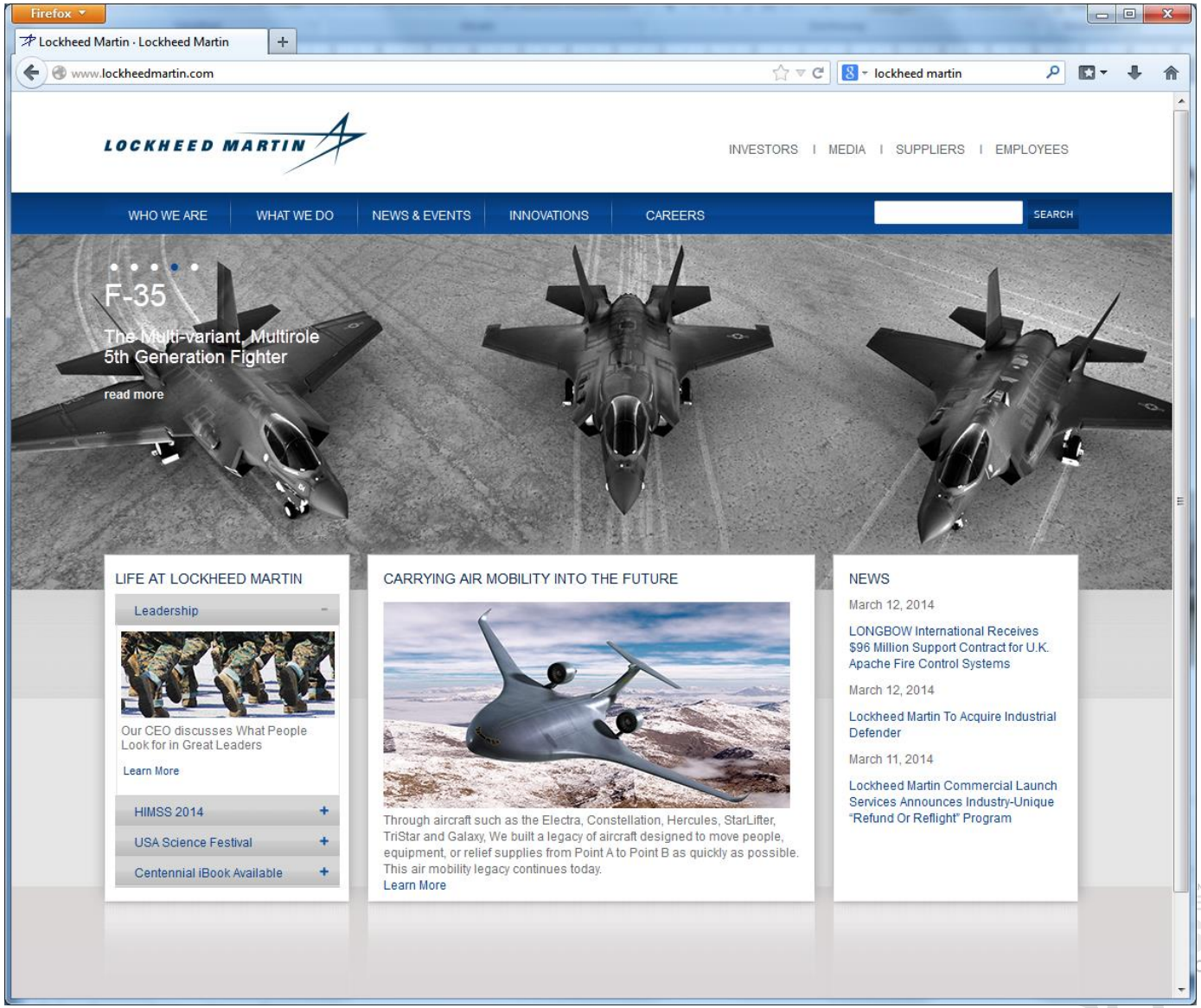
Spear-Phishing

- Gezieltes Phishing
  - Informationen kommen häufig aus sozialen Netzwerken
  - Oder aus den Kundendaten gehackter Shops



RSA / Lockheed Martin 2011

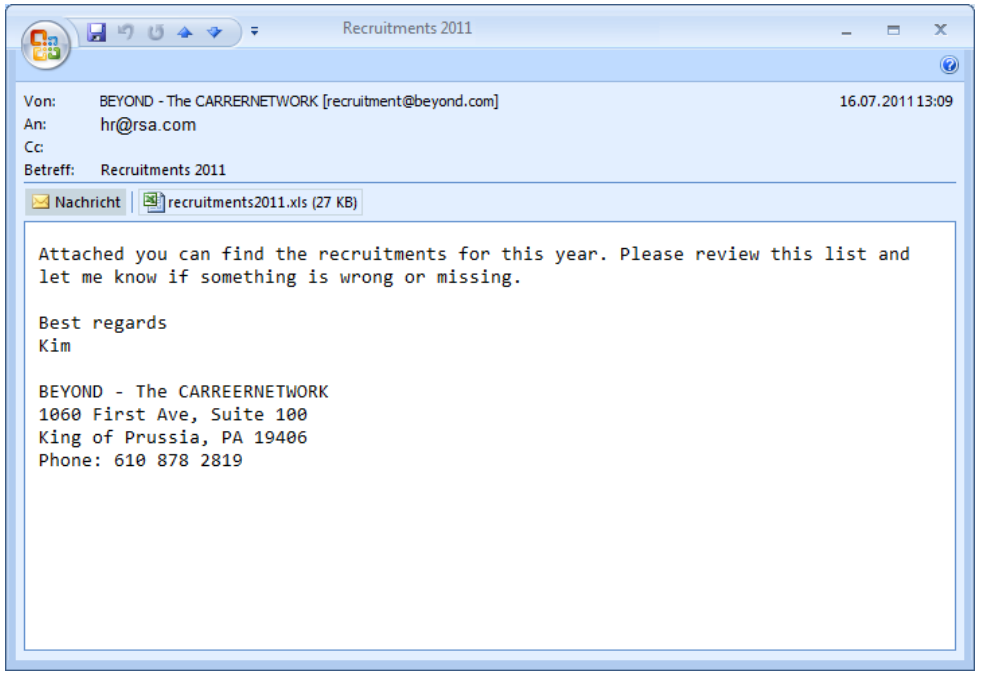
cirosec



DATA LOSS PREVENTION
PENETRATIONSTEST
IT-FORENSIK
MOBILE/WIRELESS SICHERHEIT
SICHERHEIT SENSIBLER DATEN
SECURITY

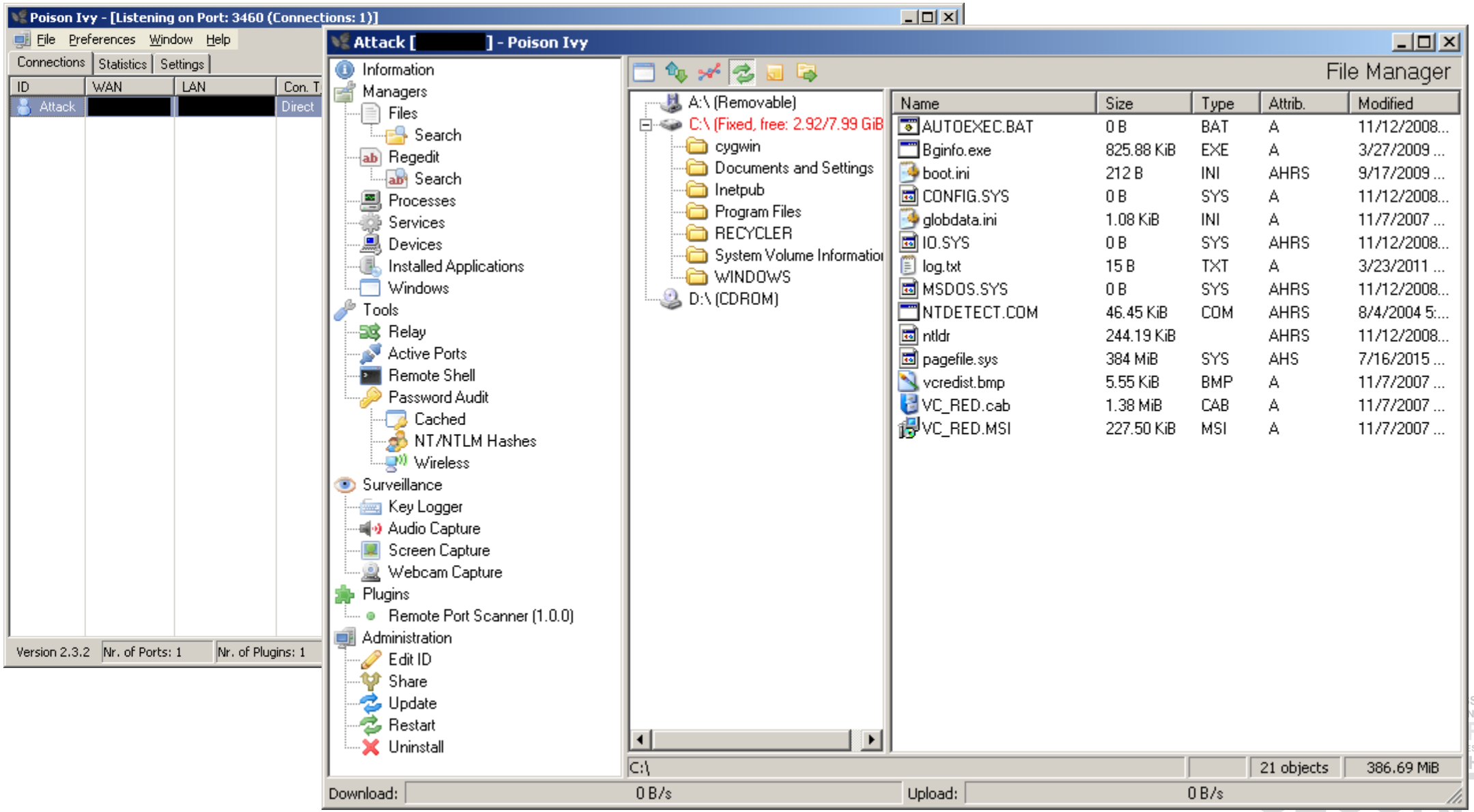
Der RSA Hack - targeted, aber nicht wirklich advanced

- Mail mit angehängter Excel-Datei
  - Darin Angriff auf Adobe Flash
  - Installiert bekannte Backdoor Poison Ivy
- Von dort aus Zugriff auf die Schlüsselinformationen der RSA-Tokens von Kunden

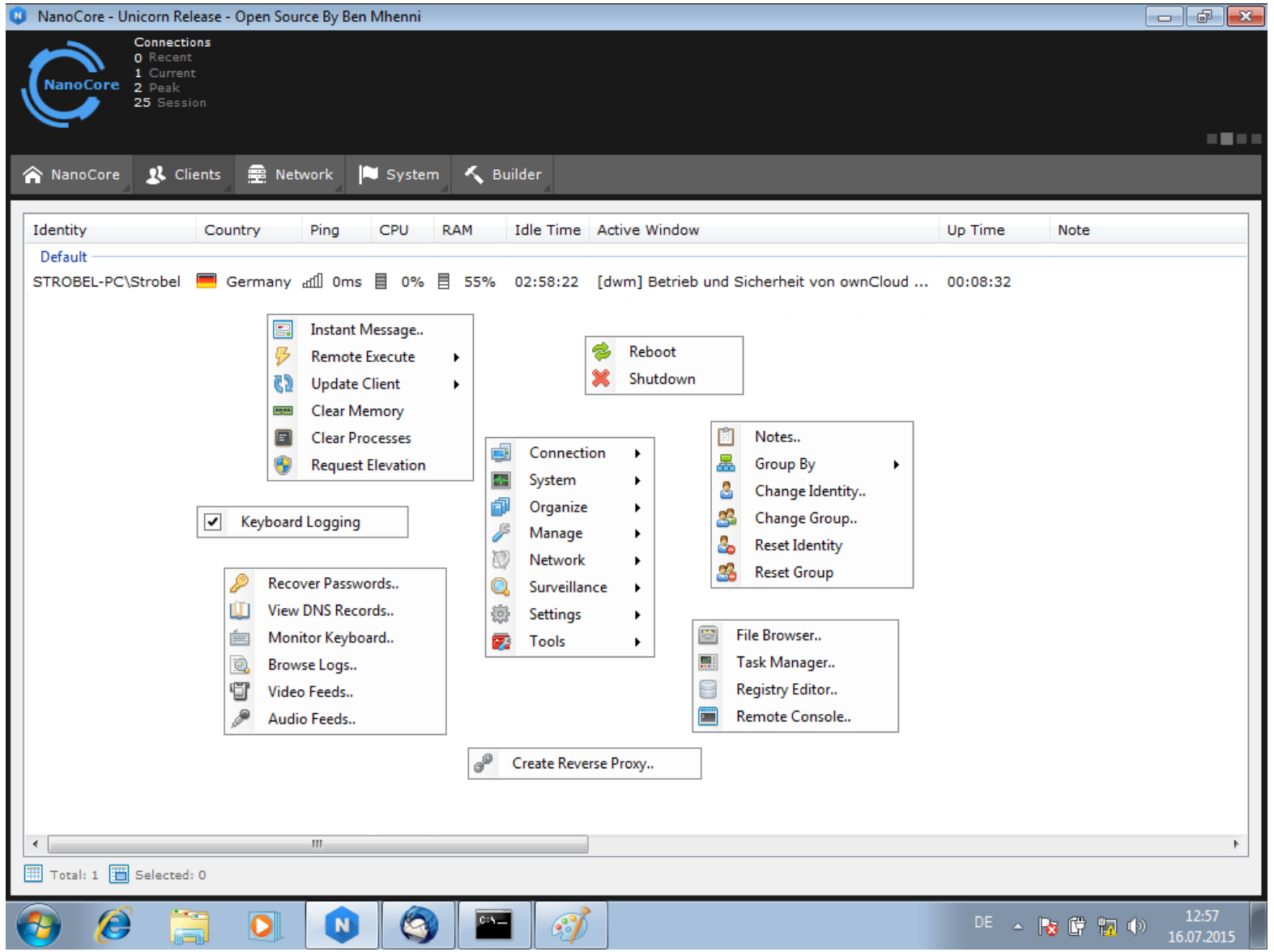


Poison Ivy - kostenlos oder kommerziell mit Erfolgsgarantie

cirosec



NanoCore - 2015 geleakt

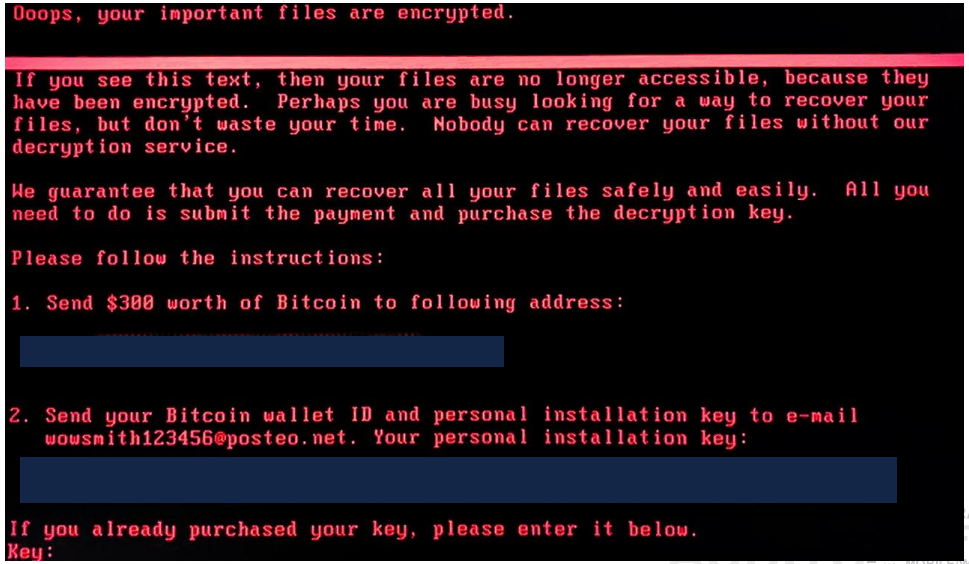


Moderne Würmer: WannaCry

- Erstmals am 12. Mai 2017 bekannt geworden.
- Mehr als 230.000 infizierte Computer in 150 Ländern.
  - u.A. 450 Rechner bei der deutschen Bahn.
- Ransomware, die sich wie Wurm verbreitet.
  - Daten der Opfer werden verschlüsselt.
  - Verbreitung erfolgt wurmartig.
- Nutzt Sicherheitslücke im SMB-Protokoll aus.
- Befällt Systeme, die nicht gepatcht wurden oder keine Updates mehr erhalten.
- Hauptsächlich ältere Systeme betroffen.

Moderne Würmer: (Not)Petya

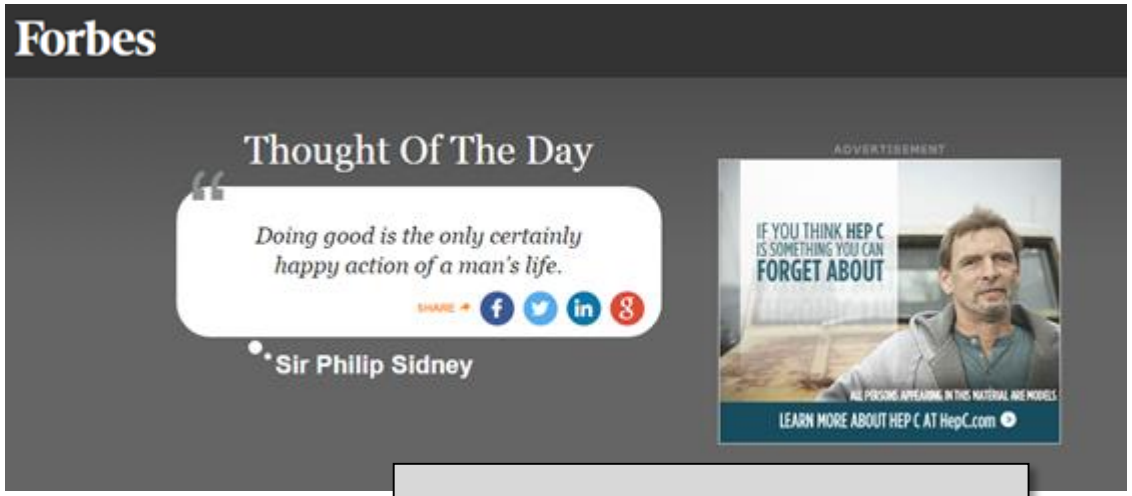
- Vermutlich Angriff von Russland auf die Ukraine
  - Zerstörung im Vordergrund, nicht Geld
- Komplexere Verbreitung als Wannacry
  - MeDoc Update
  - EternalBlue Exploit
  - Copy auf $ADMIN, psexec
  - WMCI



Chinesische Angriffe auf US-Unternehmen im November 14

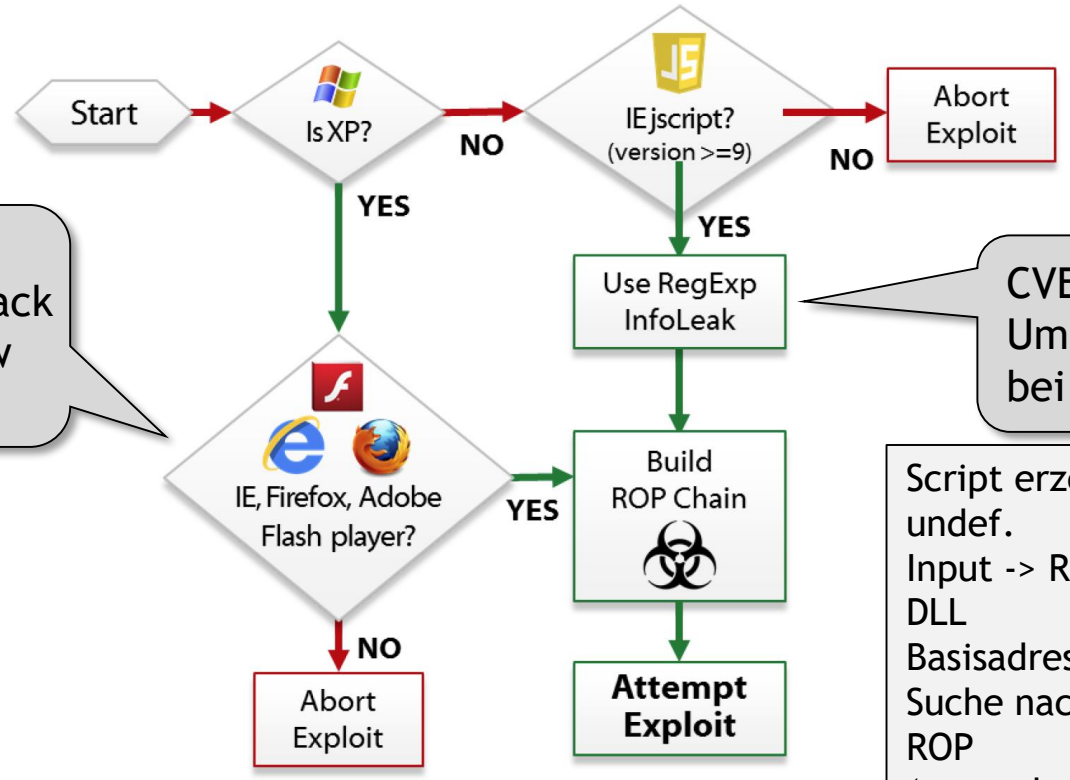
cirosec

- November 2014: chinesische Gruppe manipuliert Website von Forbes und andere
  - Flash Widget Forbes „Thought Of The Day“ auf Exploit umgeleitet



Erscheint automatisch beim ersten Aufruf der Site

Forbes-Hack im November 2014: Kombination von zwei Zero-Day-Exploits



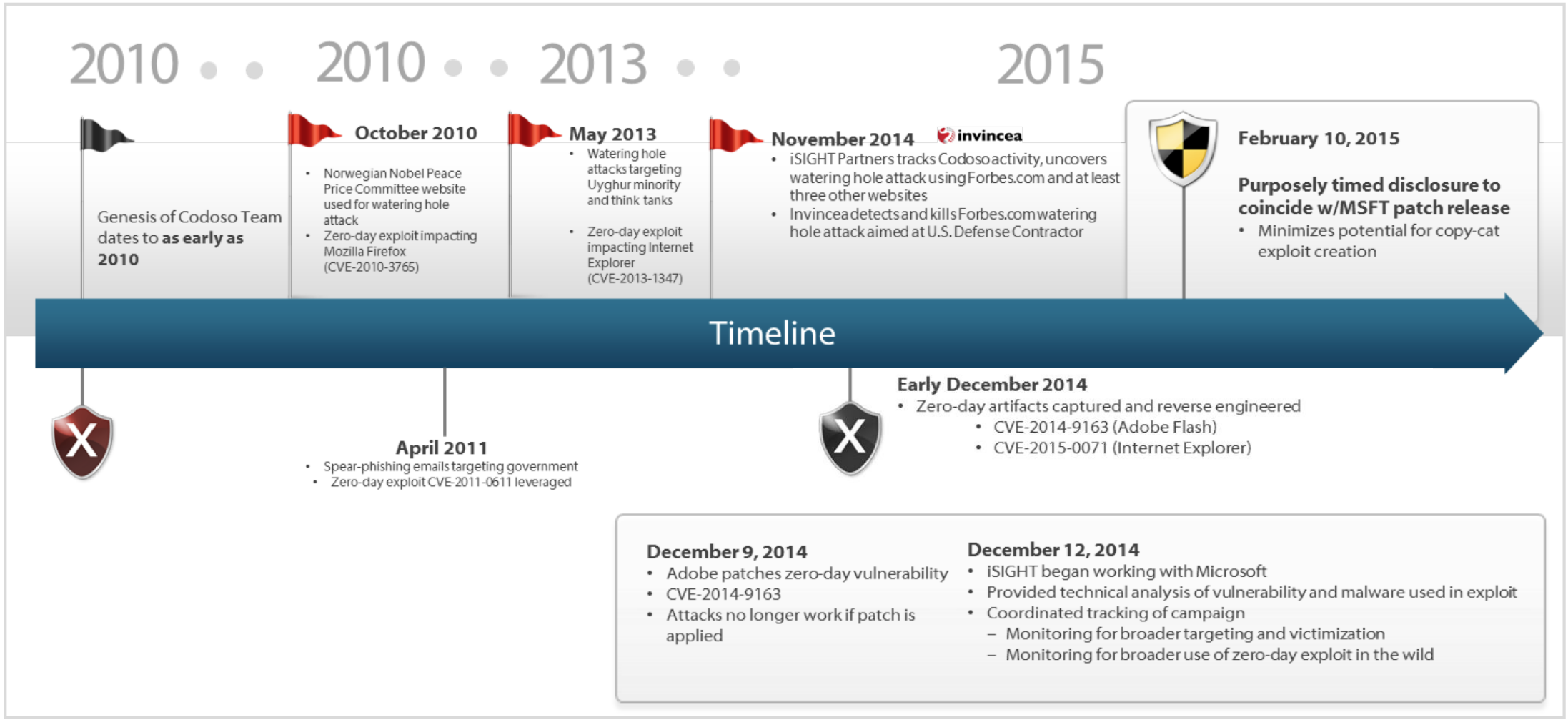
CVE-2014-9163
Adobe Flash Stack
Buffer Overflow
in parseFloat

CVE-2015-0071
Umgehung von ASLR
bei neueren IE-Versionen

Script erzeugt RegExp object mit undef.
Input -> Rückgabe von Speicher aus DLL
Basisadresse von jscript9.dll bekannt
Suche nach passenden Befehlen für ROP
(„pop ebp; ret“ etc.)

Quelle: iSIGHT Partners

Timeline aus dem finalen Bericht vom 10.02.15 von iSIGHT Partners



Quelle: iSIGHT Partners

Threat Intelligence am 12.12.14

cirosec

iSIGHTPARTNERS 1

Flash Exploit Used by Chinese Cyber Espionage Operators to Target Visitors to Forbes Website

Threat Detail

Forbes Site Visitors Targeted by Strategic Web Compromise

Cyber espionage actors exploited a Flash vulnerability to compromise visitors to forbes.com, a prominent business and news site. iSIGHT Partners believes the site was specifically targeted as part of a strategic web compromise targeting individuals likely to have access to valuable information.

- Sensitive sources indicate that visitors to forbes.com were affected by a Flash exploit in late November and early December. iSIGHT has obtained a copy of this exploit and is working to identify the vulnerability it leverages. Given the timing of this incident we consider the vulnerability may be CVE-2014-9163, patched by Adobe on Dec. 9, 2014.
- Strategic web compromises (or watering hole operations) compromise large numbers of site visitors and most likely require significant resources to identify specific victims of value to cyber espionage sponsors. Coupled with the use of a zero-day vulnerability, this probably indicates that the actors behind this campaign were well resourced and sophisticated.
- For additional technical indicators related to the compromise, please see the Technical Annex.

We believe the compromise was carried out by Chinese cyber espionage operators based on technical indicators and the use of the same undisclosed exploit in an incident attributed to Chinese cyber espionage operators.

- Resources within the payload were written in simplified Chinese.
- The command and control (C&C) domain used by malware in the incident was passively connected to tiiztm.com, a domain leveraged in several Chinese cyber espionage incidents associated with Codoso malware.

Threat Intelligence am 12.12.14

cirosec

Execution

Files Dropped

After successful exe
following files are wr

- %APPDATA
  - ♦ Stag

The stage 1 downloa
beacons it to the C&

- Systeminfo
- Ipconfig /all
- Tasklist /v

The payload stores a

- %APPDATA
- %APPDATA

The filename for the

The stage two paylo
at the following URL

The payload was an encoded DLL made to
decoded, the DLL will have the MD5 hash

The stage 2 payload
the payload are XOR

- /questions/16
- /show/informa
- /show/contac
- if exist %%1
- 5D08B586-34
- 42aedc87-21

Registry Keys

The malware proceed

Key: HKCU\Software
Settings\ZoneMap\Dc
Modification: ADD

Key: HKCU\Software
Settings\ZoneMap\Dc

Modification: ADD

Persistence Method

The stage 1 malware does not appear to h
is established by the stage 2 payload.

Network Comm

After successfu
server "iad12s0

VICTIM to C&C
GET /pv.png?b
Accept: text/htn
Accept-Langua
User-Agent: Mo
Accept-Encodir
Host: iad12s04
DNT: 1
Connection: Ke

C&C to VICTIM
HTTP/1.1 404 N
Server: nginx
Date: Thu, 11 D
Content-Type: t
Content-Length
Connection: ke

Network Intelligence

The following are domains related to this activity:

- 1b100.net
- 1e1000.net
- 1h100.net
- 1q100.net

All domains observ

Passive DNS

Passive DNS was

Passive DNS was

Passive DNS was

IP Address
106.185.35.198 25
106.185.35.198 25

Passive DNS was

IP Address
23.92.26.175 69
23.92.26.175 69

IP Information

IP Location: Ja
ASN:
IP Address: 1
NetRange: 1
OrgName: K

IP Location: U
ASN:
IP Address: 2
NetRange: 2
OrgName: F

Threat Intelligence
Intended Audience
Technical Indicator

Indicators of Compromise

Hash	Name	Description
FAA74BE286C58BE616470558D78A137F	8hthrx.swf	CVE-2014-9163 Flash Movie
CA5A35D71A01AAECC28877D316230D20	8hthrx.swf	CVE-2014-9163 Flash Movie
F81E20C5059FE1D364080E51974418D8	main.swf	CVE-2014-9163 Flash Movie
7bdf8fdb2849ef8ca24586976eb28c0b	wuservice.dll	Stage 1 Downloader DLL
3E92802BA89F3F2F66CE04311E0F3882	Wuservice.dll	Stage 1 Downloader DLL
D1CDE3D83D2AF0F5C874B821D3771A7E	Wuservice.dll	Stage 1 Downloader DLL
b8a37f47f7745a37d04866ca6edda91b	Wuref.png	Encoded Stage 2
ca293bb343eb740bd2e0cac109e37e75	Wuref.png	Encoded Stage 2
2b71a7f8a567399831e4eabe56608e79	Wuref.dll	Stage 2 DLL
A86DAC7EF848D6FF3FEB858E5706E1A6	Wuref.dll	Stage 2 DLL

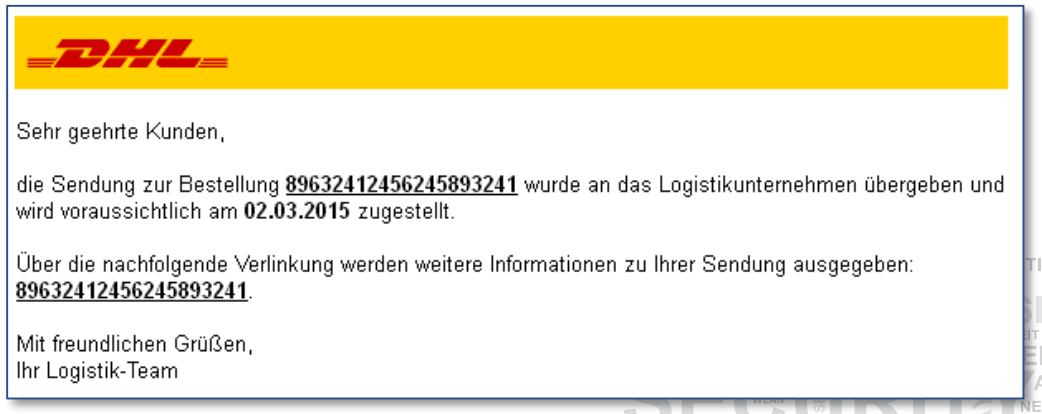
Domain	IP	Description
1h100.net	23.92.26.175	Stage 1 Domain
1b100.net	106.185.35.198	Stage 2 Domain
feedback.turkishairiine.com	46.45.171.58	Stage 1 Domain
cast.turkishairiine.com	173.255.209.141	Stage 2 Domain
1e1000.net		Related Domain
1q100.net		Related Domain
1c1000.com		Related Domain

Auch klassische Malware ist heute sehr dynamisch: Beispiel Emotet

- Bei einem Kunden aufgetreten vom 8. bis 12. Juni
- 12 infizierte Clients, 18 verschiedene Mutationen
- Verbreitung über Phishing-Mails (DHL und Telekom)
- 250 Dateidownloads (ausführbare Programme!)
  - z.B. Dhl_Status_2946396746797704__Id10__4017980311429897MXJJJ ____LC__TRZ__H11_06_2015___atdeDHL_DLU235115.exe
- Bank-Trojaner
  - stiehlt Bankkontodaten der Anwender
  - Kunden deutscher und österreichischer Banken im Fokus
  - Module
    - Abhören des Datenverkehrs
    - Senden von Spam
    - Sammeln von E-Mail-Adressen
    - Stehlen von E-Mail-Accounts
    - Organisation von DDoS-Attacken

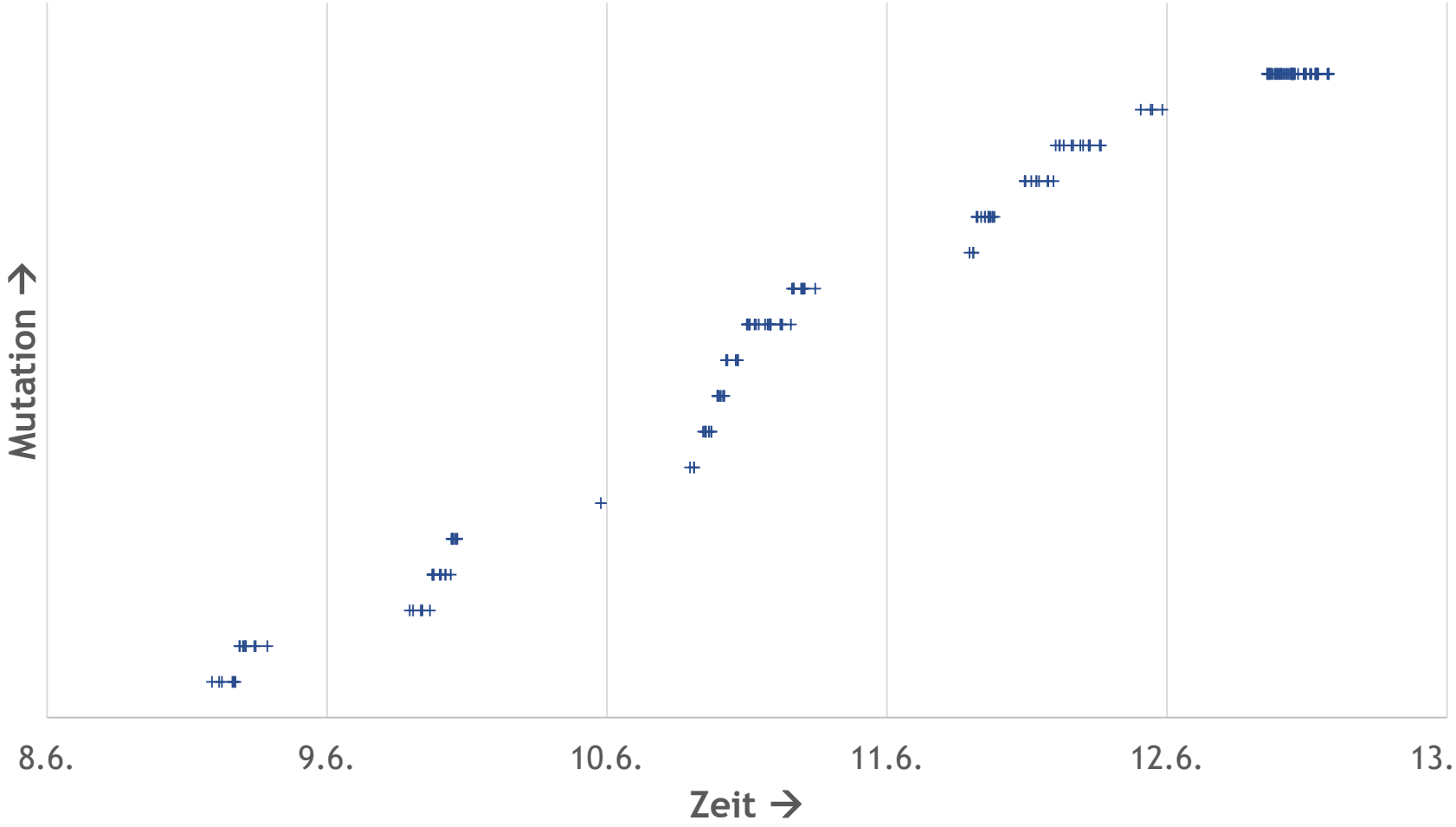
Auch klassische Malware ist heute sehr dynamisch: Beispiel Emotet

- Bei einem Kunden aufgetreten vom 8. bis 12. Juni
- 12 infizierte Clients, 18 verschiedene Mutationen
- Verbreitung über Phishing-Mails (DHL und Telekom)
- 250 Dateidownloads (ausführbare Programme!)
  - z.B. Dhl_Status_2946396746797704__Id10__401798031142____LC__TRZ__H11_06_2015___atdeDHL_DLU235115.
- Bank-Trojaner
  - stiehlt Bankkontodaten der Anwender
  - Kunden deutscher und österreichischer Banken im Fokus
  - Module
    - Abhören des Datenverkehrs
    - Senden von Spam
    - Sammeln von E-Mail-Adressen
    - Stehlen von E-Mail-Accounts
    - Organisation von DDoS-Attacken



Emotet: Mutationen

Mutationen der Malware über die Zeit



Angriffe von außen und Maßnahmen über die letzten 20 Jahre

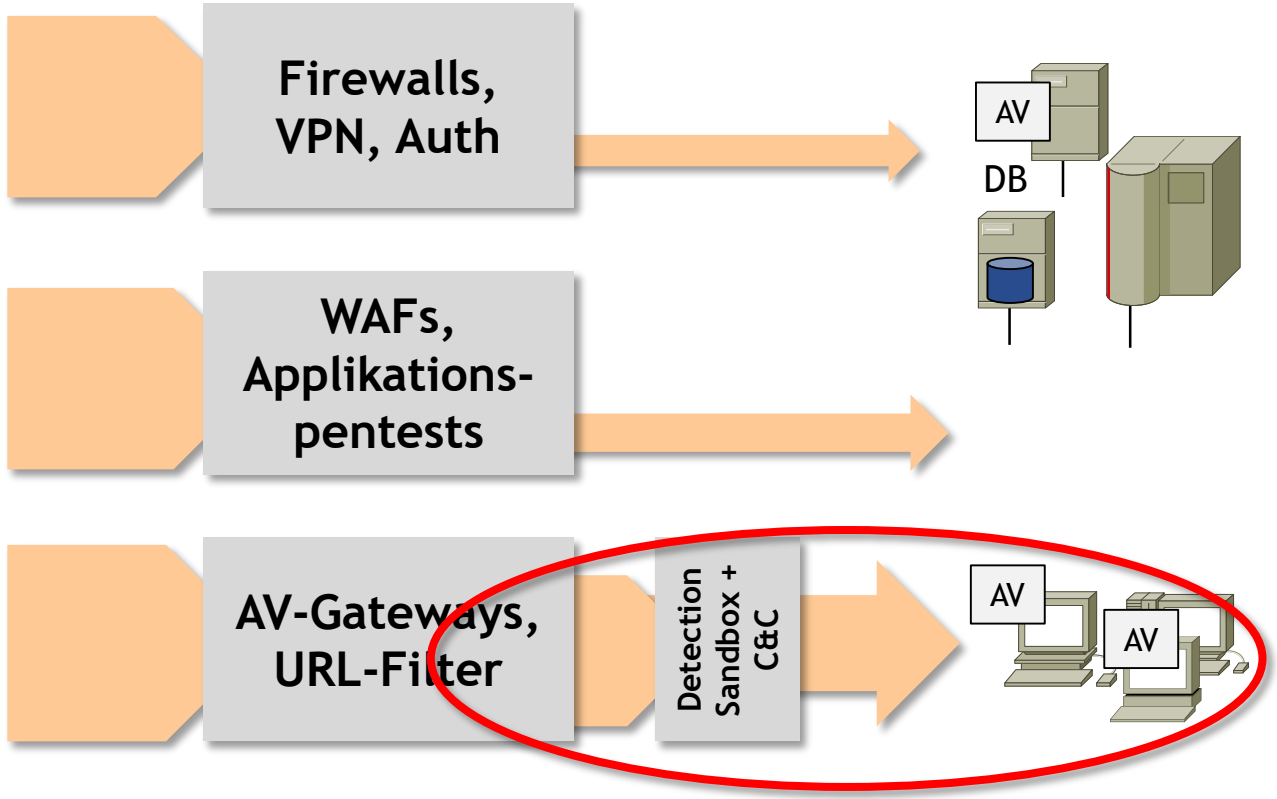
cirosec

Direkte Angriffe auf ungesicherte Server

Angriffe auf Web-applikationen, Shops, Portale, Webservices

Phishing, Viren, Würmer, Trojaner, Active Code

Individuelle / sich schnell ändernde Malware, APTs

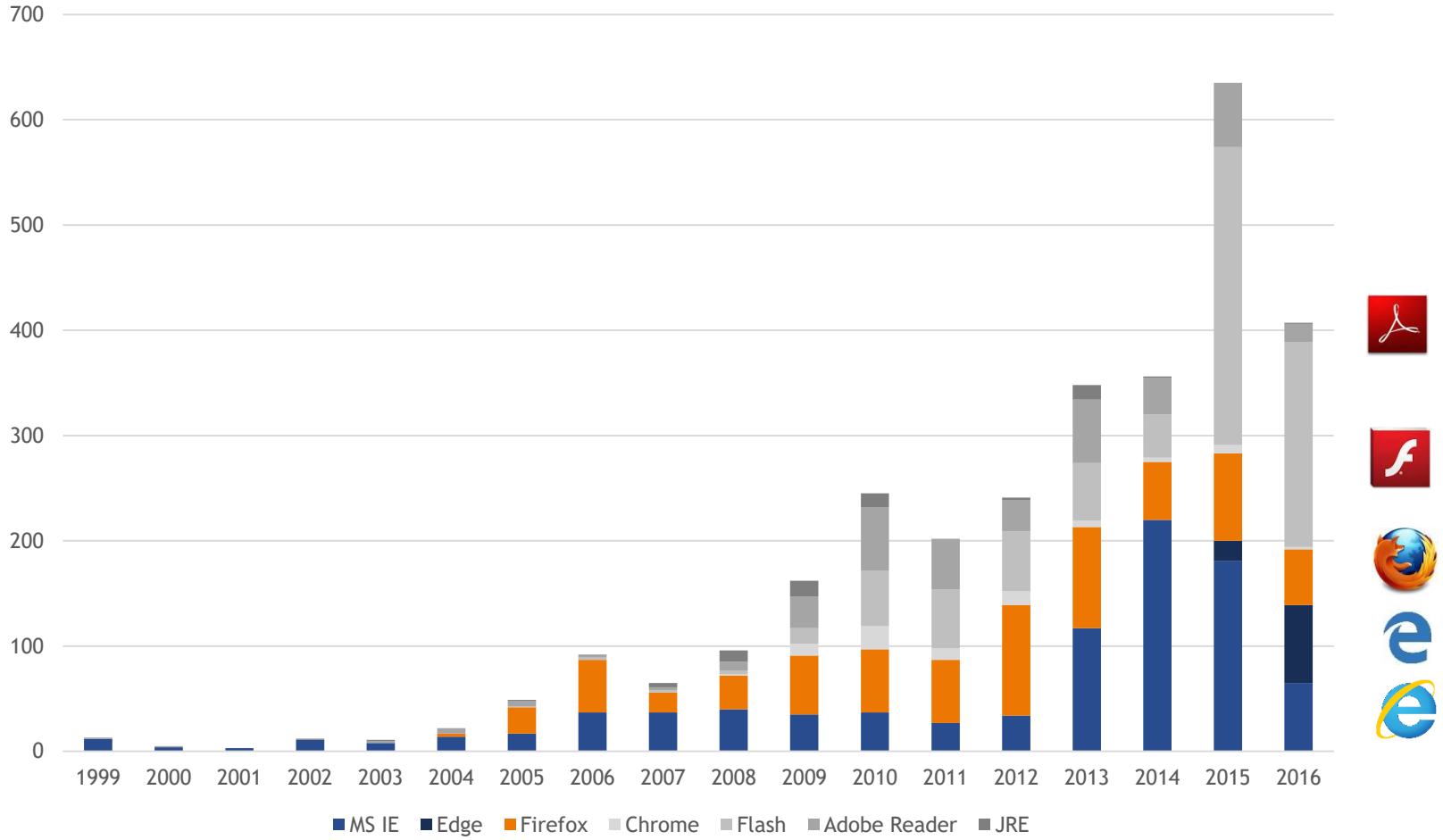


Wo liegt das Problem?

- Spear-Phishing
  - Gut gemachte / gezielte Phishing-Mails werden auch von sensibilisierten Mitarbeitern nicht erkannt
- Poisoned Search Results
  - Den Top-Ergebnissen von Suchmaschinen wird meist vertraut
- Bad Social Media Links
  - Links von „Freunden“
- Watering Hole Attacks
  - Die bekannten und häufig besuchten Websites
- Malvertisements
  - Werbung auf vertrauenswürdigen Sites
- Malicious Hot Spots
  - WLAN unterwegs
- USB Devices
  - Rubber Duckies etc.

Sind die Anwender das Problem?

Code-Execution-Schwachstellen in den Top-Browsern und Plug-ins

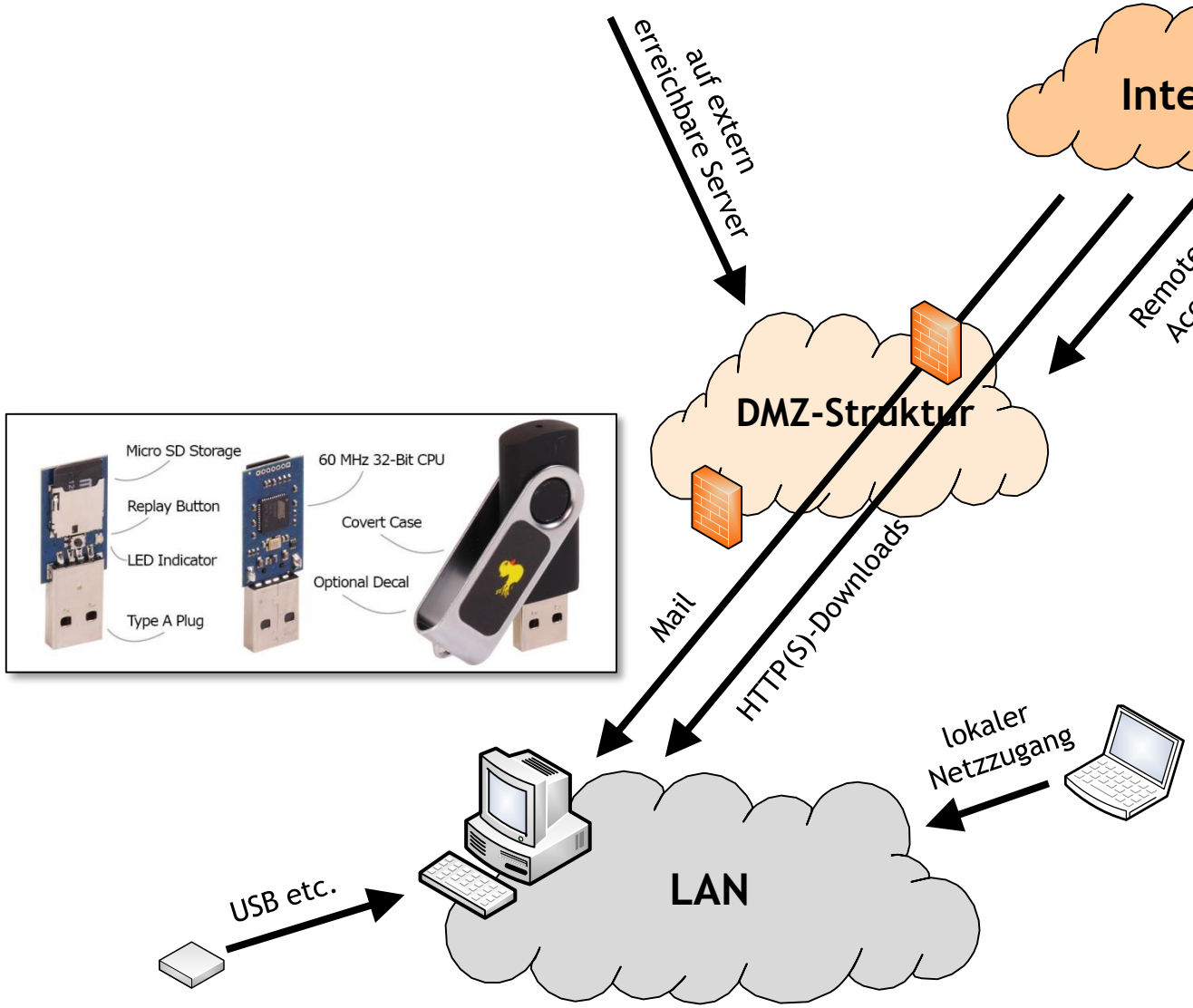


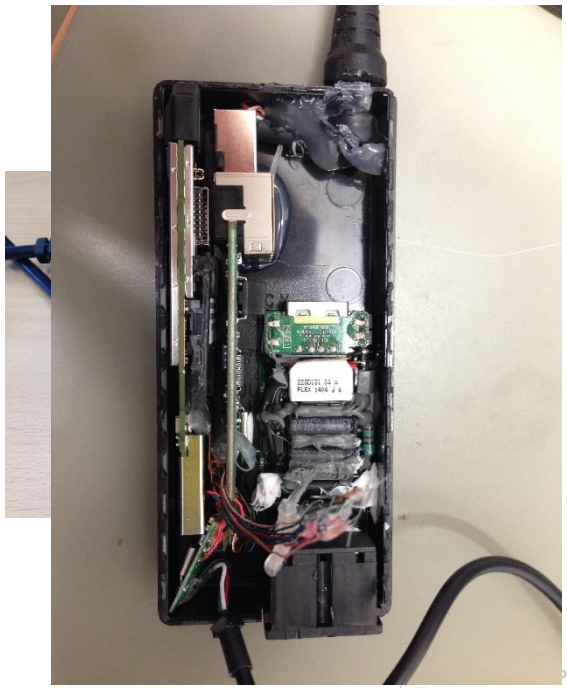
Quelle: http://www.cvedetails.com/ - Top 50 Products

Das eigentliche Problem heute

- Phishing ist inzwischen kaum noch erkennbar
  - Persönliche Ansprache, Zielgruppenspezifisch korrekt
- Malware über vertraute Kanäle
  - Watering-Hole-Attacks, Malvertisements
  - Social-Media Freunde, Software-Updates, Hot Spots
- Professionelle Malware für Jedermann
  - Crime as a Service für sehr wenig Geld
- Signaturbasierte Erkennung wirkt nicht mehr gut genug
  - Schnelle Änderung der Malware, explizite Umgehung
- Verwundbarkeit der Endgeräte

Typische Vektoren für gezielte Angriffe





cirosec

Technische Maßnahmen im Netzwerk

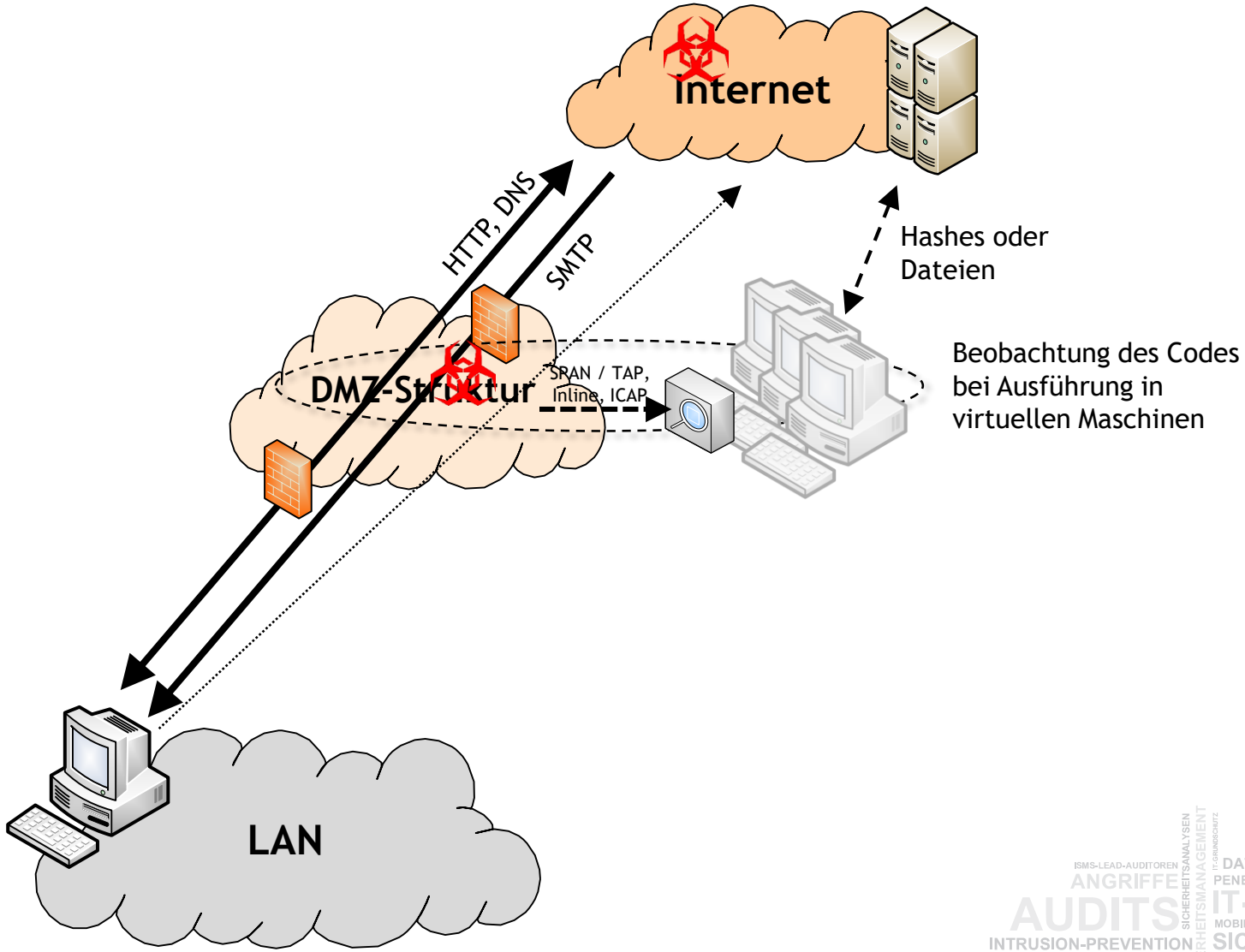
Aufbau der folgenden Folien

- Beschreibung einzelner funktionaler Bausteine
- Diese finden sich meist bei mehreren Herstellern
- Hersteller implementieren oft auch mehrere funktionale Bausteine innerhalb eines Produkts oder einer Produktfamilie

Erkennung von Malware: Sandbox-Analyse als Teilfunktion

cirosec

Bekannte Anbieter z.B.:
FireEye, Lastline, Fortinet,
Blue Coat, Trend Micro, AhnLab,
Palo Alto, Cisco Sourcefire,
Check Point, General Dynamics,
Zscaler, Cyphort



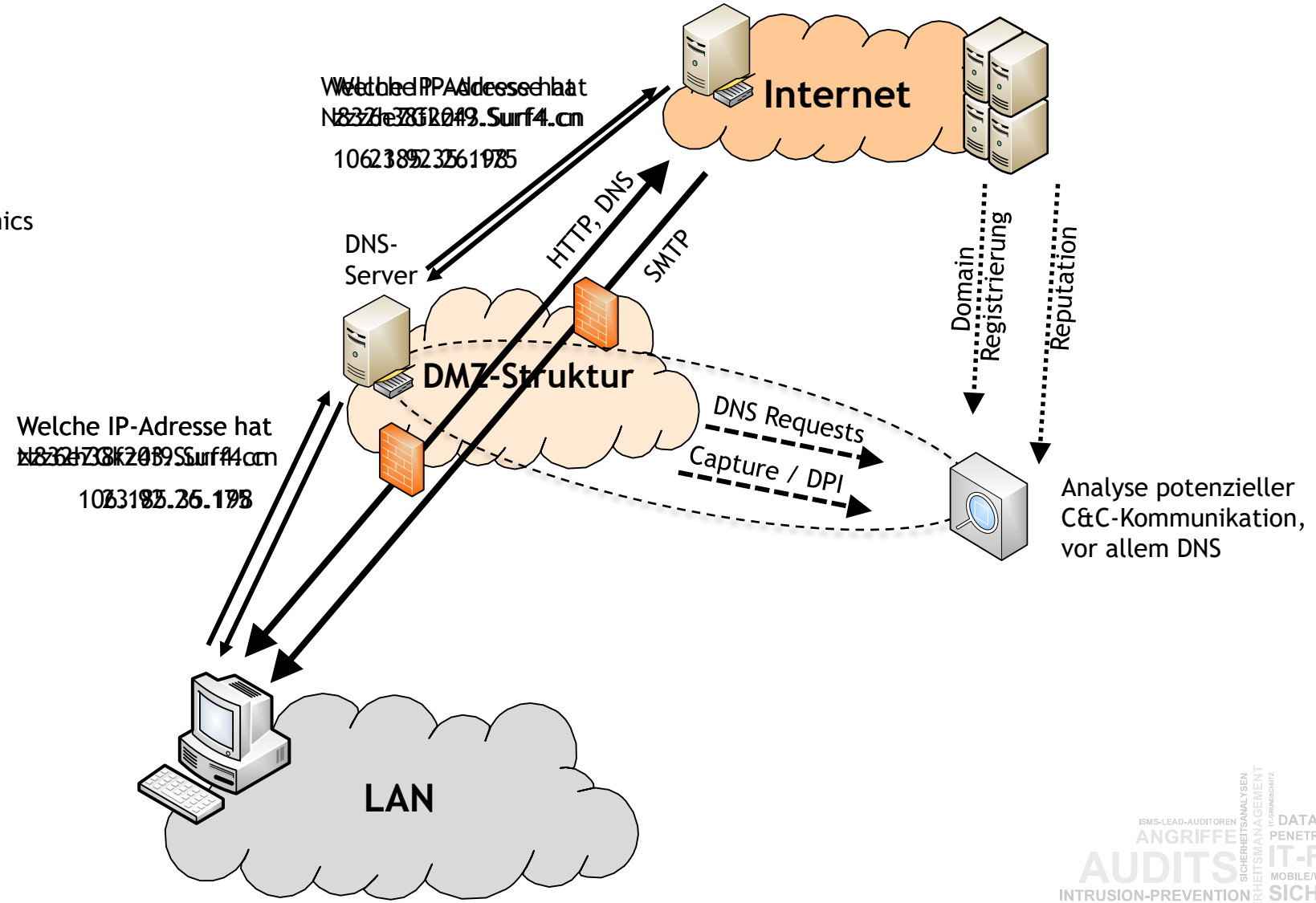
Tests im Rahmen einer Bachelor Thesis

cirosec

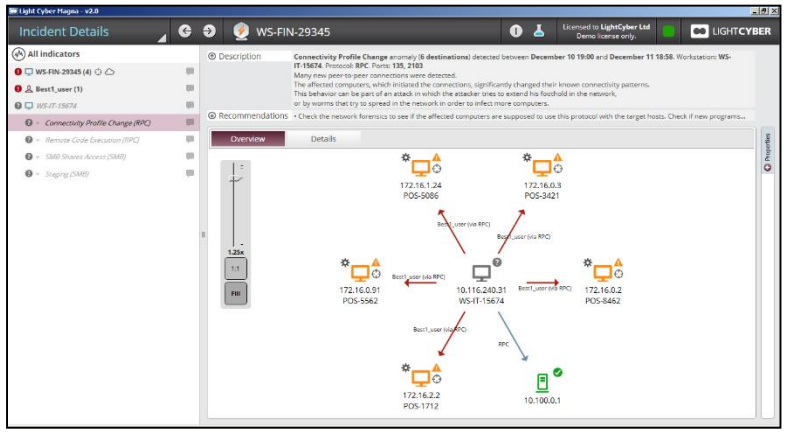
- Test-Malware
  - Verschlüsselter Content
    - sollte bereits als gefährlich erkannt werden
  - Entpackt mehrere Dateien
    - Exe + DLL
  - DLL Injection / Ausführung eines Keyloggers
    - Protokollierung aller Tastendrücke in eine Datei auf dem Desktop
- „Tarnfunktionen“
  - Schlafen für 10 Minuten in Einzelsekunden
  - Vortäuschen von Berechnungen
- Ergebnis
  - Cisco / Sourcefire FireAMP — nicht erkannt
  - Check Point Threat Emulation — nicht erkannt
  - Lastline — nicht erkannt
  - FireEye — keine Analyse gestartet
  - Palo Alto — nicht erkannt

Erkennen von C&C-Kommunikation

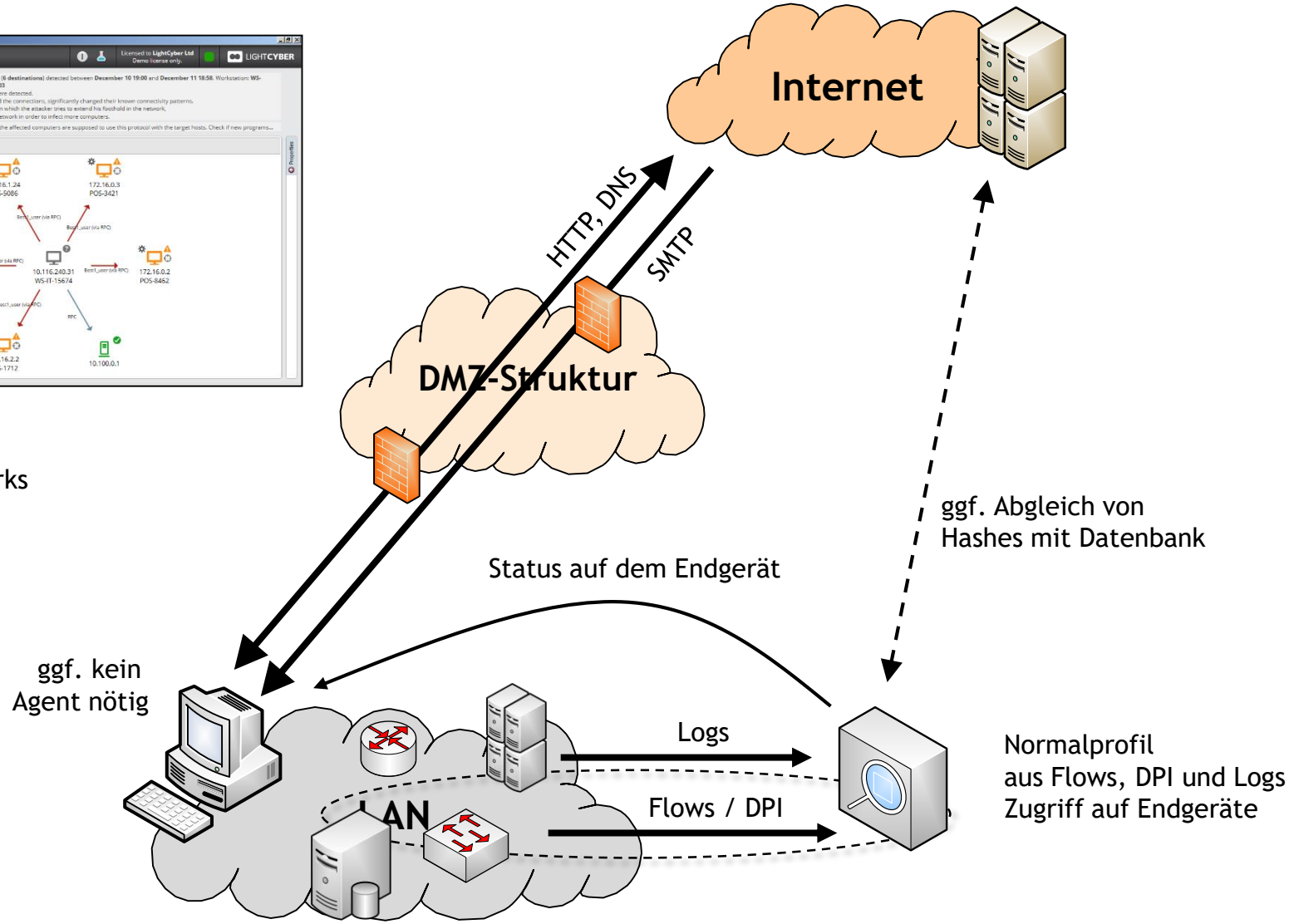
Bekannte Anbieter z.B.:
FireEye, Damballa,
Trend Micro, General Dynamics



Security / Behavioral Analytics



Bekannte Anbieter z.B.:
LightCyber, Vectra Networks
oder DarkTrace



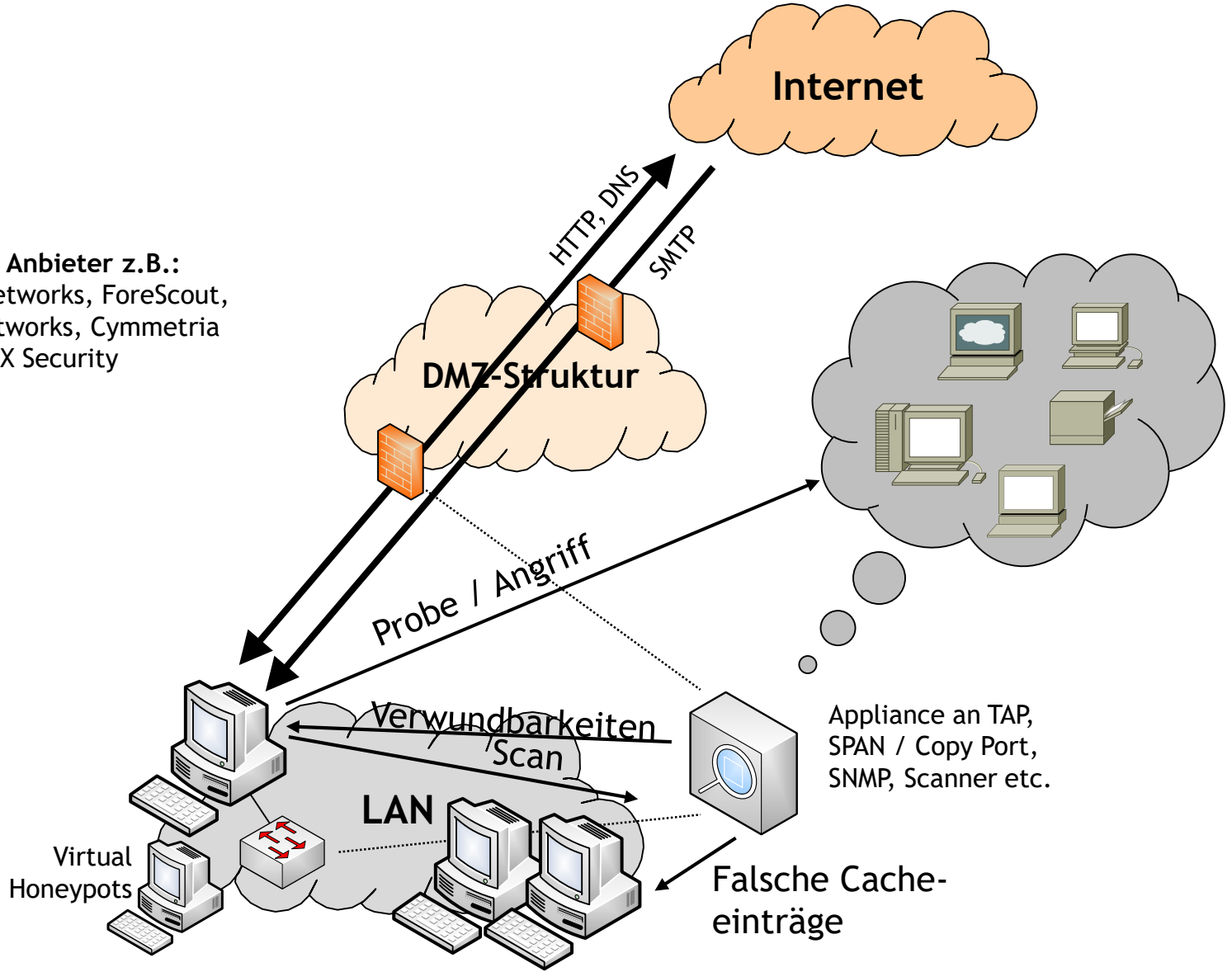
Einbruchserkennung mit Fallen

- Nutzung von Accounts
  - Domain_Admin_Temp, Passwort in der Beschreibung, Logon Hours 0
- Zugriff auf Shares / Dokumente
  - Fileshare „Password Audit 2015“
  - Excel-Files mit 4 MB, aber everyone:deny
- Spezielle interne (virtuelle) Server
  - Virtueller Server „BackupDB“ mit alter MySQL-Version
- Netzwerkzugriff
  - DHCP-Vergabe – neue MACs melden (nur in kleineren Netzen sinnvoll)
- Web-Applikationsebene
  - .HTACCESS auf Webserver mit Verweis auf passwd mit Fallen-Account
  - Debug=false in URL-Parameter einbauen
  - Versteckte Variable in HTML mit authenticated = 0

- Quelle:
  - Kundenprojekte, kommerzielle Lösung, Mubix, Jason Street, …

Deception / Honey Tokens

Bekannte Anbieter z.B.:
Illusive Networks, ForeScout,
Attivo Networks, Cymmetria
Oder TrapX Security



Erkennung in SCADA-Netzen

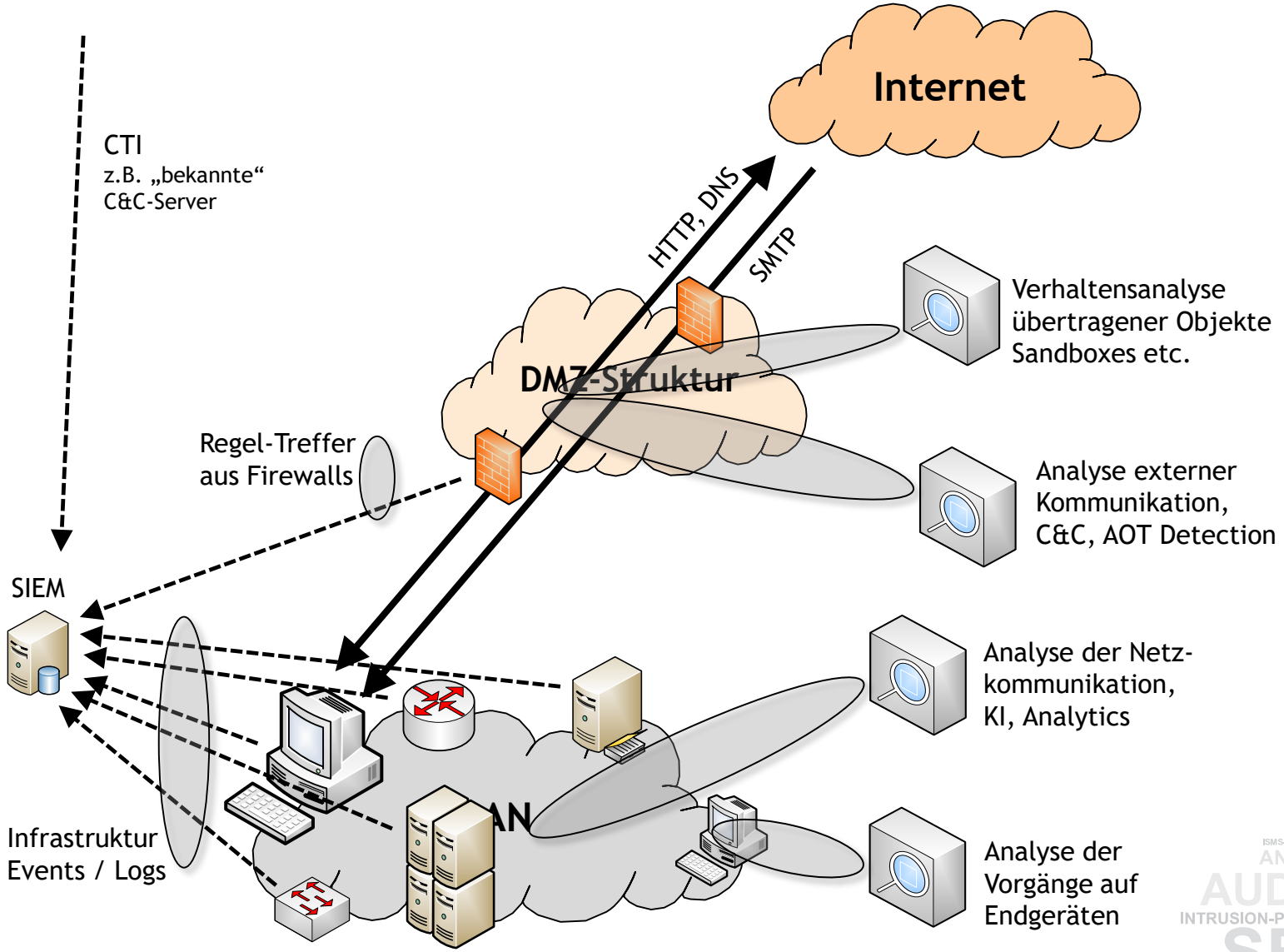
- Spezialisierte Anbieter
  - Analysieren zahlreiche Spezialprotokolle wie Modbus, DNP3, PROFINET, IEC 60870, 61850
  - Lernen das normale Kommunikationsverhalten
    - Wer spricht mit wem, über welche Funktionen und Register?
    - Timing der normalen Kommunikation
  - Abweichungen / Anomalien werden erkannt und alarmiert

Bekannte Anbieter z.B.:
CyberX, radiflow, Rhebo,
NexDefense, CyberBit, SCADAFence
oder Security Matters

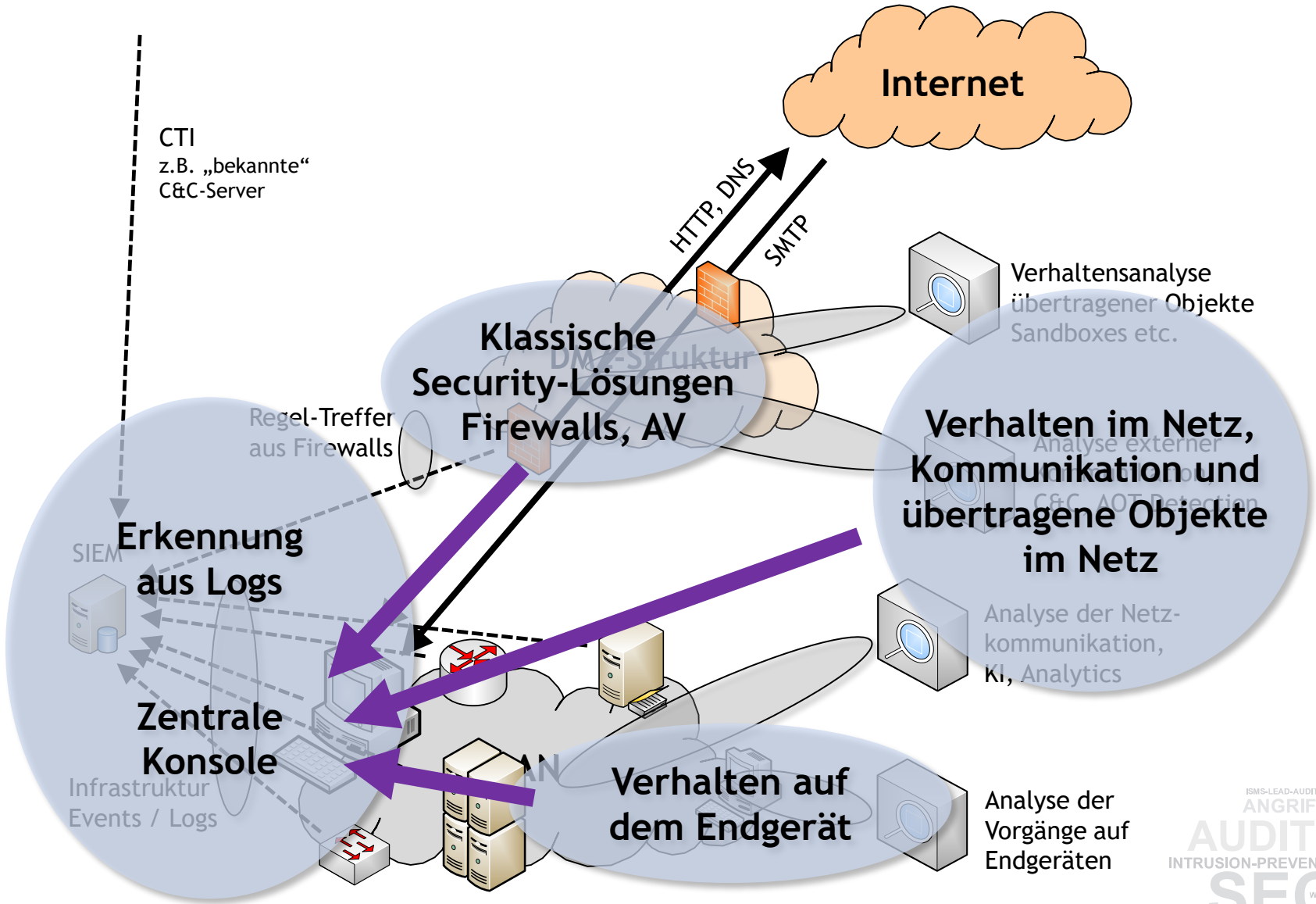
SIEM / Security Analytics mit Logs?

- Reicht es aus, die Logs / Events klassischer Systeme zu korrelieren?
  - In der Regel fehlen
    - interessante Events
    - Kontext
  - Auch Big-Data-Techniken können nichts herbeizaubern
  - Moderne Security-Analytics-Werkzeuge sind eine Perspektive, doch auch hier werden sinnvolle Ausgangsdaten benötigt

Erkennungstechnik im Gesamtbild



Erkennungstechnik im Gesamtbild



Grundsätzliches Problem

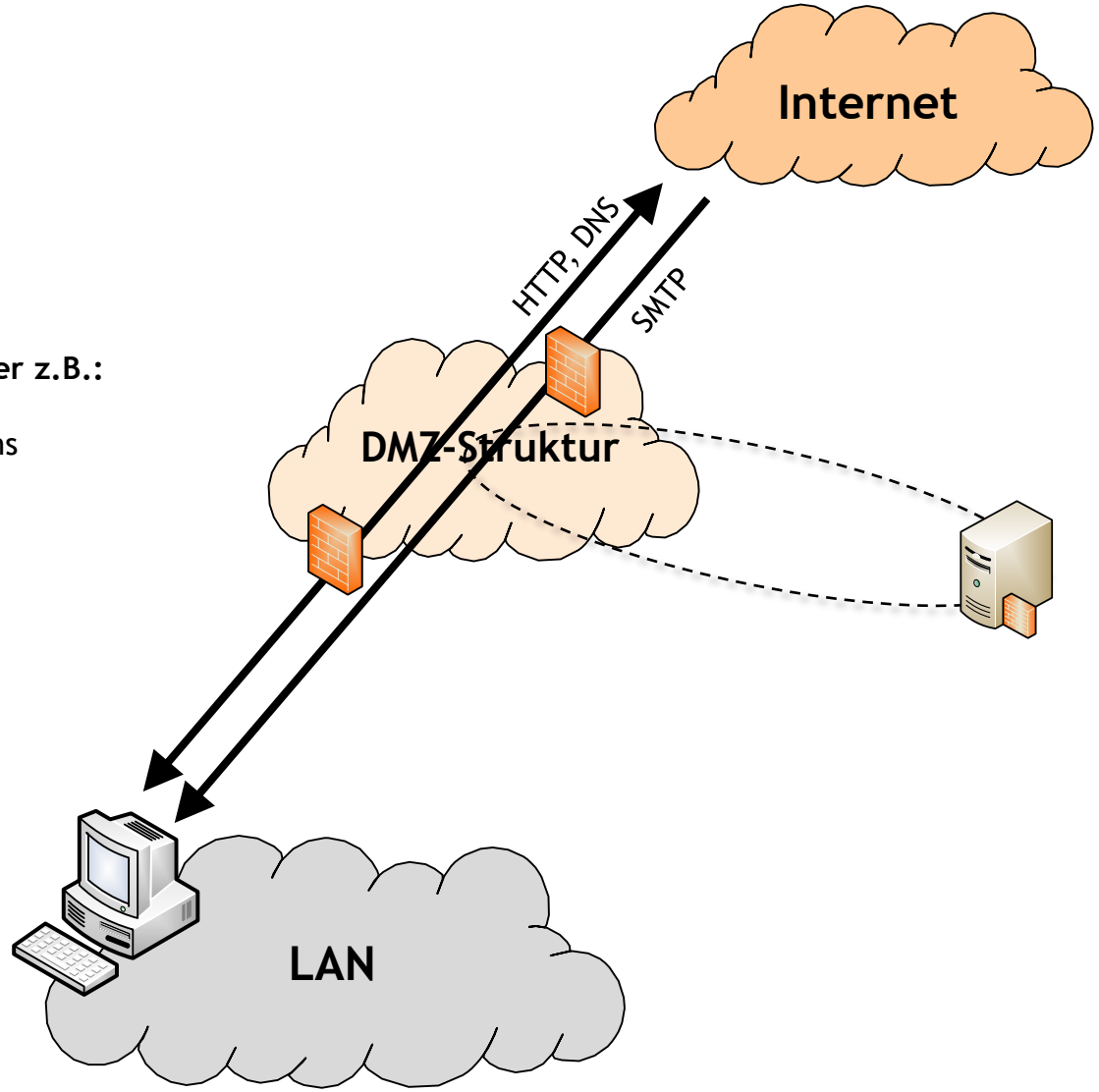
cirosec

- Erkennung hinkt immer hinter den Angriffen her
  - Man erkennt alte bzw. typische Verhaltensmuster
  - Der Angreifer muss Fehler machen, um erkannt zu werden

- Prävention vs. Detektion
  - Kenntnis über die Detektionsmuster reicht aus, um sich als Angreifer anders zu verhalten
  - Kenntnis von Präventionsmechanismen reicht nicht aus
    - Der Hersteller muss einen Fehler gemacht haben, der bekannt wird

- Prävention mag alleine nicht ausreichen, aber:
  - Wie weit haben wir sie ausgeschöpft?
  - Wie wirtschaftlich sind Erkennung und Reaktion, wenn große Lücken in der Prävention vorhanden sind?

Sanitisierung



Bekannte Anbieter z.B.:
Votiro, Sasa,
Glasswall Solutions

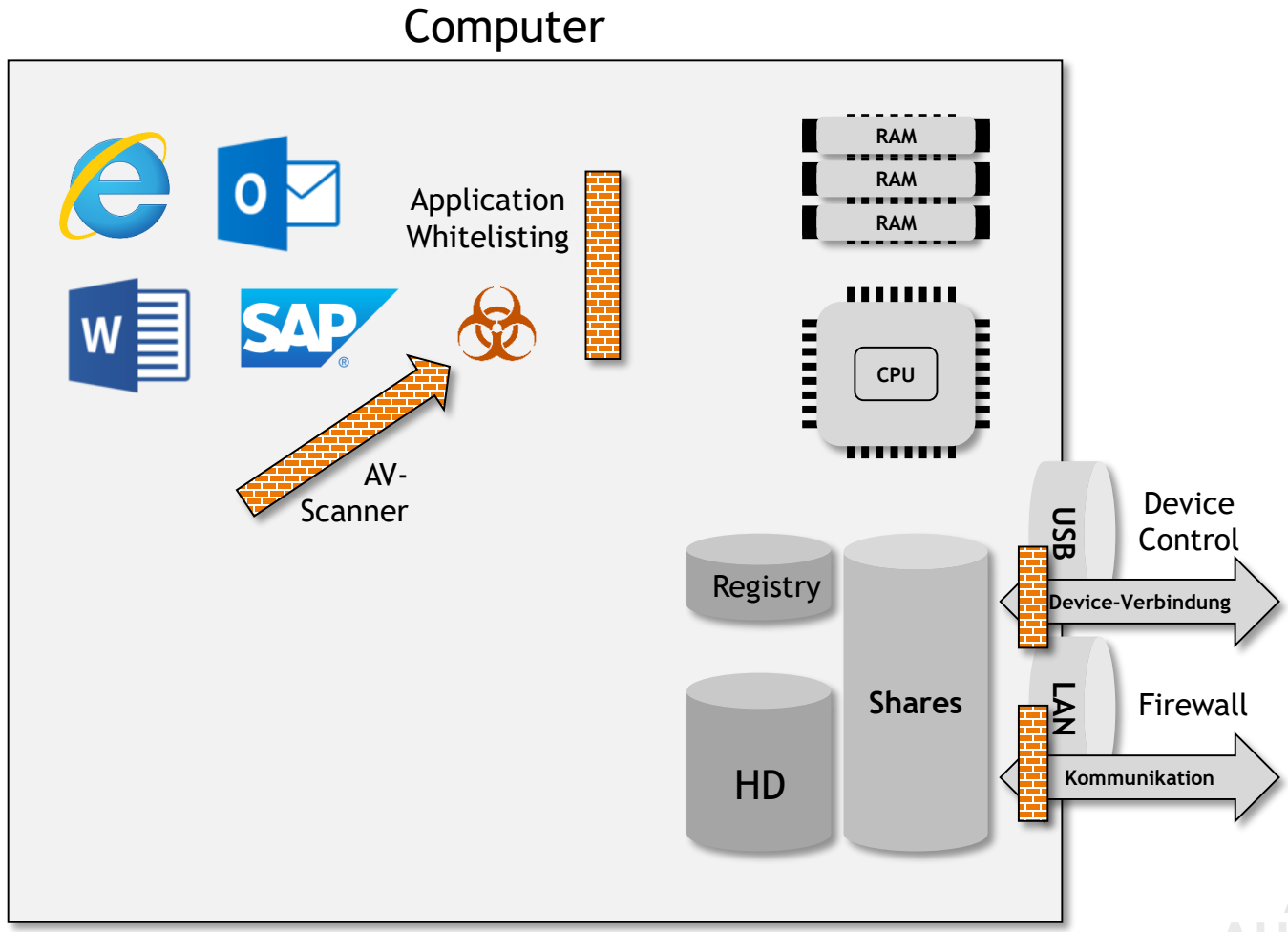
Zerlegen und
neu zusammensetzen
von Objekten

cirosec

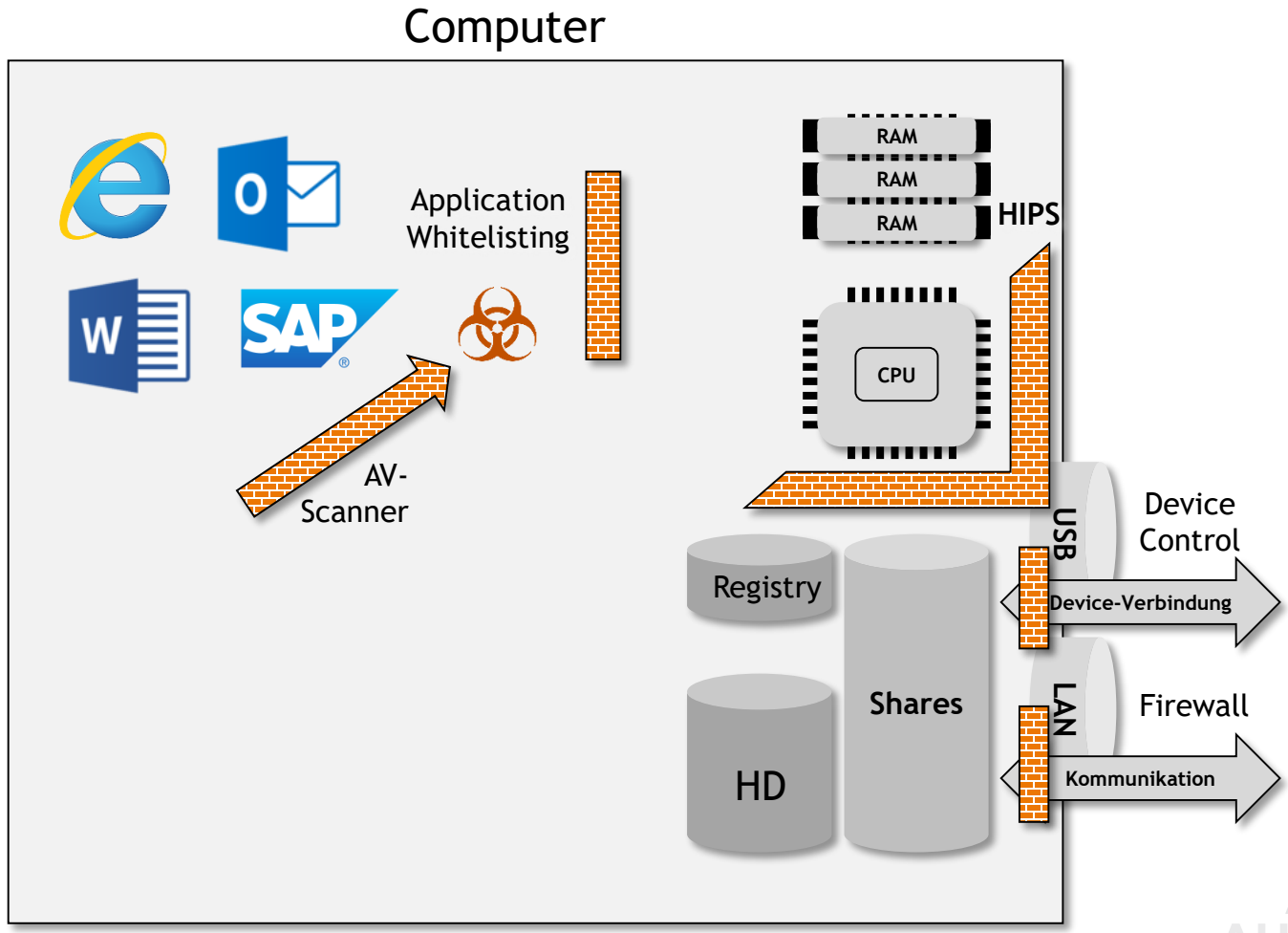
ISMS-LEAD-AUDITOREN
ANGRIFFE
AUDITS
RUSION-PREVENTION
SECURITY
WLAN
SICHERHEITSANALYSEN
SICHERHEITSMANAGEMENT
IT-GRUNDSCHUTZ
DATA LOSS PREVENTION
PENETRATIONSTEST
IT-FORENSIK
MOBILE/WIRELESS SICHERHEIT
SICHERHEIT SENSIBLER DATEN
APPLIKATIONS-SICHERHEIT
NETZWERKSICHERHEIT
INTERNET SICHERHEIT

Fokus auf die Endgeräte

Klassische Ansätze auf dem Endgerät

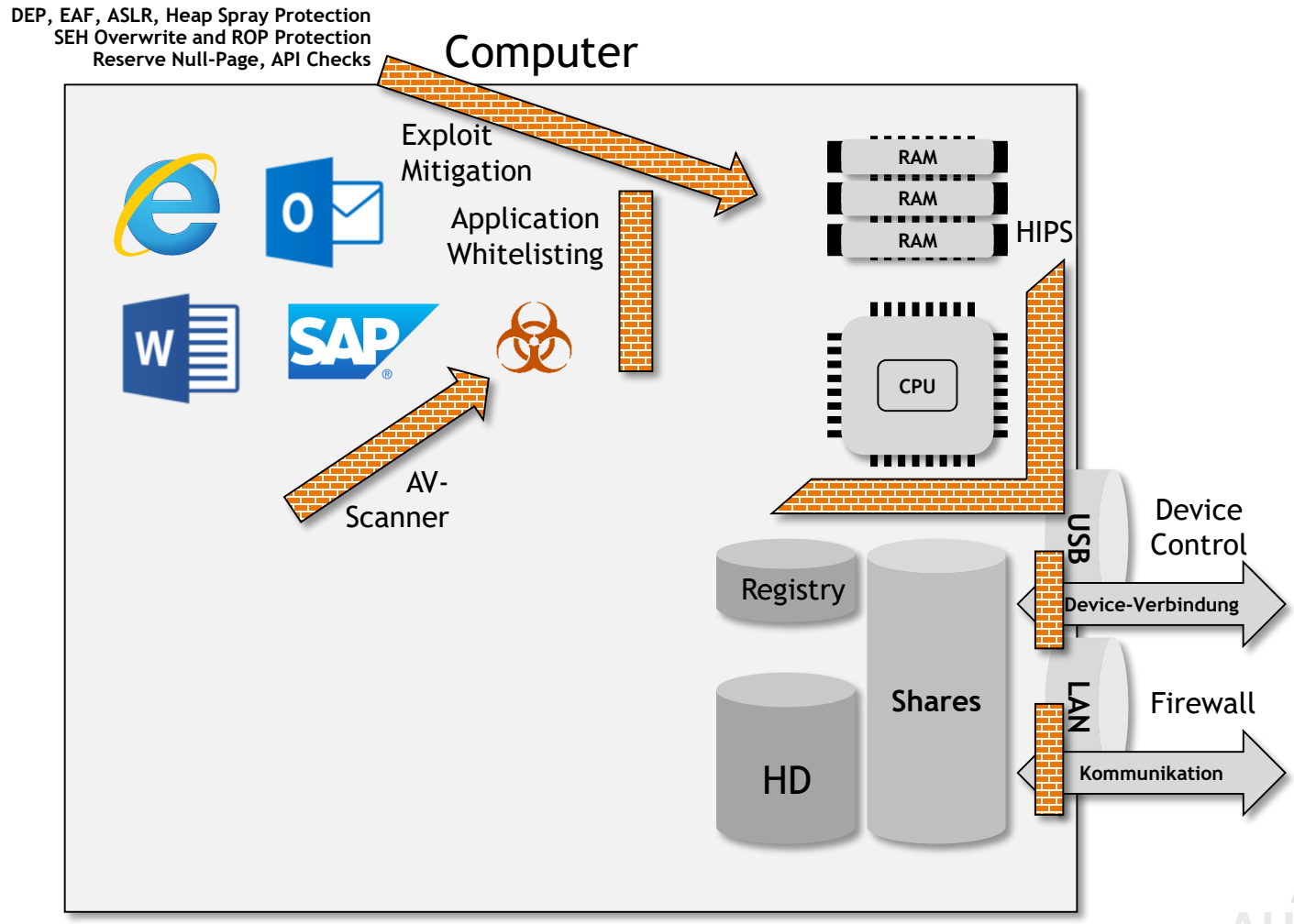


Klassische Ansätze und HIPS



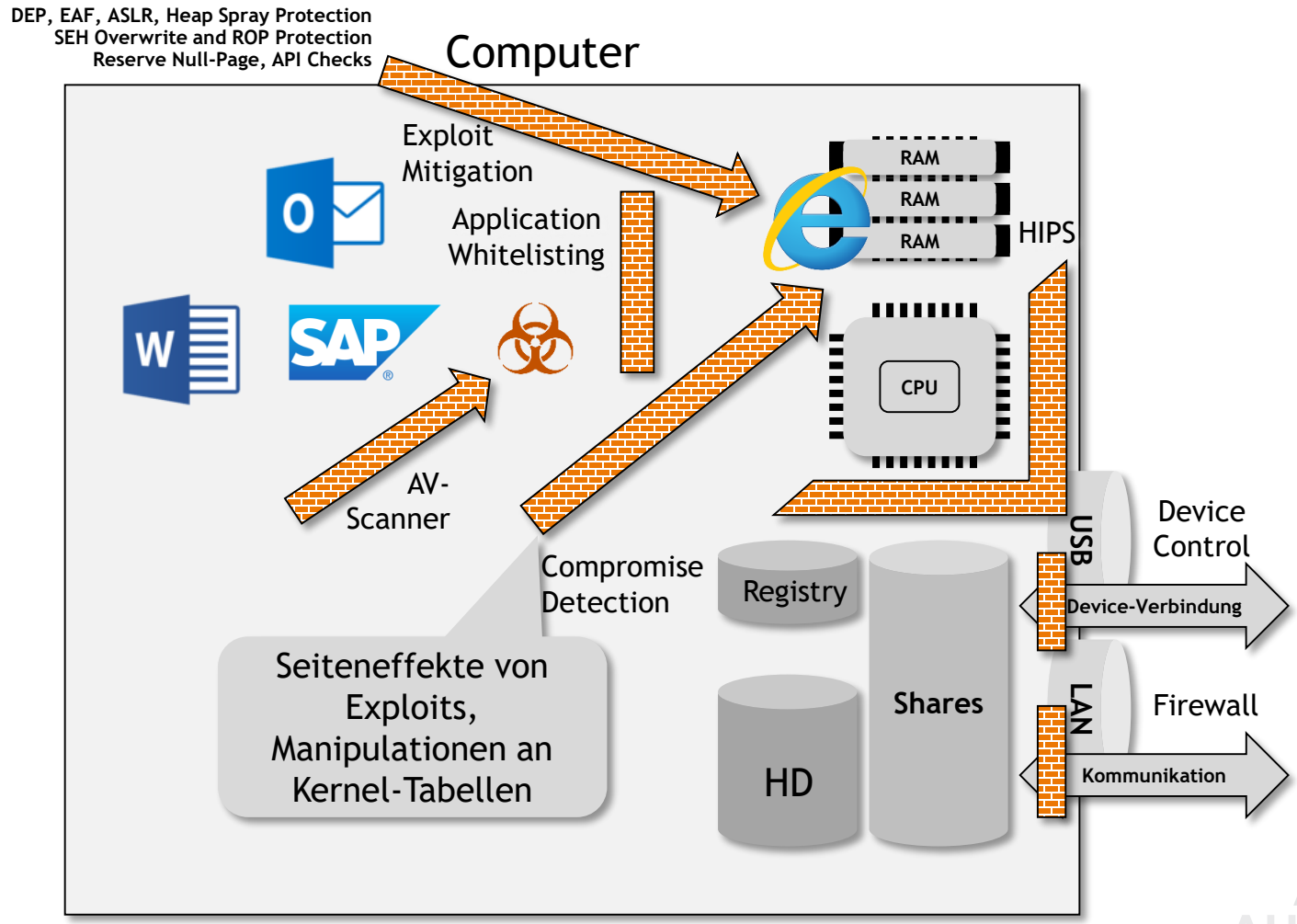
Bekannte Anbieter z.B.:
Symantec
(ehemals Platform Logic)
McAfee
(ehemals Entercept)
Ehemals Okena

Exploit Mitigation



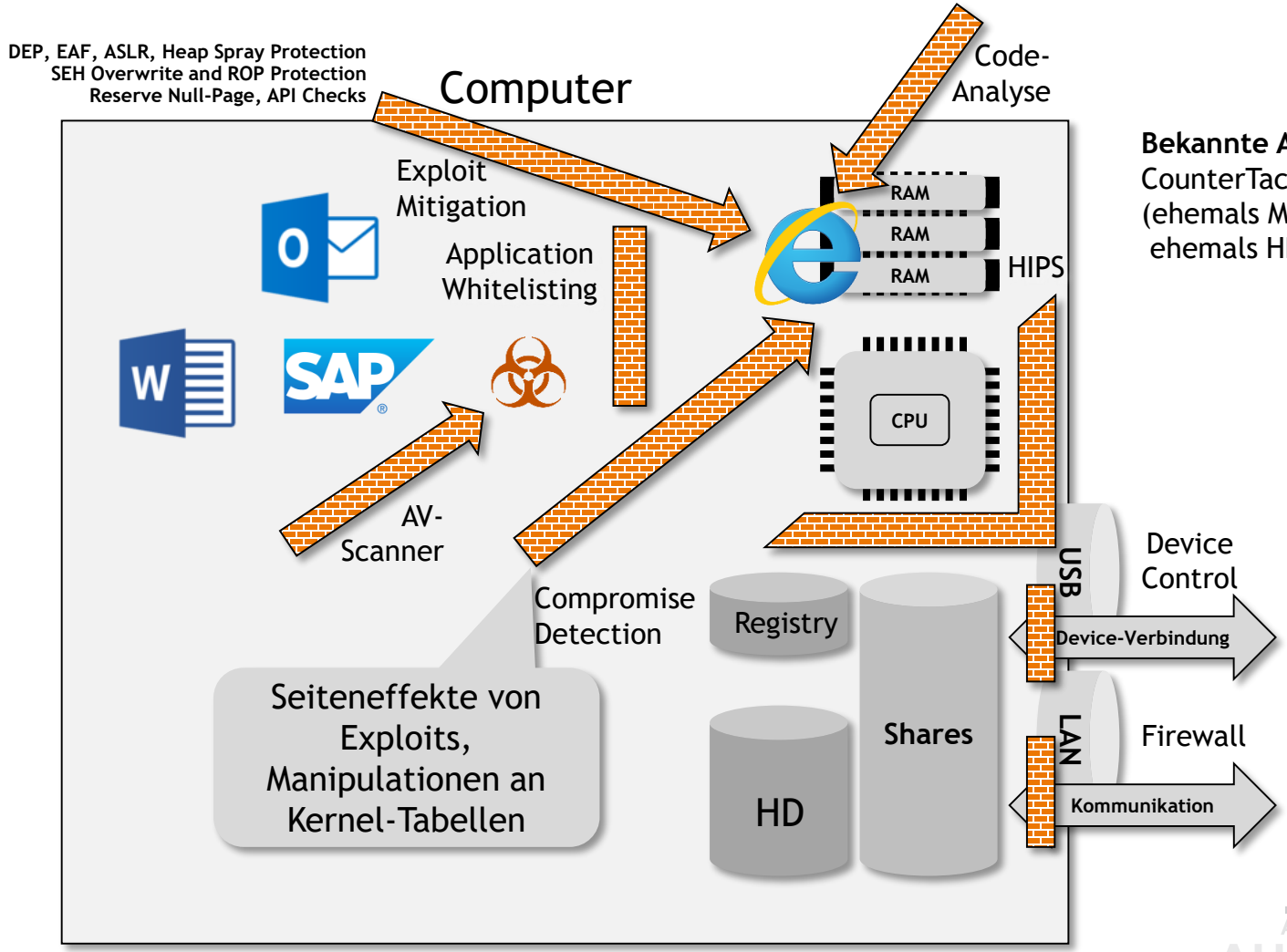
Bekannte Anbieter z.B.:
Palo Alto - Traps
(ehemals Cyvera)
Microsoft - EMET

Varianten der Hauptspeicheranalyse



Bekannte Anbieter z.B.:
RSA – ECAT
(ehemals Silicium Security)

Code-Analyse



Bekannte Anbieter z.B.:
CounterTack
(ehemals ManTech,
ehemals HB Gary)

Code-Analyse – Digital DNA

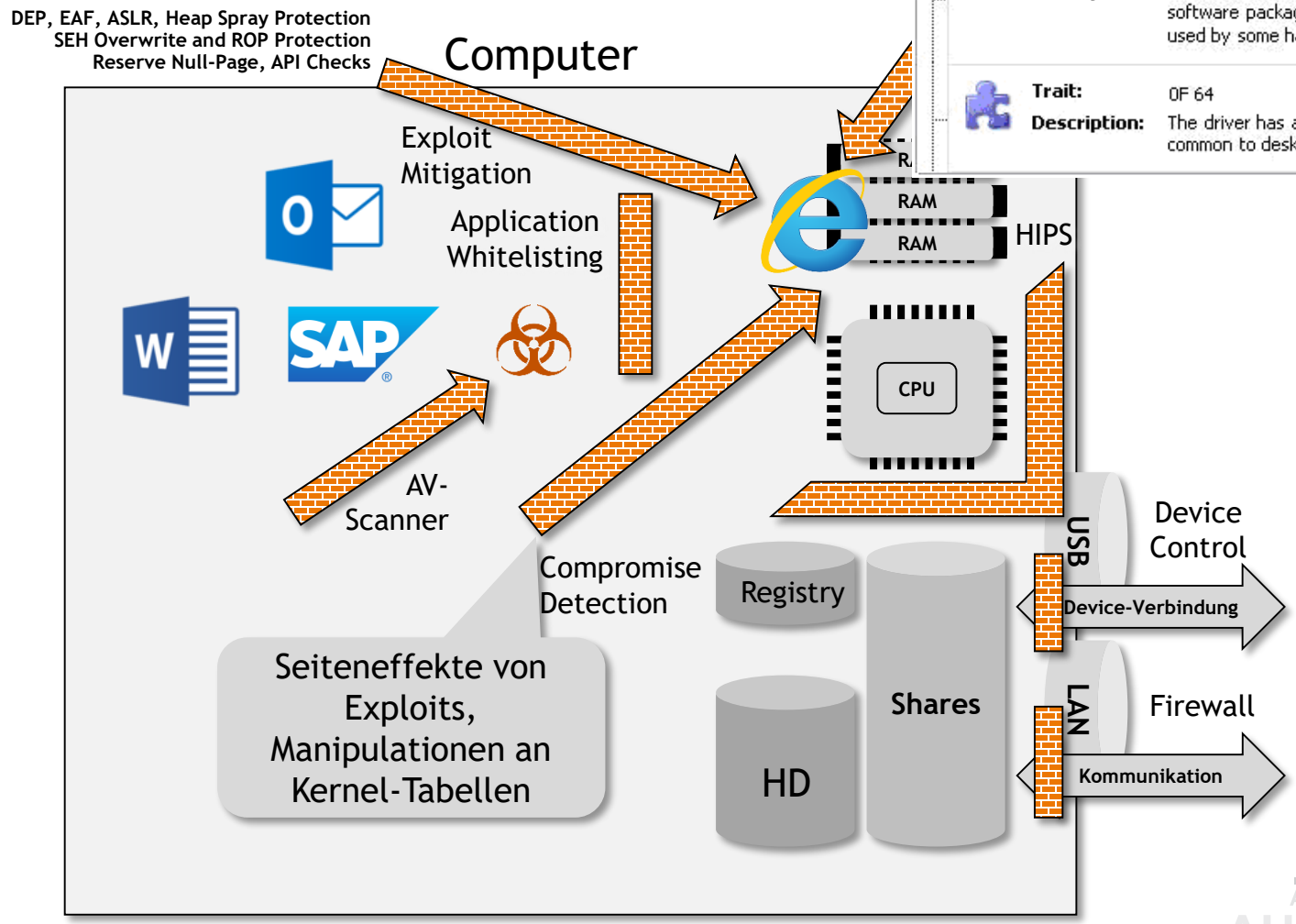
Digital DNA Sequence	Module	Process	Severity	Weight
0B 8A C2 05 0F 51 03 0F 6...	iimo.sys			
0B 8A C2 02 21 3D 00 08 63	ipfltdrv.sys			
0B 8A C2	intelppm.sys			
05 19 34 2F 57 42 00 7E 1...	ks.sys			
02 21 3D 2F 1C FD 00 08 63	ipnat.sys			

Trait

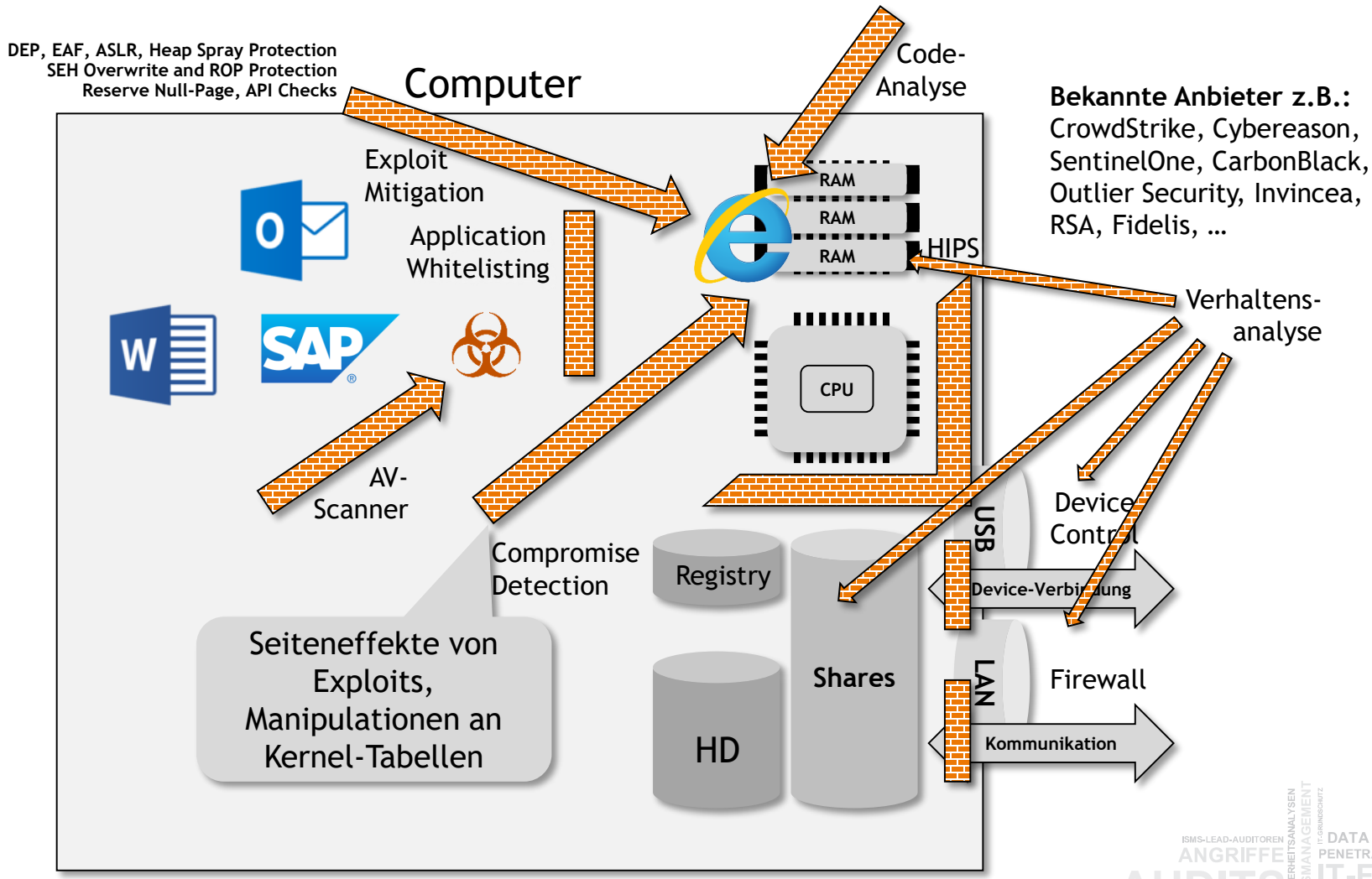
Trait: 8A C2
Description: The driver may be a rootkit or anti-rootkit tool. It should be examined in more detail.

Trait: 0F 51
Description: There is a small indicator that detour patching could be supported by this software package. Detour patching is a known malware technique and is also used by some hacking programs and system utilities.

Trait: 0F 64
Description: The driver has a potential hook point onto the windows TCP stack. This is common to desktop firewalls and also a known rootkit technique.

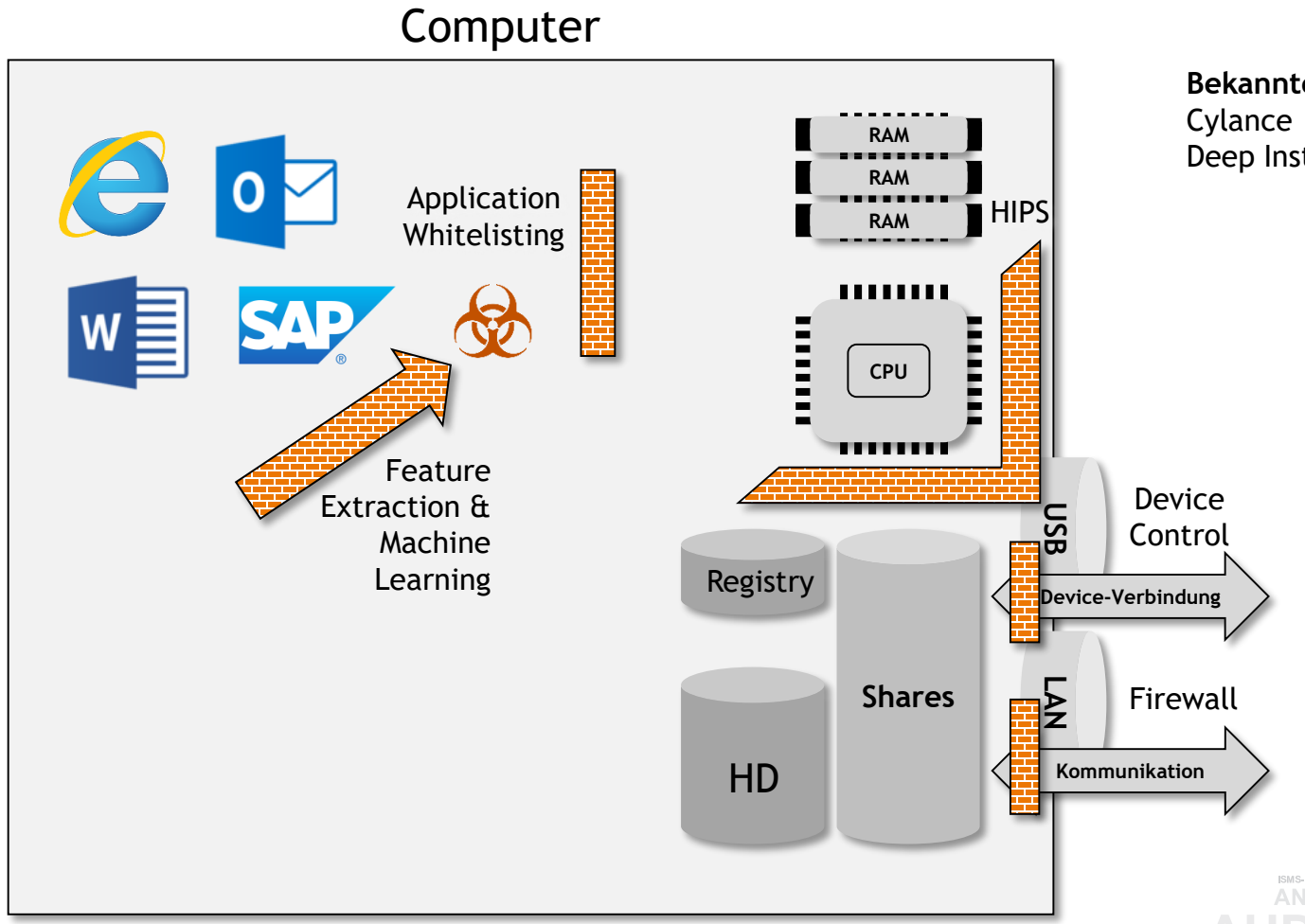


Verhaltensanalyse



Bekannte Anbieter z.B.:
CrowdStrike, Cybereason, SentinelOne, CarbonBlack, Outlier Security, Invincea, RSA, Fidelis, …

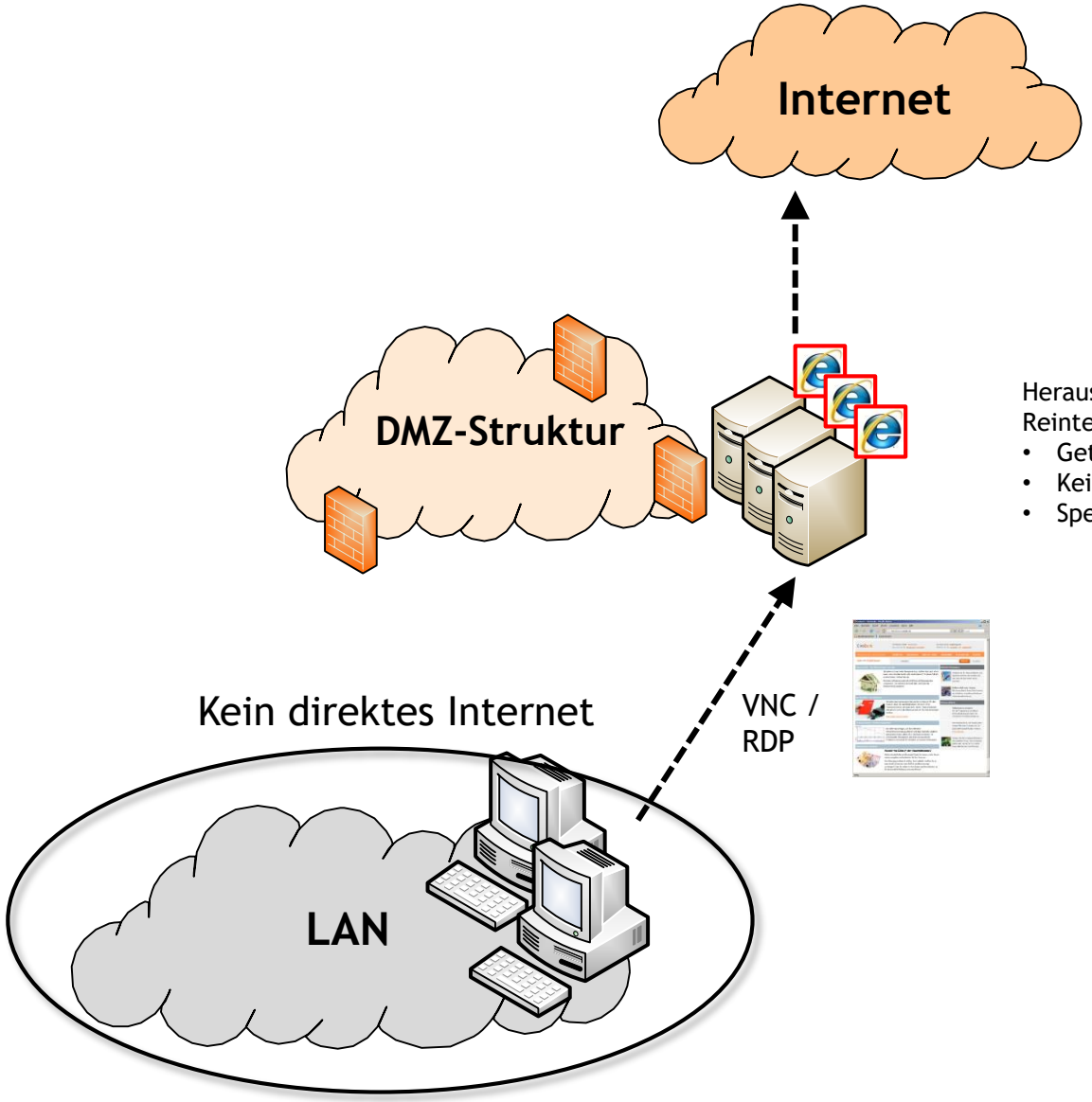
AV Reborn? Next-Generation AV?



Bekannte Anbieter z.B.:
Cylance
Deep Instinct

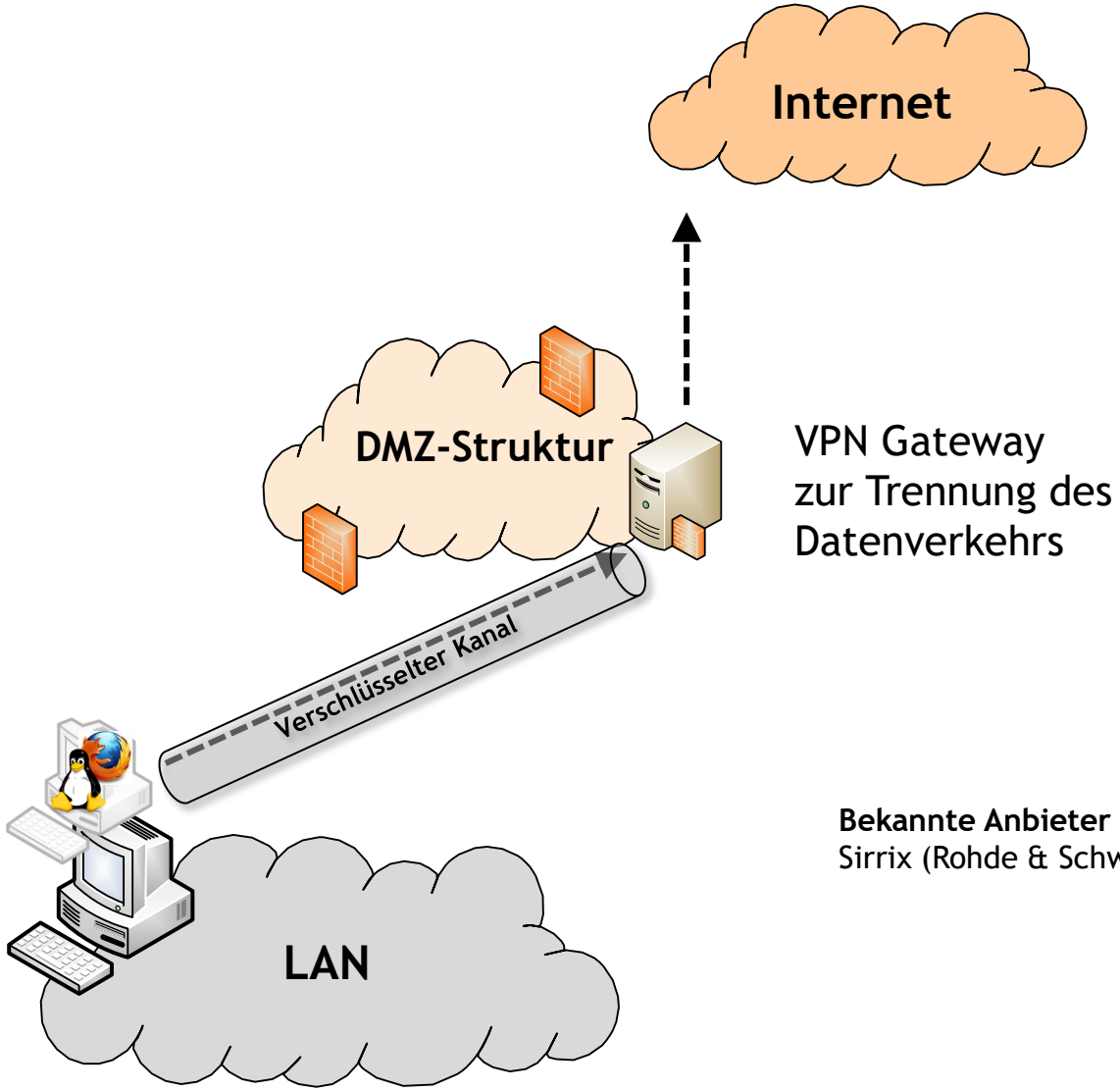
Isolation der Internetnutzung mit „ReCoBS“ o.ä.

Bekannte Anbieter z.B.:
Fireglass, m-privacy, Spikes, Menlo, Digital Guardian, BrowserBlade



Herausforderung:
Reintegration / „User Experience“
- Getrennte Browser?
- Kein spürbarer Unterschied?
- Speichern / Downloads

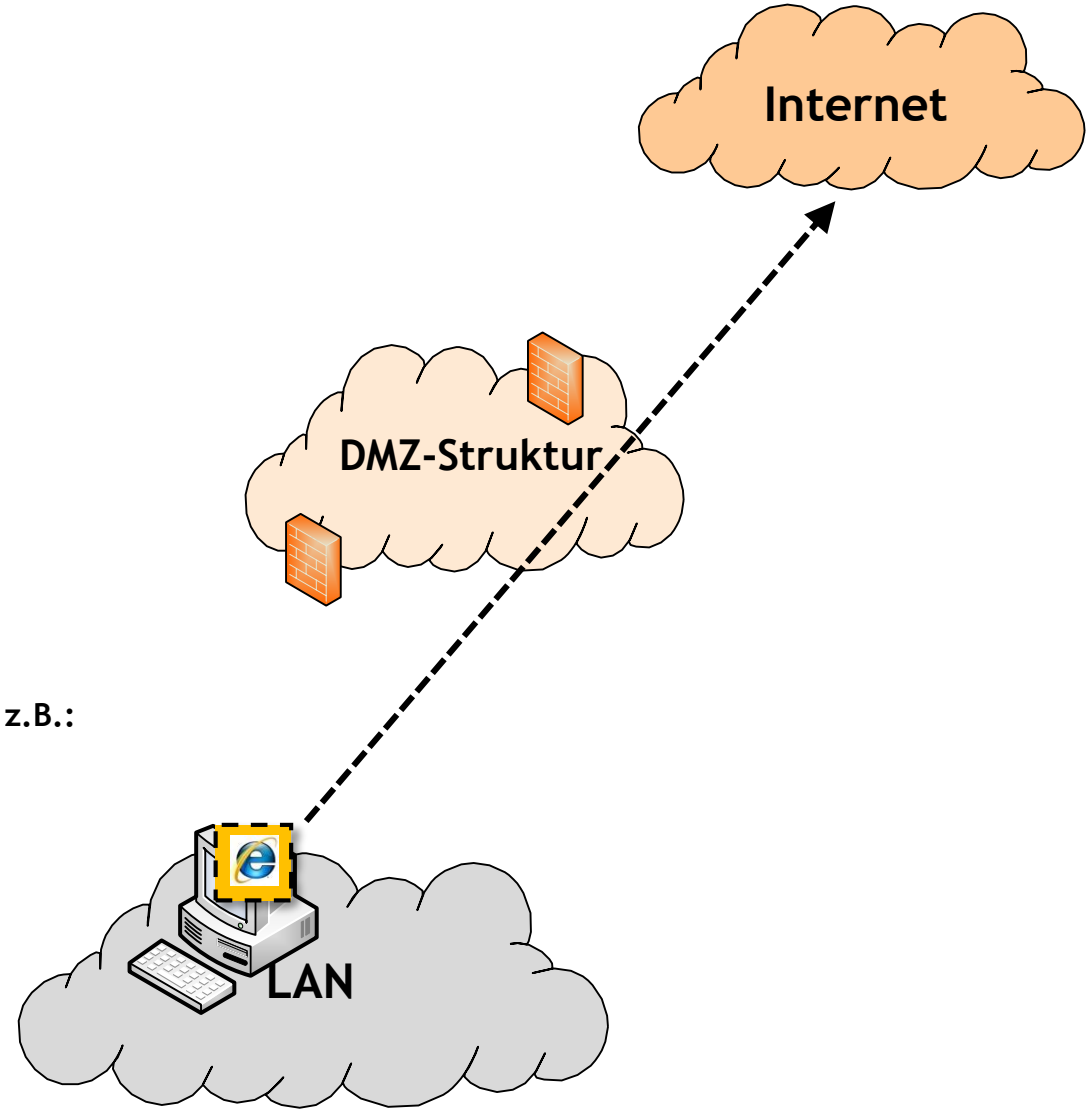
Separate virtuelle Maschinen zur Isolation der Internetnutzung



VPN Gateway
zur Trennung des
Datenverkehrs

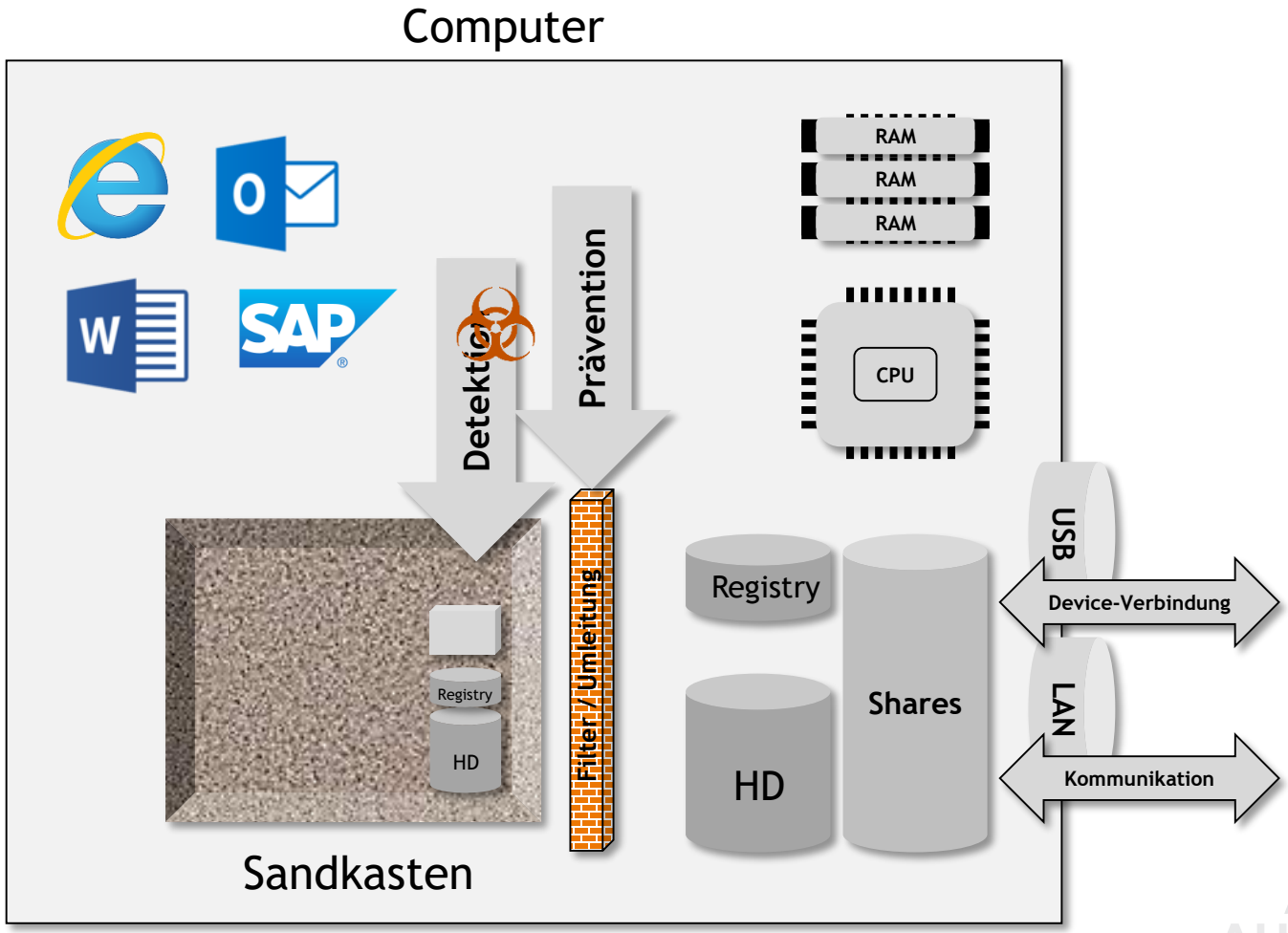
Bekannte Anbieter z.B.:
Sirrix (Rohde & Schwarz)

Sandboxing zur Isolation der Internetnutzung

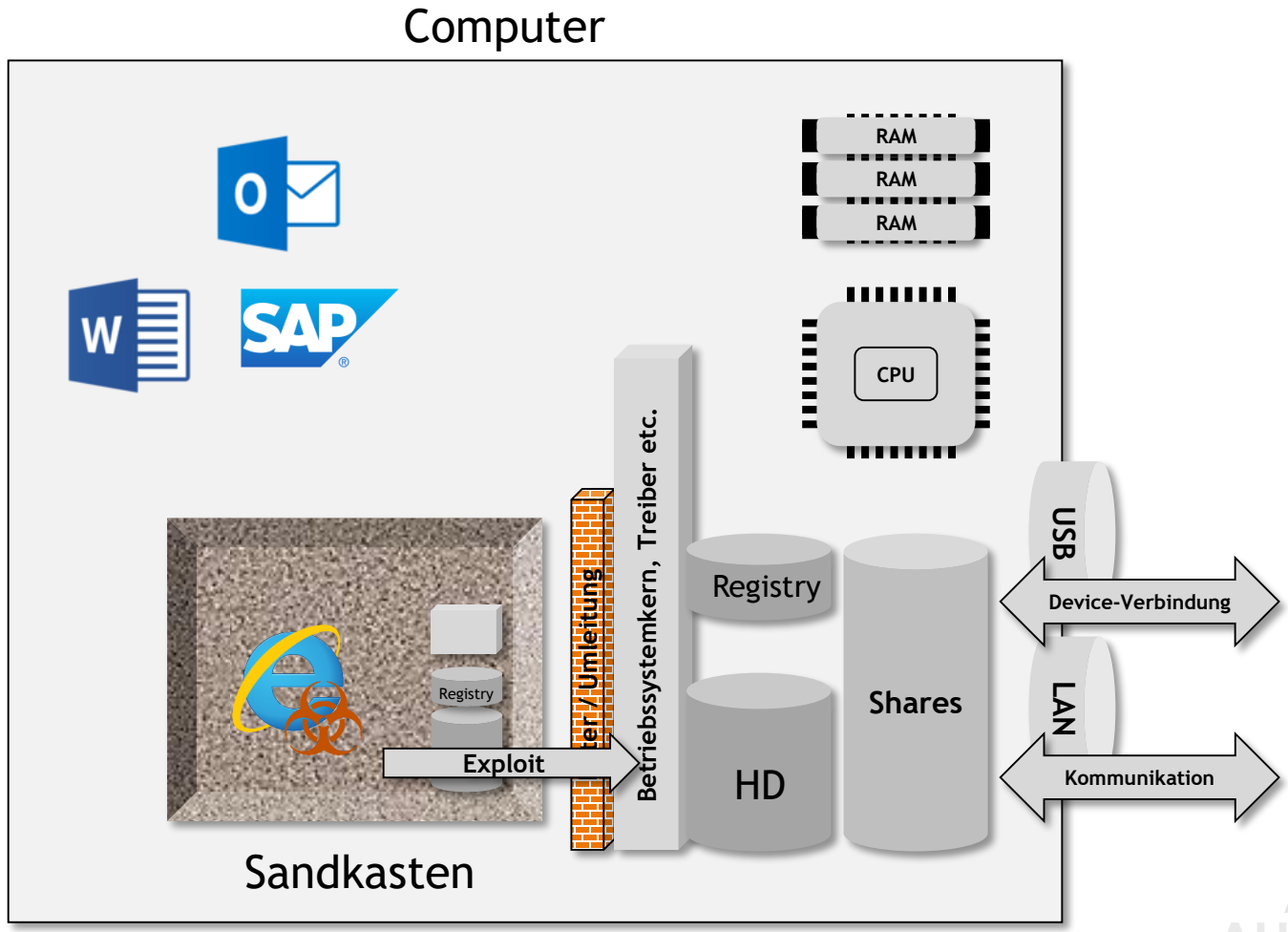


Bekannte Anbieter z.B.:
Invincea, Trustware

Grundidee von Sandboxen

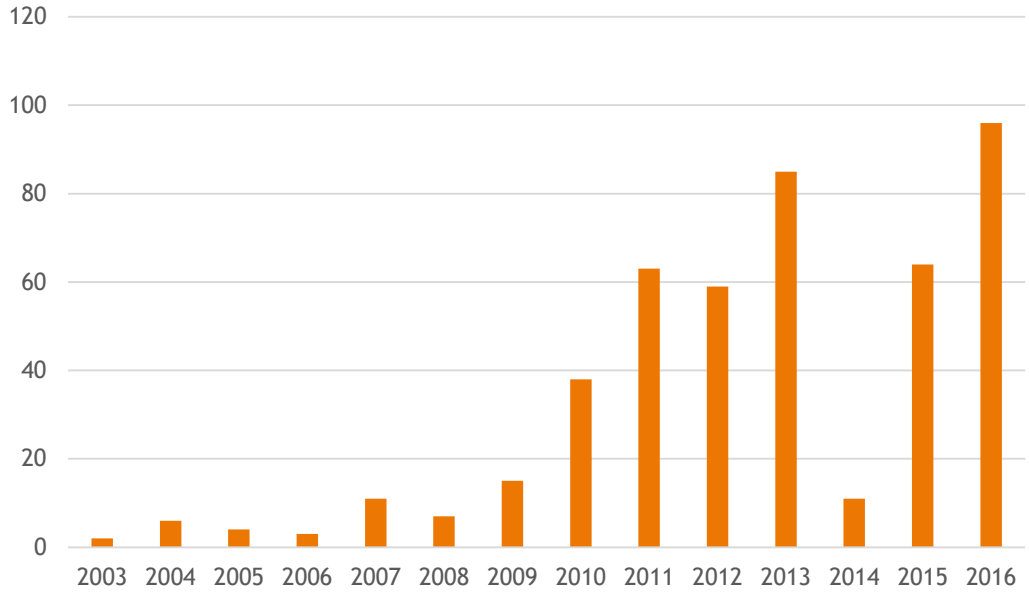


Grenze von Sandboxen



Sicherheit von Sandboxen heute: Windows Kernel CVEs seit 2003

cirosec



- 400+ Microsoft Kernel CVE's seit 2010
- Viele wurden / werden bereits ausgenutzt
  - z.B. Stuxnet, Duqu, Gapz, Gameover, CVE-2013-5065 (NDProxy.sys), TDL4 etc.

Quelle: https://web.nvd.nist.gov, Stand 13.1.17

Mikrovirtualisierung

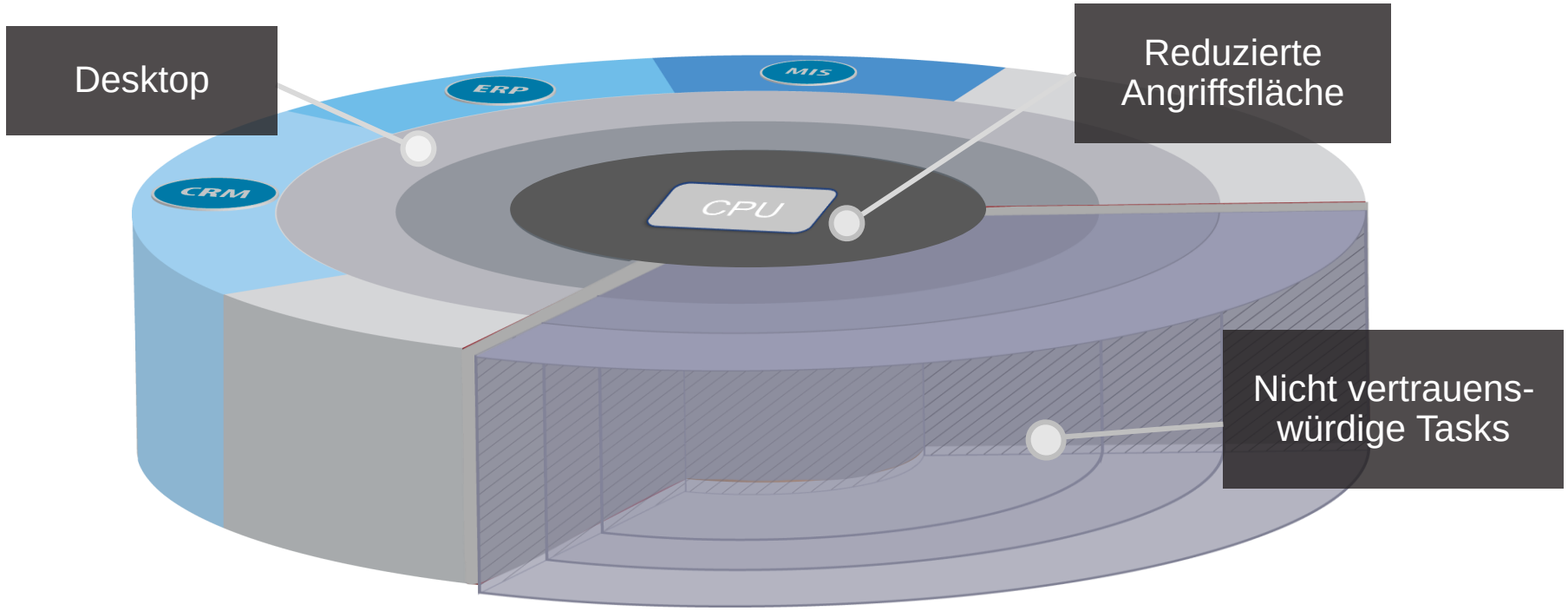
Bromium®

cirosec

- Weiterentwicklung der Hypervisor-Technik zu einem Microvisor
  - Ian Pratt und Simon Crosby (Mitgründer von XenSource)

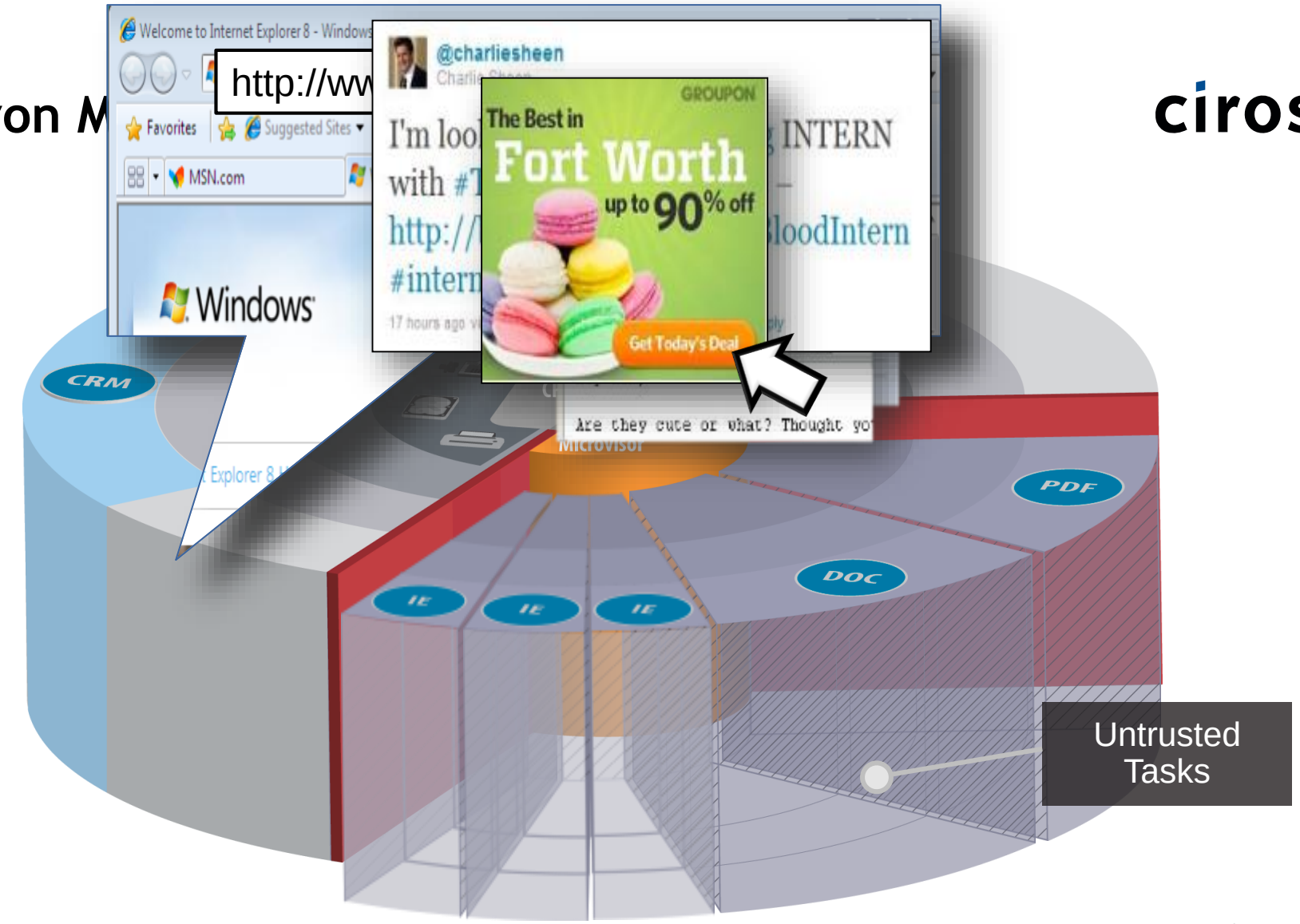
- Isolation auf dem Endgerät statt Erkennung
- Task-Isolation statt Applikationen oder Betriebssysteme
- Verwendet Hardware-Funktionen für Virtualisierung
- Micro-VM Inspection

Grundidee von Mikrovirtualisierung



Microvisor isoliert nicht vertrauenswürdige Tasks voneinander und vom Betriebssystem

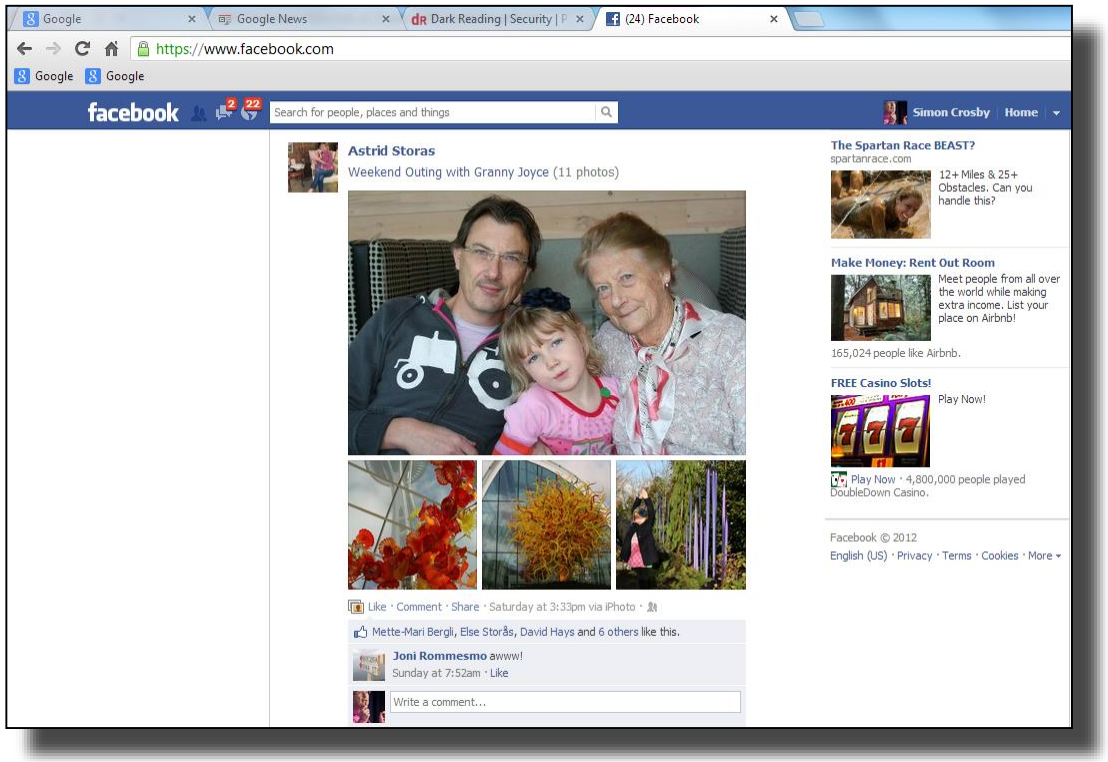
Grundidee von M



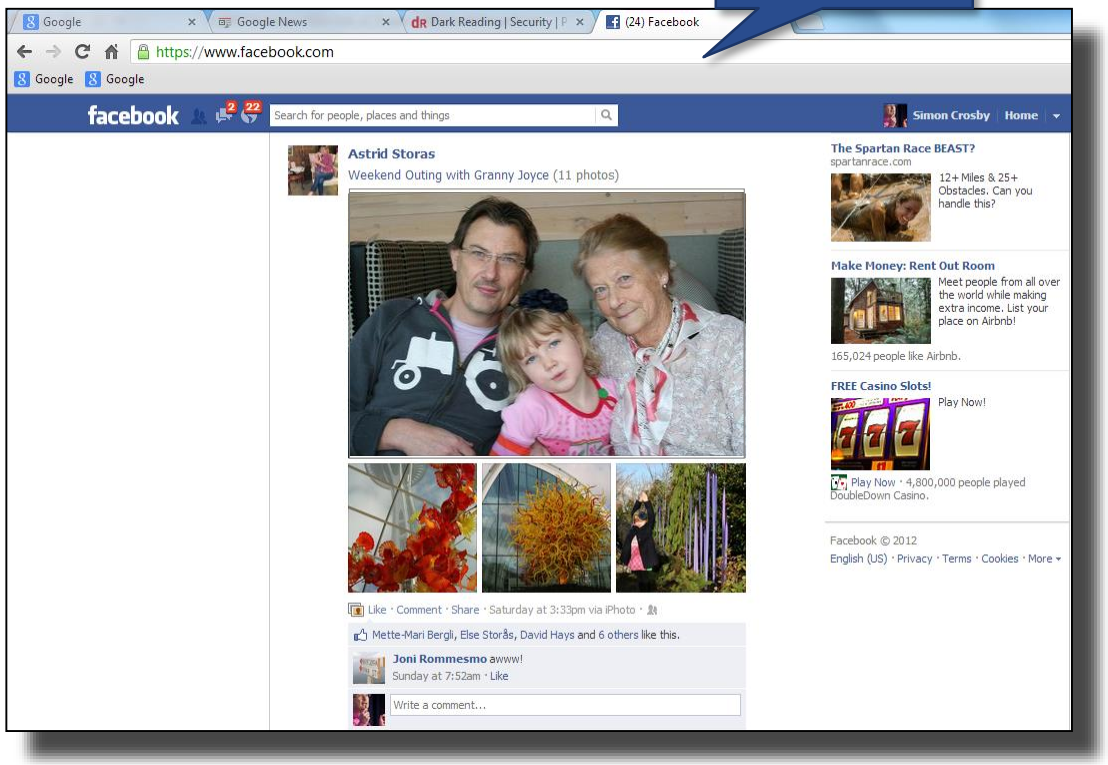
Jeder nicht vertrauenswürdige Task wird sofort in einer Micro-VM isoliert. Für den Benutzer ist dies nicht sichtbar.

Least Privilege für Micro-VMs

cirosec



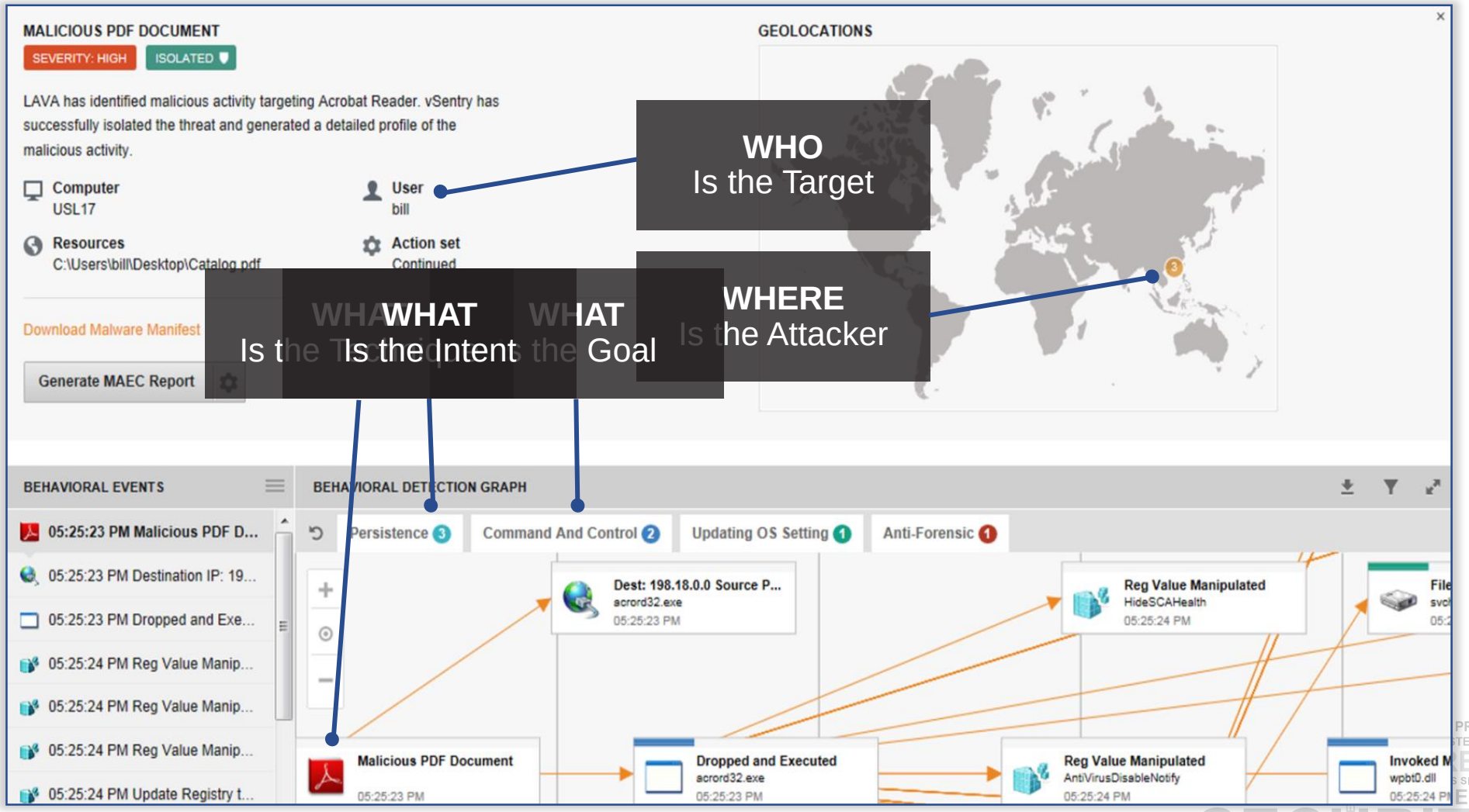
Speicherung von Daten?



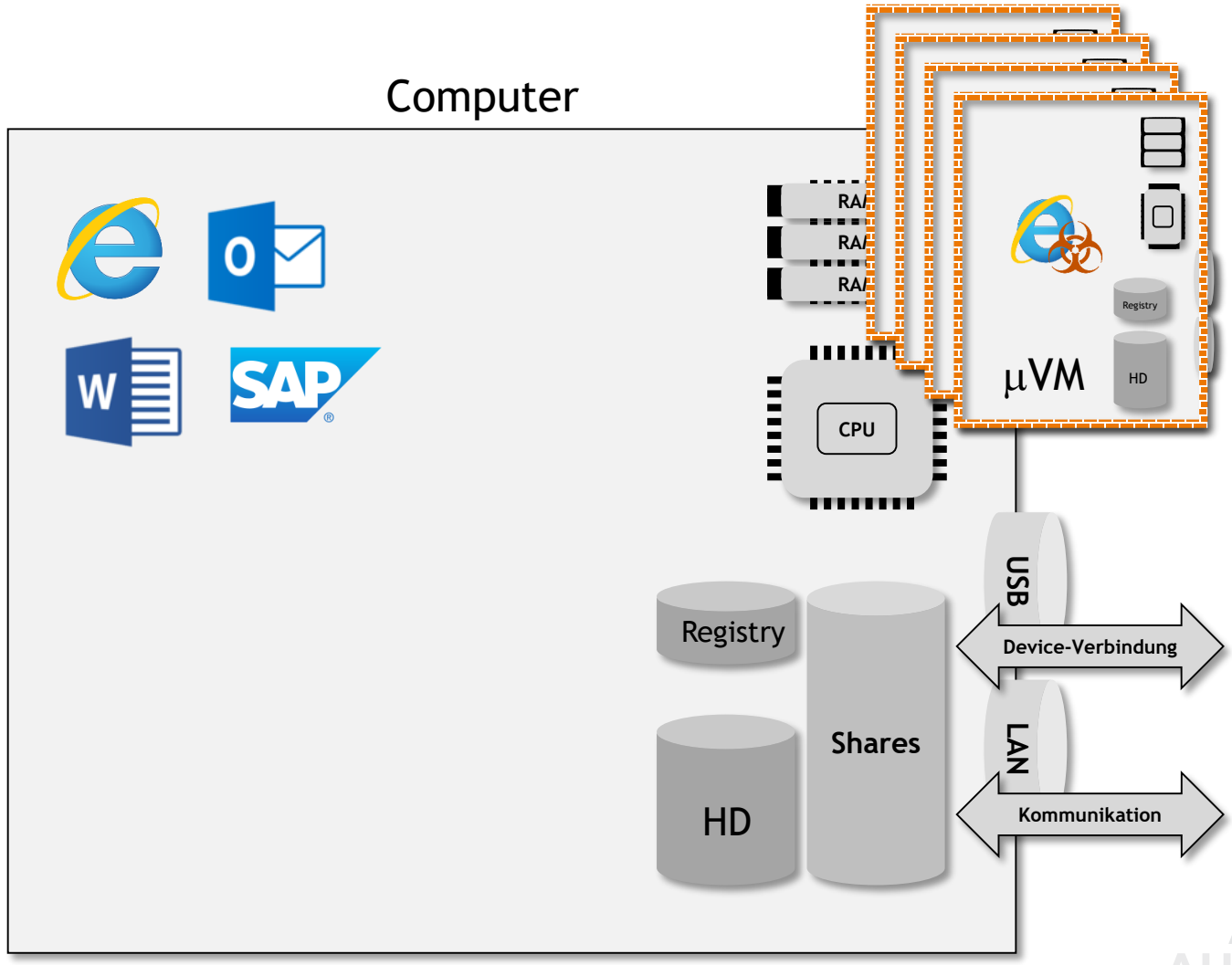
Untrusted

LAVA - Understanding the Kill Chain

cirosec



Mikrovirtualisierung



cirosec

ISMS-LEAD-AUDITOREN
ANGRIFFE
AUDITS
RUSION-PREVENTION
SECURITY
WLAN
SICHERHEITSANALYSEN
SICHERHEITSMANAGEMENT
IT-GRUNDSCHUTZ
DATA LOSS PREVENTION
PENETRATIONSTEST
IT-FORENSIK
MOBILE/WIRELESS SICHERHEIT
SICHERHEIT SENSIBLER DATEN
APPLIKATIONS-SICHERHEIT
NETZWERKSICHERHEIT
INTERNET SICHERHEIT

Bewertung technischer Maßnahmen

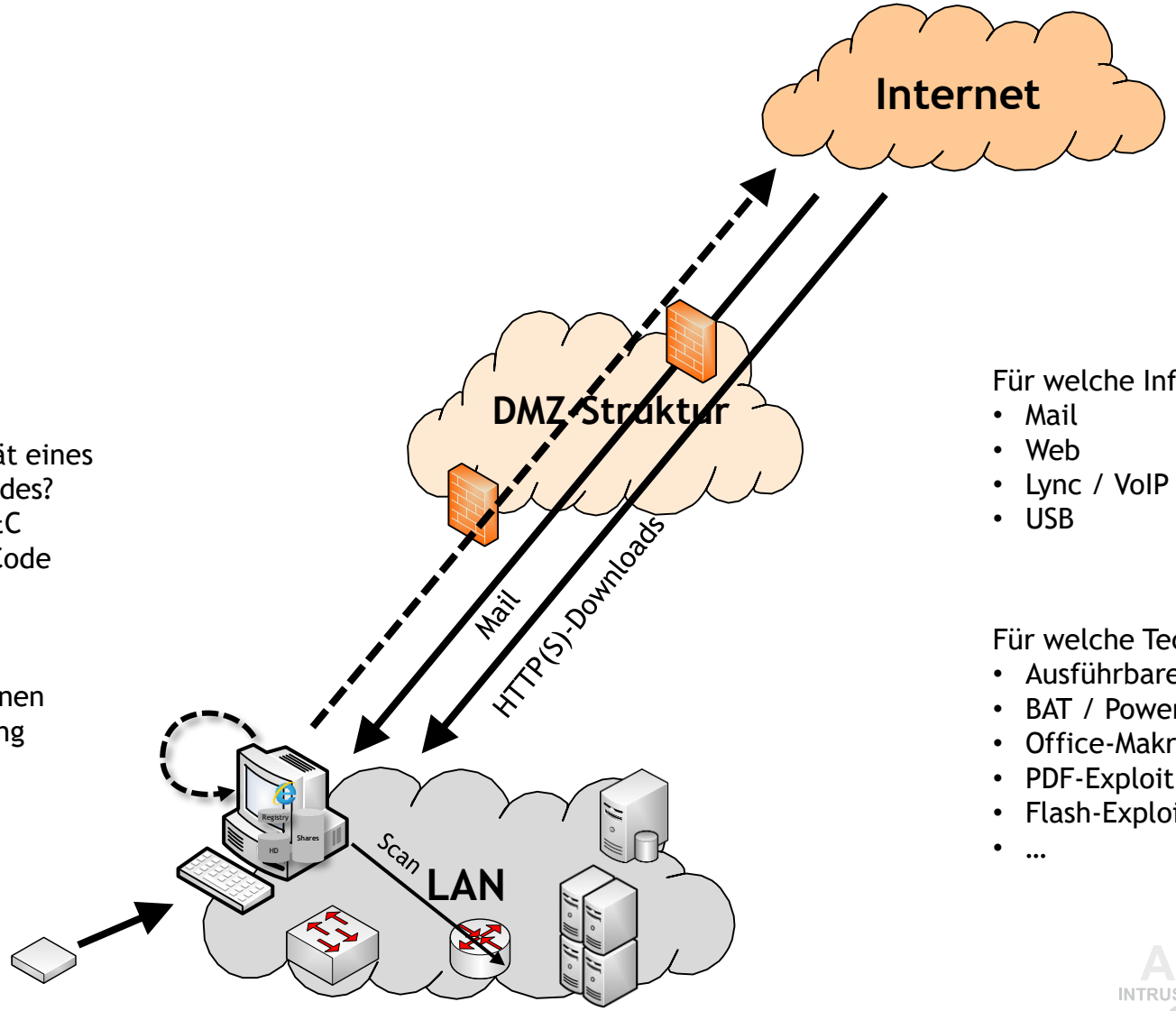
Grundidee der Bewertung technischer Maßnahmen in einer Matrix

- Gegenüberstellung der Wirksamkeiten gegen die relevanten Bedrohungsszenarien
  - Inwieweit schützt die jeweilige Technik tatsächlich vor den Bedrohungen, vor denen sie schützen soll?

- Vorgehensweise
  - Gliederung der Bedrohungen anhand von mehreren Achsen
    - An welchen Stellen greift die Schutztechnik?
  - Betrachtung der Angreifbarkeit bzw. Umgehbarkeit der Schutztechnik selbst
    - Wie einfach kann die Schutztechnik selbst angegriffen / umgangen werden?

Wo wirkt die Maßnahme überhaupt?

cirosec



Für welche Aktivität eines laufenden Schadcodes?
- DNS-Tunnel / C&C
- Nachladen von Code
- CMD.exe
- Scanning
- Datenextraktion
- File-Manipulationen
- Registry-Änderung
- …

Für welche Infektionswege?
- Mail
- Web
- Lync / VoIP / …
- USB

Für welche Techniken?
- Ausführbares Programm
- BAT / PowerShell-Script
- Office-Makro
- PDF-Exploit
- Flash-Exploit
- …

Am Beispiel klassisches AV

cirosec

Wirkmechanismus:

Antivirus - Endgerät	
Gezielt	**Standard**
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Mittel
Kein Schutz	Kein Schutz
Kein Schutz	Mittel
Kein Schutz	Kein Schutz
Kein Schutz	Kein Schutz
Kein Schutz	Kein Schutz
Kein Schutz	Kein Schutz
Kein Schutz	Kein Schutz
Kein Schutz	Kein Schutz
Einfach	

- Ausführen von Executables
- Ausführen von Batch / PowerShell-Skripte
- Makros, die beim Öffnen von Dokumenten aktiv werden
- Exploits, die einen Viewer / ein Plug-in kompromittieren

Prävention, bevor Code auf dem Endgerät ausgeführt wird

- Webseite / aktiver Code in Webseiten
- Mail-Attachments
- Externe Geräte (USB-Datenträger etc.)
- Über weitere Applikationen (Exploits für Lync, WebEx etc.)

Infektionsweg

- Nachladen von Code
  - in den laufenden Prozess / auf die Arbeitsplatz-Festplatte und anschließender Start
- Starten von (erlaubten) Programmen über cmd.exe / Browser auf dem Arbeitsplatz
- Rückverbindung
  - per DNS-Tunnel, HTTPS, TOR, Social Media etc. / per Socker Reuse
- Lokale Manipulationen an Registry, File System etc. des Arbeitsplatzes
- Extraktion von sensiblen Daten
- Lateral Movement
  - Scannen im internen Netz / Angriff / Zugriff auf andere Systeme im lokalen Netz

Verhinderung der Aktivitäten nach Infektion des Endgeräts

Umgehbarkeit

Umgehbarkeit

Überblick klassische Verfahren

cirosec

Wirkmechanismus:	Antivirus		Lokale Firewalls		Application Whitelisting		Device Control	
	Gezielt	Standard	Gezielt	Standard	Gezielt	Standard	Gezielt	Standard
Einbruch / erster Code-Start über								
Ausführen von Executables	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Sehr Hoch	Sehr Hoch	Kein Schutz	Kein Schutz
Ausführen von Batch / PowerShell-Skripte	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Hoch	Hoch	Kein Schutz	Kein Schutz
Makros, die beim Öffnen von Dokumenten aktiv werden	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Exploits, die einen Viewer / ein Plug-in kompromittieren	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Infektionsweg								
Webseite / aktiver Code in Webseiten	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Gering	Gering	Kein Schutz	Kein Schutz
Mail-Attachments	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Gering	Gering	Kein Schutz	Kein Schutz
Externe Geräte (USB-Datenträger etc.)	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Gering	Gering	Hoch	Hoch
Über weitere Applikationen (Exploits für Lync, WebEx etc.)	Kein Schutz	Mittel	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Aktivitäten von Malware / Shellcode nach Infektion des Endgeräts								
Nachladen von Code in den laufenden Prozess	Kein Schutz	Kein Schutz	Kein Schutz	Gering	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Nachladen von Code auf die Arbeitsplatz-Festplatte und Start	Kein Schutz	Mittel	Kein Schutz	Gering	Hoch	Sehr Hoch	Kein Schutz	Kein Schutz
Starten von (erlaubten) Programmen über cmd.exe / Browser	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Mittel	Mittel	Kein Schutz	Kein Schutz
Rückverbindung per DNS-Tunnel, HTTPS, TOR, Social Media etc.	Kein Schutz	Kein Schutz	Gering	Gering	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Rückverbindung per Socket Reuse	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Lokale Manipulationen an Registry, File System etc.	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Extraktion von sensiblen Daten	Kein Schutz	Kein Schutz	Gering	Gering	Kein Schutz	Kein Schutz	Gering	Gering
Lateral Movement: Scannen im internen Netz	Kein Schutz	Kein Schutz	Mittel	Mittel	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Lateral Movement: Angriff auf andere Systeme im lokalen Netz	Kein Schutz	Kein Schutz	Mittel	Mittel	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Umgehbarkeit	Einfach		Einfach		Mittel		Schwer	

cirosec

ISMS-LEAD-AUDITOREN
ANGRIFFE
AUDITS
RUSION-PREVENTION
SECURITY
WLAN
SICHERHEITSANALYSEN
SICHERHEITSMANAGEMENT
IT-GRUNDSCHUTZ
DATA LOSS PREVENTION
PENETRATIONSTEST
IT-FORENSIK
MOBILE/WIRELESS SICHERHEIT
SICHERHEIT SENSIBLER DATEN
APPLIKATIONS-SICHERHEIT
NETZWERKSICHERHEIT
INTERNET SICHERHEIT

Fragen ?