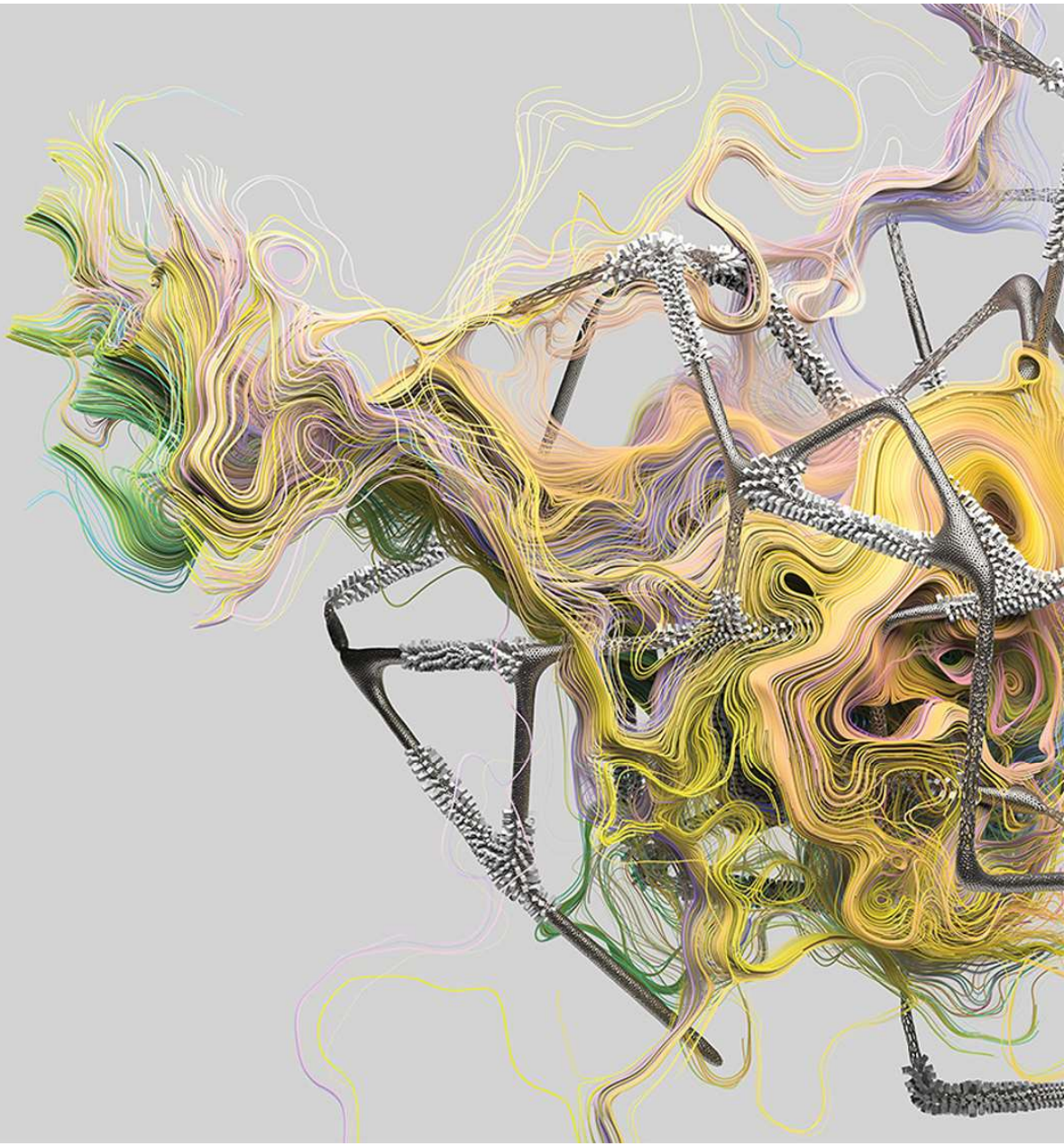
Channel Webinar: End of Support does not mean End of Security

Richard Werner Business Consultant
Timo Wege, Senior Senior Technical Consultant
20.09.2019



Stand 03.09.2019

196

24

In 2019 gefundene Sicherheitslücken für Windows Server 2008 (R2)

Davon kritisch
CVSS Score >= 9


Microsoft | Windows Server
Vergleich
Kaufen
Lösungen
Vorherige Versionen
Jetzt testen
Der Support für Windows Server 2008 wird eingestellt
Am 14. Januar 2020 wird der Support für Windows Server 2008 und 2008 R2 eingestellt. Dies bedeutet, dass keine regelmäßigen Sicherheitsupdates mehr bereitgestellt werden. Sorgen Sie dafür, dass Ihre Infrastruktur und Anwendungen weiterhin geschützt sind. Wir unterstützen Sie bei der Migration zur aktuellen Version für mehr Sicherheit, Leistung und Innovation.
Den Migrationsleitfaden herunterladen
Die Ignite-Sitzung ansehen

September CVEs

ZERO DAY INITIATIVE

PRIVACY WHO WE ARE HOW IT WORKS BLOG ADVISORIES LOG IN | SIGN UP

Here's the full list of CVEs released by Microsoft for September 2019.

Neu auf Windows Server 2008

CVE	Title	Severity	Public	Exploited	XI - Latest	XI - Older	Type
CVE-2019-1214	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important	No	Yes	3	0	EoP
CVE-2019-1215	Windows Elevation of Privilege Vulnerability	Important	No	Yes	0	0	EoP
CVE-2019-1235	Windows Text Service Framework Elevation of Privilege Vulnerability	Important	Yes	No	2	2	EoP
CVE-2019-1294	Windows Secure Boot Security Feature Bypass Vulnerability	Important	Yes	No	2	2	SFB
CVE-2019-0787	Remote Desktop Client Remote Code Execution Vulnerability	Critical	No	No	1	1	RCE
CVE-2019-0788	Remote Desktop Client Remote Code Execution Vulnerability	Critical	No	No	1	1	RCE
CVE-2019-1138	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	2	N/A	RCE
	VBScript Remote Code Execution						

Was bedeutet das?

Keine neuen Sicherheitsupdates mehr.

offiziell

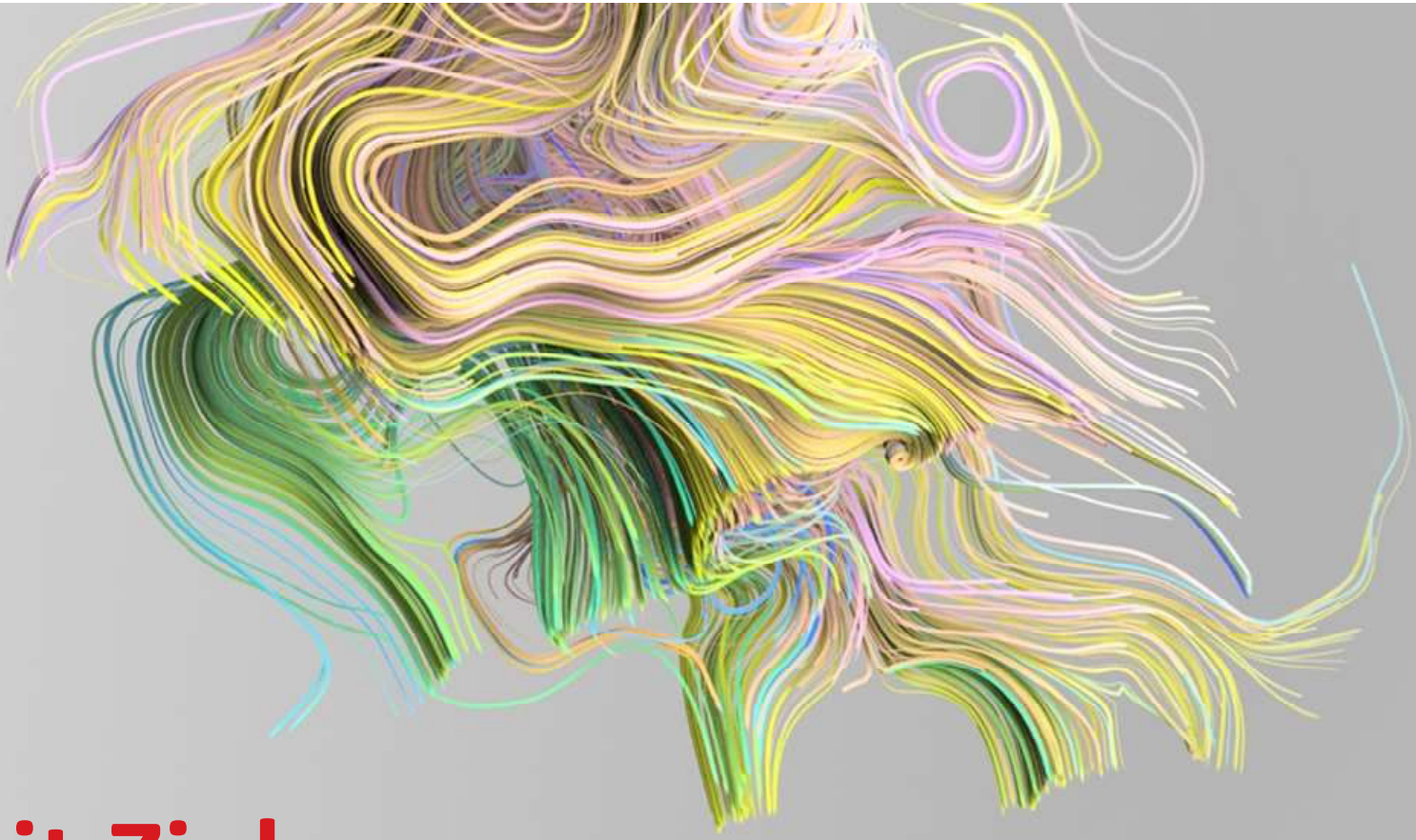
Ausnahmen:

- Migration auf Microsoft Azure (+ 3 Jahre)
- Kostenpflichtiger Support (+ x Jahre)
- richtig gefährliche Malware ?

Richtig gefährliche Malware?

CVE-2017-0144 wurde offiziell im März 2017 gepatcht

EOL - XP, 8 und Server 2k3 kamen am 13. May hinzu. Einem Tag nach Wannacry.



Angriffe mit Ziel Rechenzentrum

Zwei populäre Schemata mit Fokus auf Rechenzentren

Spearhead Phishing (z.B. Emotet)

- Klassisch E-Mailbasiert
- Angriffe auf Unternehmen nehmen zu

„Supply Chain“ Modell (z.B. Not-Petya)

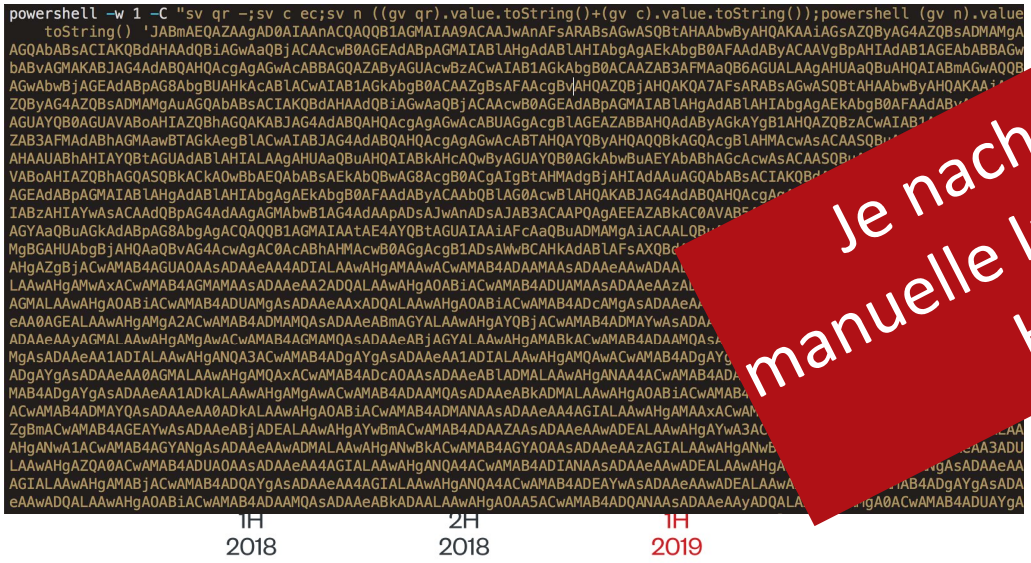
- Hack eines Service Anbieters
- Modifizierter Aktualisierungsprozess
- Inter-Server Attacke

Emotet – Trickbot die „klassische Ransomware“

- E-Mail aus vertrauenswürdiger Quelle
- Referenz auf tatsächliches Ereignis
- Payload mit Fileless Angriff
- Erstes Ziel: Clients

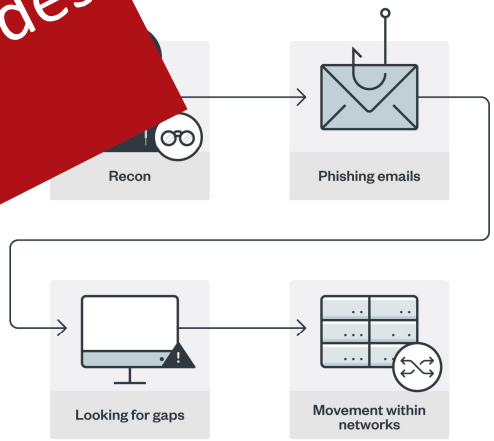
Die Kill Chain

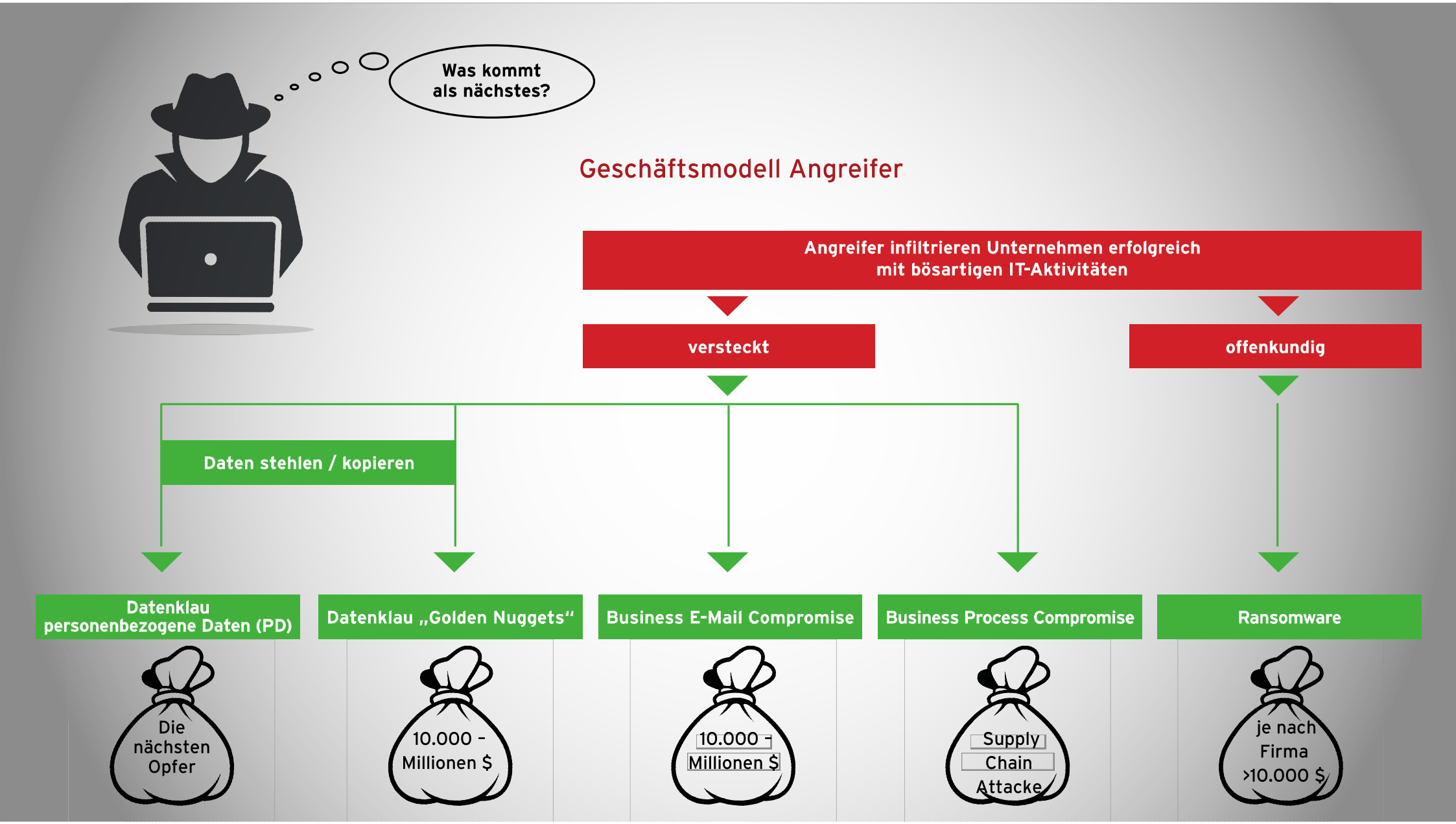
Initialangriff durch „Fileless“ Attacke



Lateral Movement über Schwachstellen und A hen von Passwörtern

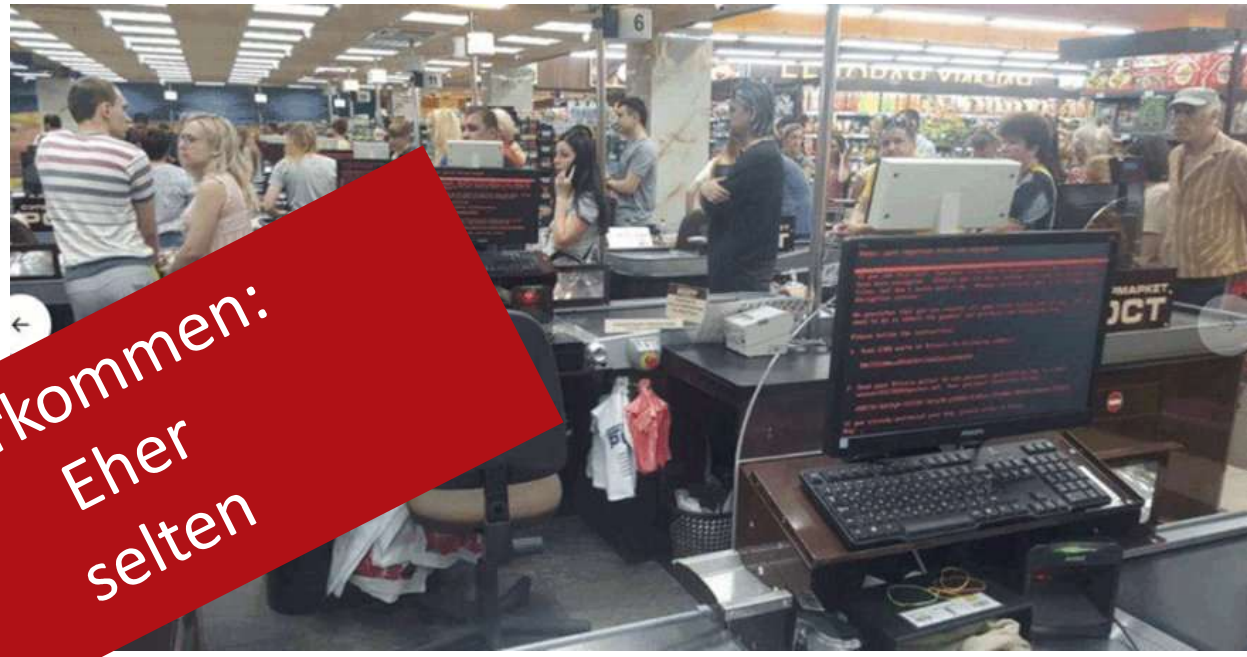
Je nach Größe - manuelle Interaktion des Hackers




Was kommt als nächstes?
Geschäftsmodell Angreifer
Angreifer infiltrieren Unternehmen erfolgreich mit bösartigen IT-Aktivitäten
versteckt
offenkundig
Daten stehlen / kopieren
Datenklau personenbezogene Daten (PD)
Datenklau „Golden Nuggets“
Business E-Mail Compromise
Business Process Compromise
Ransomware
Die nächsten Opfer
10.000 – Millionen $
10.000 – Millionen $
Supply Chain Attacke
je nach Firma >10.000 $

Supply Chain Angriffe

- Infektion eines Software Service Unternehmens
- Manipulation eines Kommunikationsprozesses (z.B. Update)
- Angriff auf Kunden d… initialen Opfers
- Erstes Ziel: Server
- Verteilung mittels Schwachstellen



Vorkommen: Eher selten

Angriffe in Baden-Württemberg

Stuttgarter Staatstheater

Hacker griffen über IT-Firma an

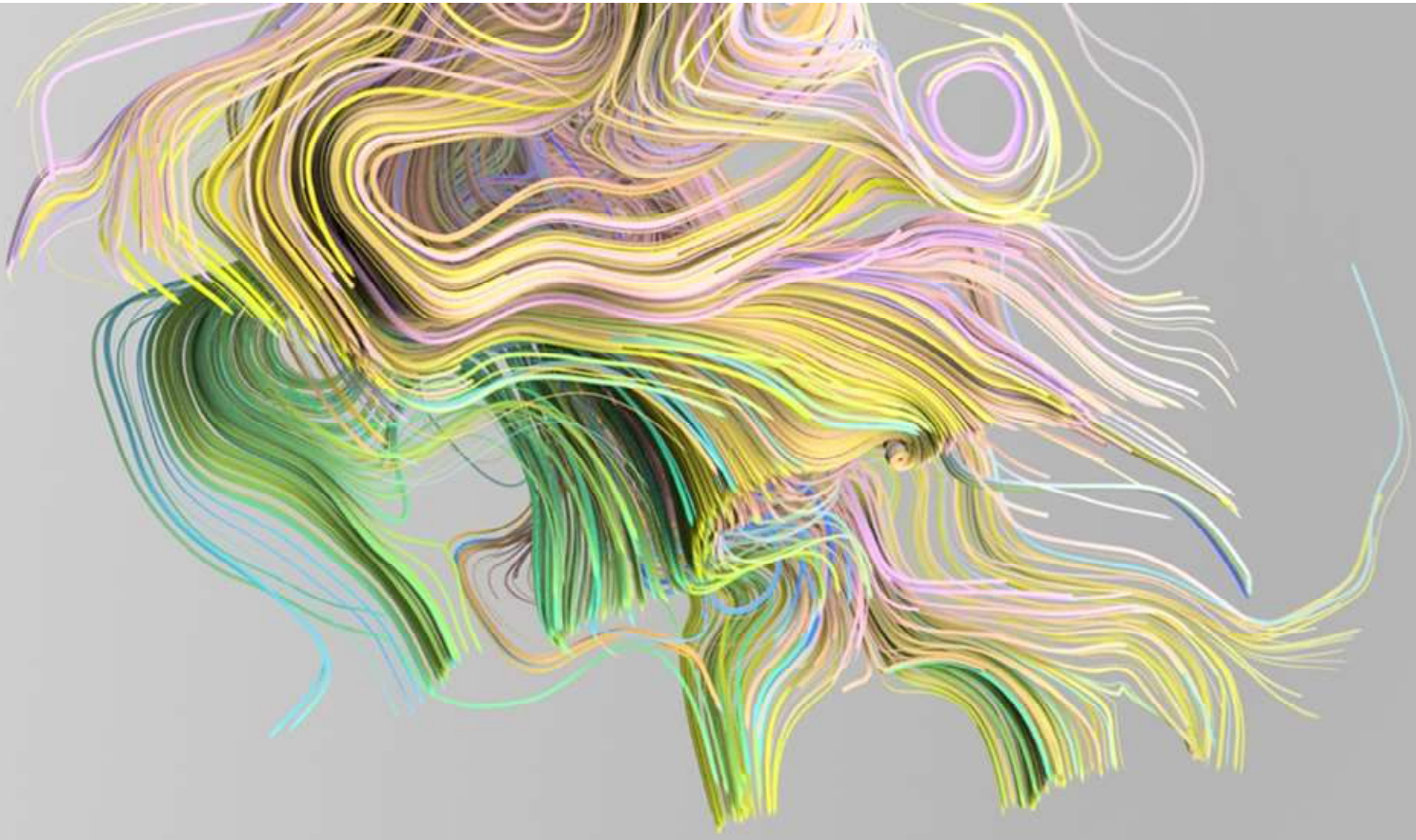
Fernwartungssystem war Einfallstor für Trojaner-Attacke - Angriff umfangreicher als bisher bekannt

https://www.rnz.de/politik/suedwest_artikel,-stuttgarter-staatstheater-hacker-griffen-ueber-it-firma-an-_arid,432947.html

Der Landesdatenschützer Stefan Brink ging im April von einer hohen zweistelligen Zahl aus…

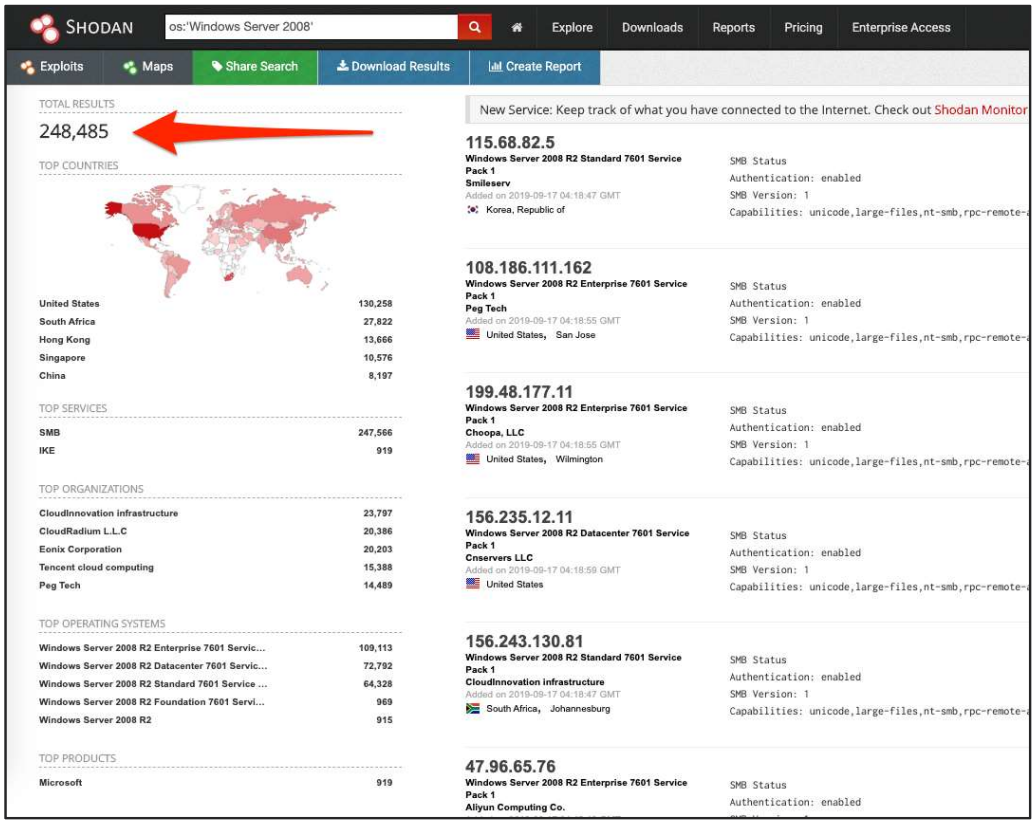
…Brink zufolge sind die betroffenen Firmen alle Kunden eines großen IT-Dienstleisters mit Sitz in Baden-Württemberg. Die Hacker nutzten offenbar ein Fernwartungstool des Dienstleisters aus und forderten von ihren Opfern ein Lösegeld. Die ersten Angriffe sollen laut Brink bereits Ende Februar, Anfang März erfolgt sein. Erste Meldungen gingen bei seiner Stelle aber erst Ende März ein.

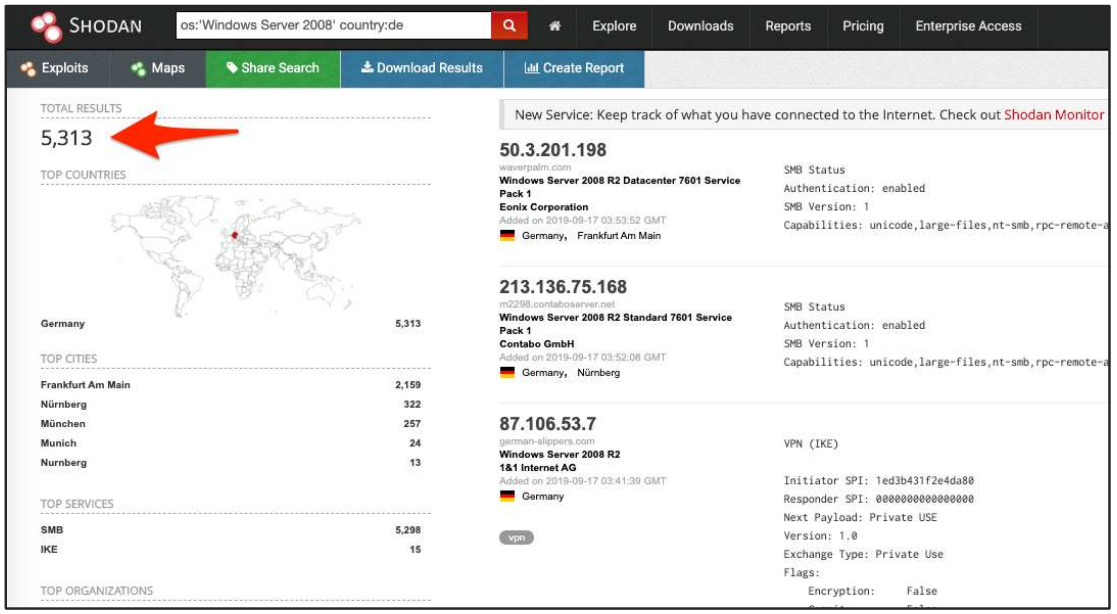
https://www.welt.de/regionales/baden-wuerttemberg/article199661746/Cyberangriff-auf-Messe-Stuttgart.html?wtrid=onsite.onsitesearch

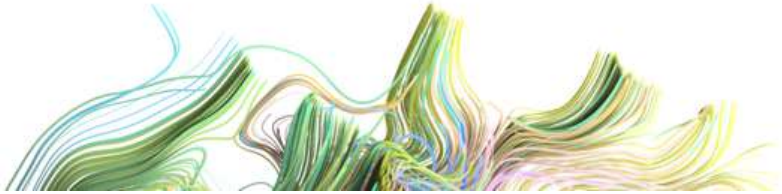


Verteidigung

Ist Server 2008 ein lohnendes Ziel?

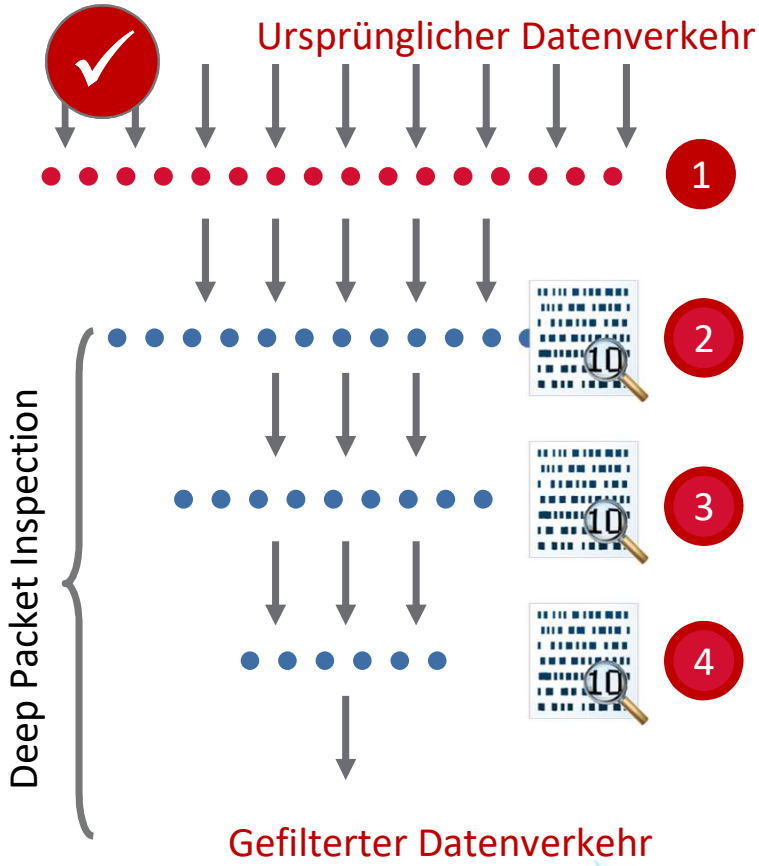






TREND MICRO

Virtuelles Patching mit Deep Security



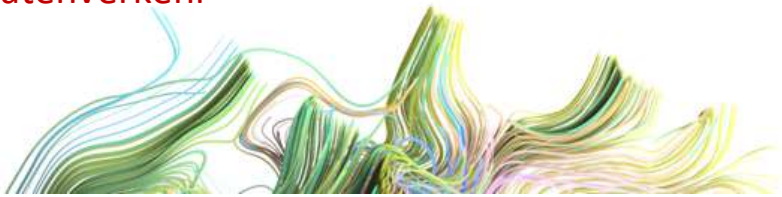
1 **Stateful-Firewall**
Bekannte unbedenkliche Daten werden zugelassen.

2 **Regeln zur Abwehr von Exploits**
Bekannte gefährliche Daten werden gestoppt.

3 **Regeln für Schwachstellen**
Bekannte Schwachstellen werden abgeschirmt.

4 **Intelligente Regeln**
Unbekannte Schwachstellen werden abgeschirmt und spezifische Anwendungen geschützt.

Abschirmung von mehr als 100 Anwendungen, darunter:
Betriebssysteme
Datenbankserver
Webanwendungsserver
Mail-Server
FTP-Server
Backup-Server
Speichermanagementserver
DHCP-Server
Desktop-Anwendungen
Mail-Clients
Webbrowser
Virenschutz
Sonstige Anwendungen



Trend Micro Deep Security

TREND MICRO SMART Protection Network

ZERO DAY INITIATIVE

Security Optionen

Pre-deployment
Image Scanning

Schwachstellen Scanning | Malware Erkennung | Jagen & Säubern

Stetige Image Überwachung auf Malware & Schwachstellen

Network Security

Intrusion Prevention | Firewall | Schwachstellen Scanning

Stoppt Netzwerk Angriffe, schirmt Schwachstellen ab auf Applikationen & Server

Runtime / Deployed
System Security

Applikations Kontrolle | Integrity Monitoring | Log Inspection

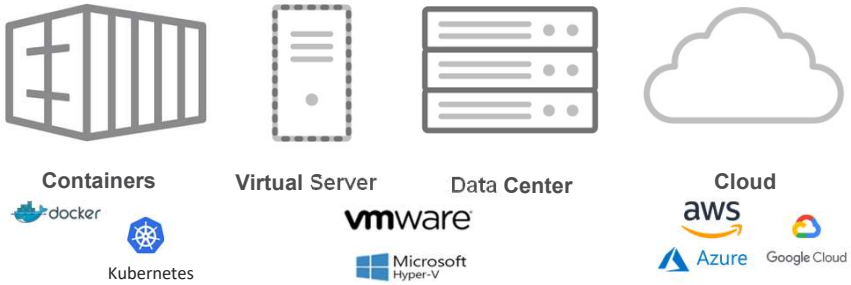
Lock down der Systeme & Erkennung verdächtiger Aktivitäten

Malware Prevention

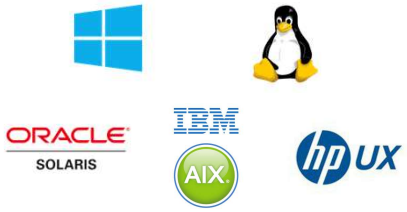
Anti-Malware | Behavioral Analyse & Machine Learning | Sandbox Analysis

Stoppt Malware & zielgerichtete Angriffe

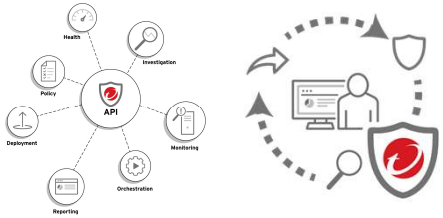
Umgebungen



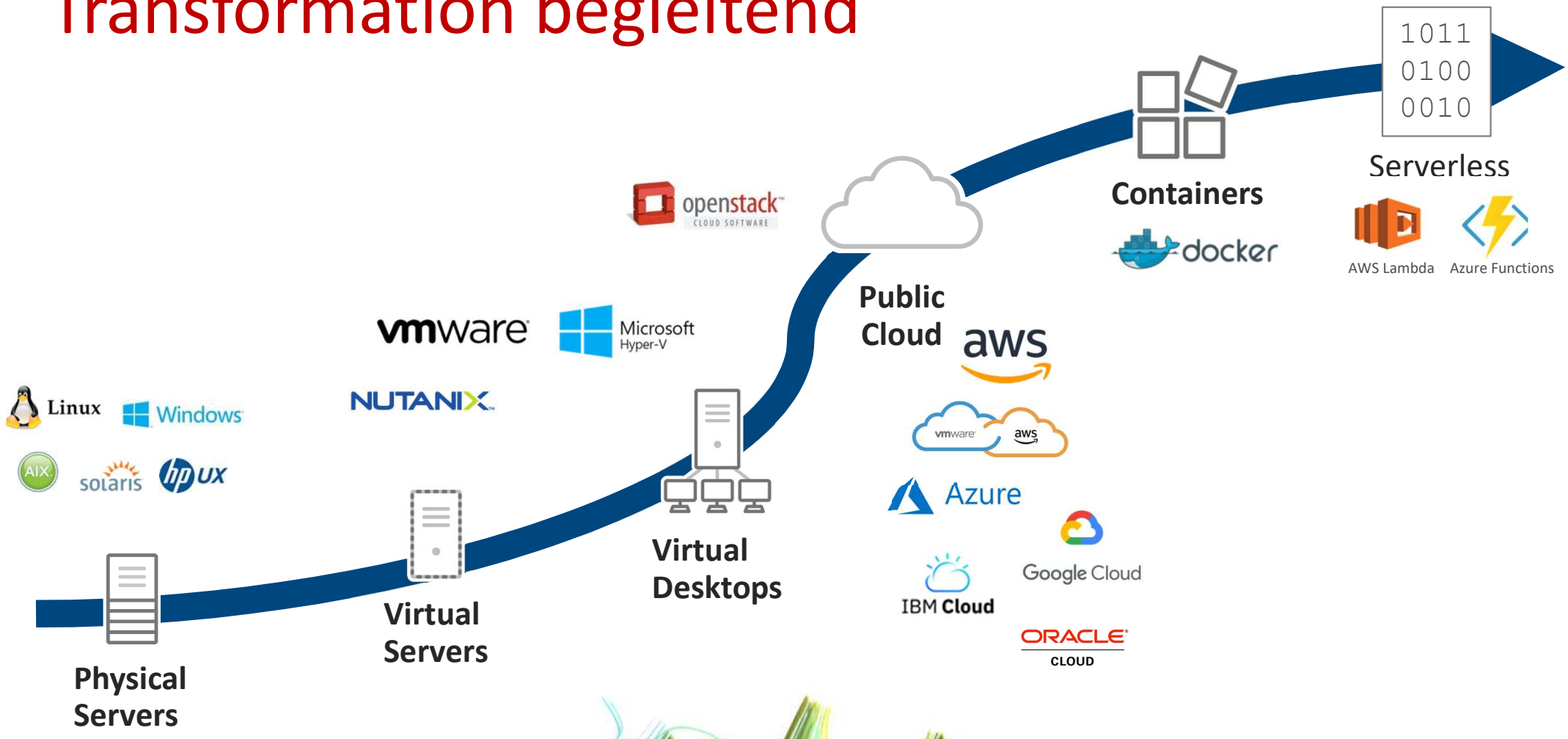
Betriebssysteme



API & Integrationen



Transformation begleitend

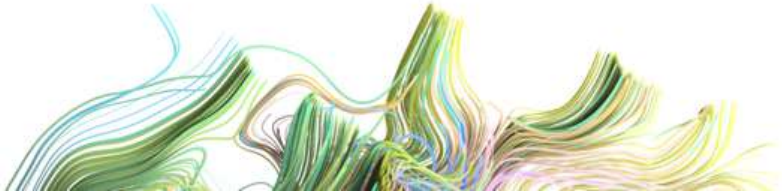


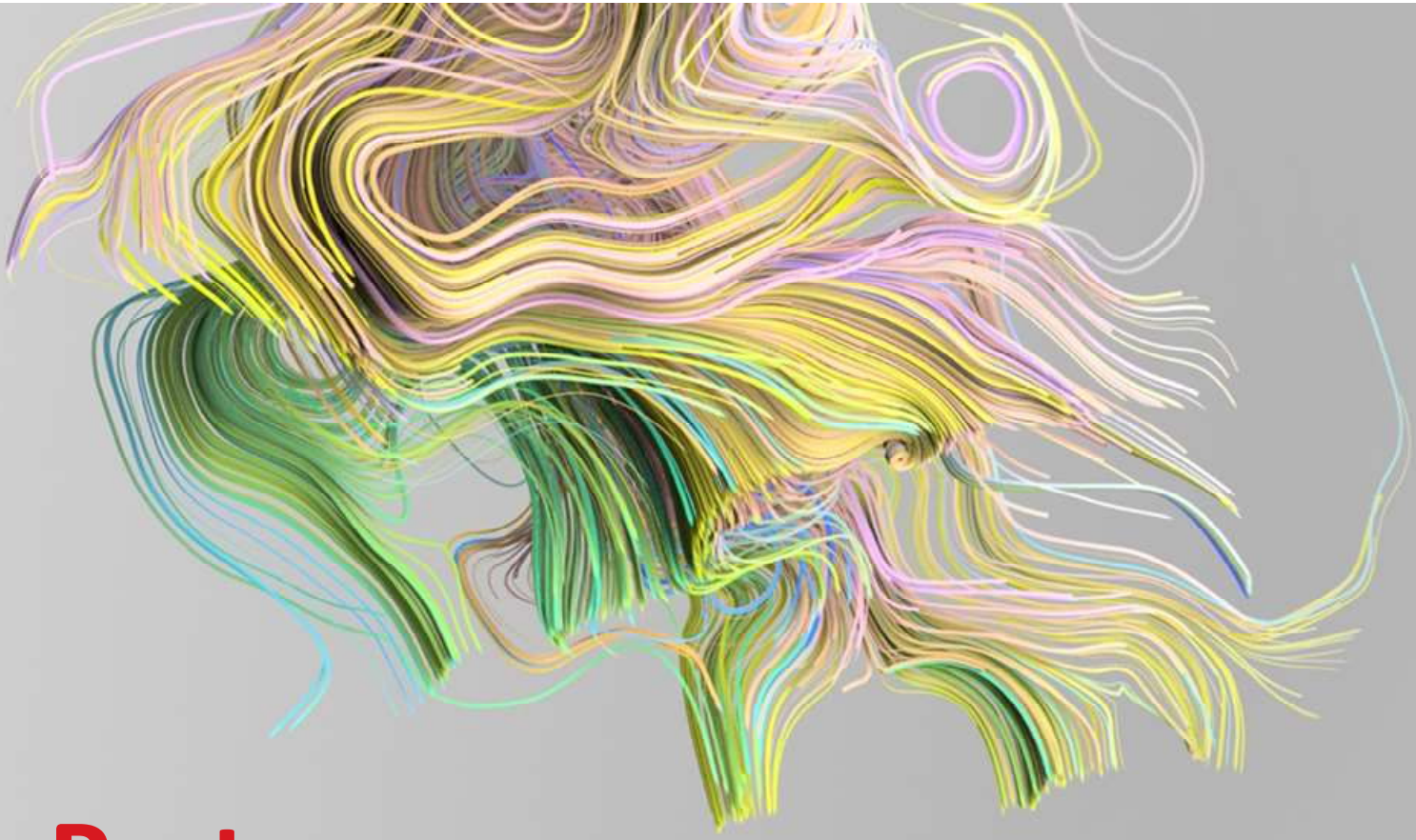
Fazit:

#1 Schwachstellen abschirmen

#2 Systeme segmentieren

#3 umfassende Sichtbarkeit schaffen





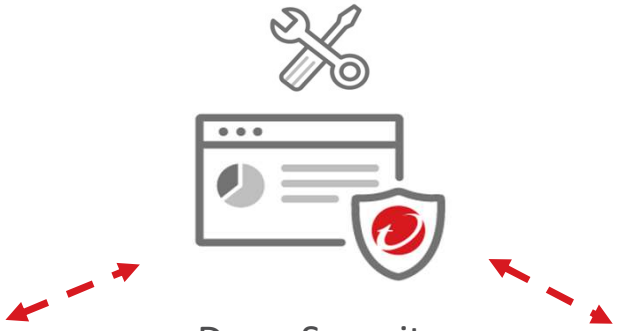
Wie Sie als Partner profitieren

Trend Micro Deep Security

Etwa 50-60% aller Server sind Windows 2008
Kunden haben die folgenden Möglichkeiten

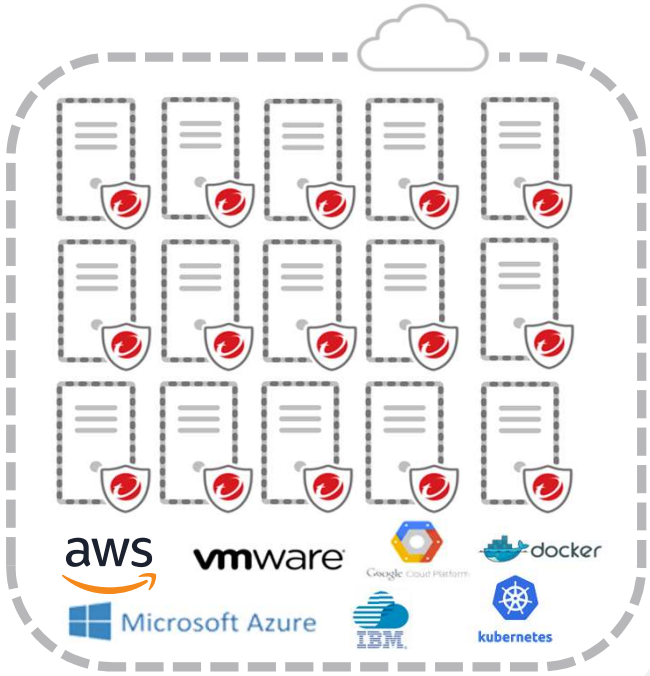
	Migration auf Azur	**Kostenpflichtiger Support**	**Kein Support**
Formfaktor	Cloud und hybride Datacenter	On Premise	On Premise
Trend Micro Argumentation	Zentrales Management, Flexibles Deployment	Hostbasierter Ansatz um Server gegeneinander zu schützen	Server sind gegen moderne Angriffe geschützt
Spezialität	Pay as you use Angebote	Agentenlos mit NSX	Trend offeriert noch Support für Windows 2003

Securing Business Transformation



Deep Security

A single security management console with complete visibility across physical, virtual, cloud and container deployments. Remove security complexity across systems.



TREND MICRO

Certified For Key Environments AND For Security

aws partner network

Advanced
Technology Partner

- Security Competency
- Government Competency
- Public Sector Partner
- Marketplace Seller
- SaaS Partner

Microsoft Azure Certified

PCI DSS COMPLIANT

Level 1 Service Provider

VCE

SAP

vmware
Partner Innovation Award
2017 Global Winner

NUTANIX PARTNER NETWORK
NUTANIX READY
NETWORKING & SECURITY

FIPS VALIDATED 140-2

Common Criteria

TREND MICRO

Security Wants To…

BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes

GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud

GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption

Server2008 für den Channel

- Informationsseite
- https://resources.trendmicro.com/Window_Server_2008_EOL_forchannel.html
- Material für den Fachhandel
  - Whitepaper „Ende des Supports bedeutet nicht Ende der Sicherheit“
  - Umfassendes Channel Sell Sheet
  - Beides in Deutsch
- Material für Ihre Endkunden
  - Email-Vorlagen
  - Infografik
  - Webinartermine für Ihre Kunden

Weiteres Material folgt ...


TREND MICRO
THE ART OF CYBERSECURITY
Unknown threats detected and stopped over time by Trend Micro. Created with real data by artist Brendan Dawes.