Ende des Supports bedeutet nicht Ende der Sicherheit: Schutz nach dem EOS von Windows Server 2008 (R2)

Trend Micro, September 2019

Stand 03.09.2019

196

In 2019 gefundene Sicherheitslücken für Windows Server 2008 (R2)

24

Davon kritisch
CVSS Score >= 9

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						

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 ▷

Was bedeutet das?

Keine neuen Sicherheitsupdates mehr.

offiziell

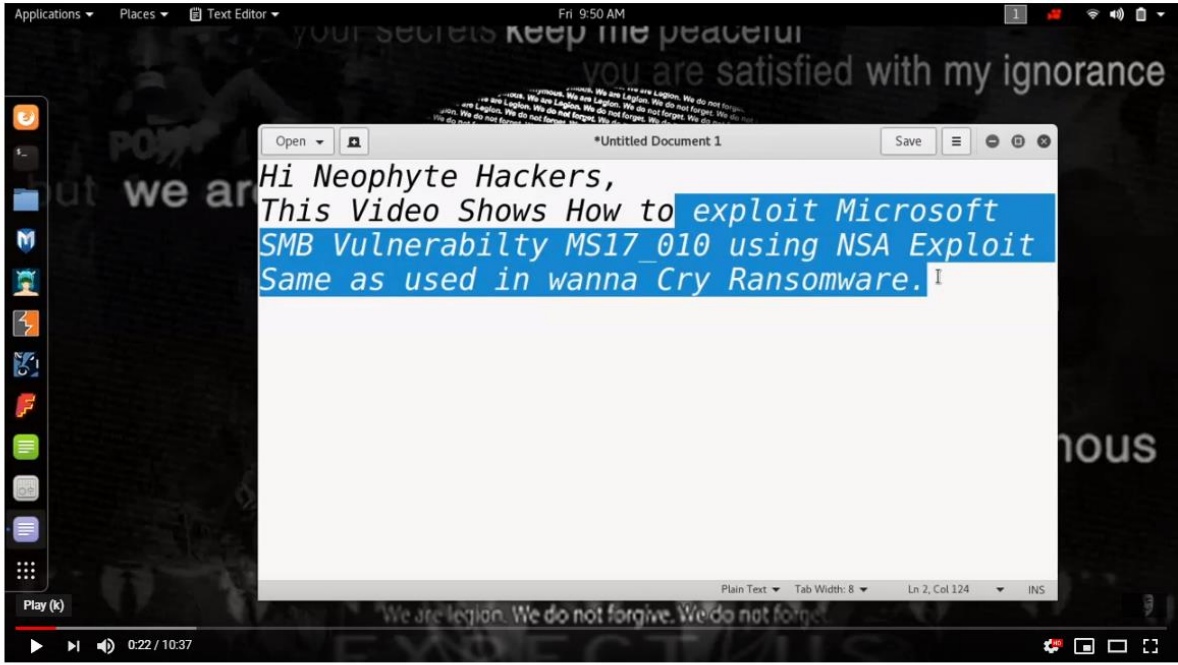
Ausnahmen:

- 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“

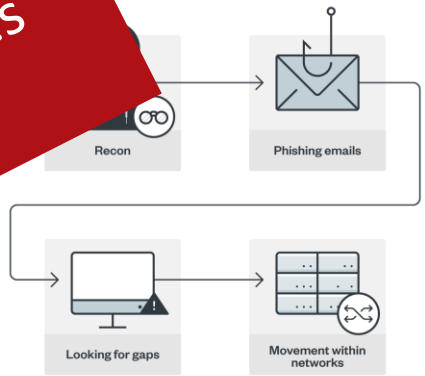
- E-Mail aus vertrauenswürdiger Quelle
- Referenz auf tatsächliches Ereignis
- Payload mit Fileless Angriff
- Erstes Ziel: Clients

Die Kill Chain

Initialangriff durch „Fileless“ Attacke

Lateral Movement über Schwachstellen und A[illegible]ähen von Passwörtern

Je nach Größe – manuelle Interaktion des Hackers



Geschäftsmodell Angreifer

Angreifer infiltrieren Unternehmen erfolgreich mit bösartigen IT-Aktivitäten

- **versteckt**
  - **Daten stehlen / kopieren**
    - **Datenklau personenbezogene Daten (PD)** — Die nächsten Opfer
    - **Datenklau „Golden Nuggets“** — 10.000 – Millionen $
    - **Business E-Mail Compromise** — 10.000 + Millionen $
    - **Business Process Compromise** — Supply Chain Attacke
- **offenkundig**
  - **Ransomware** — 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

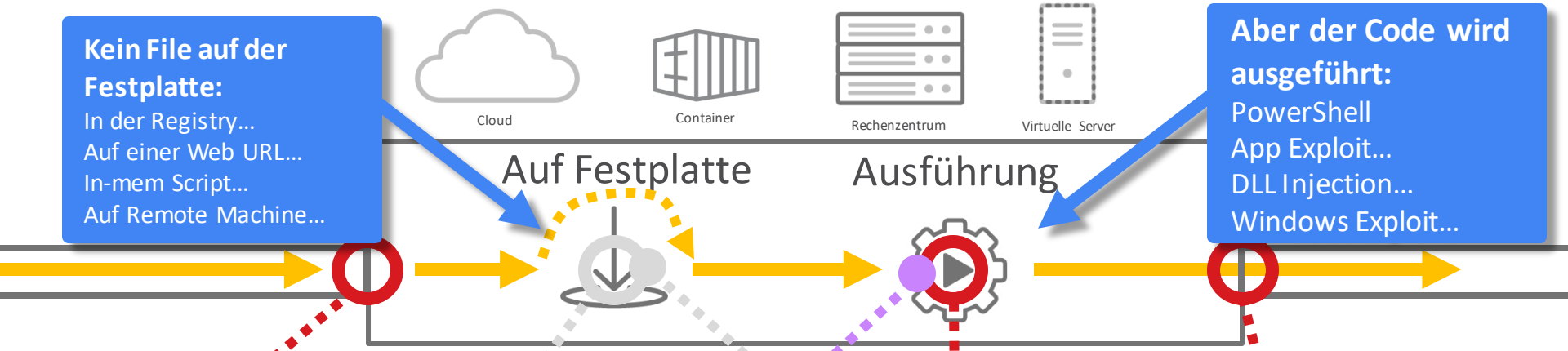
Der Landesdatenschützer Stefan Brink ging im April von einer hohen zweistelligen Zahl aus…

…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

Verteidigung gegen Fileless Malware



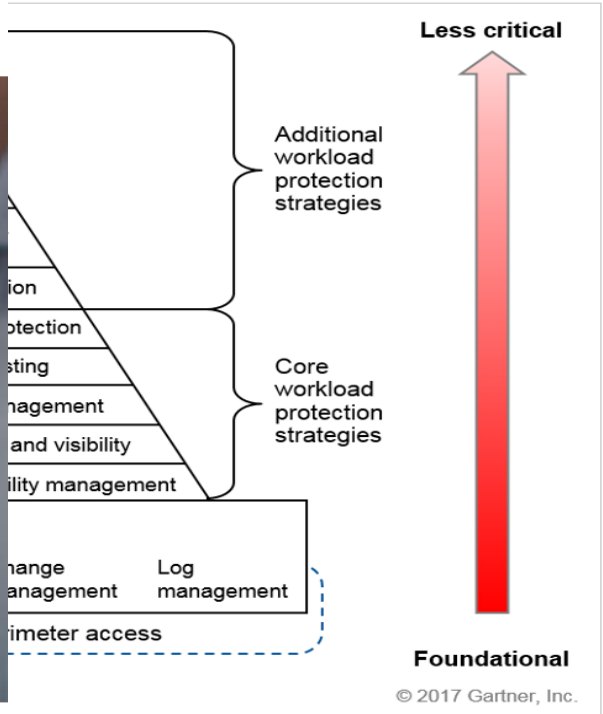
Eintrittspunkt:
Firewall
IPS,
Web Reputation

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

Server verteidigt man anders als Clients



TREND MICRO

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

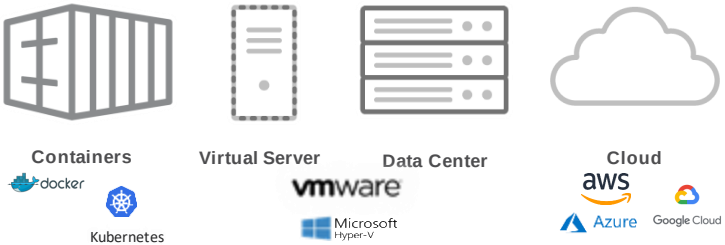
Lock down der Systeme & Erkennung verdächtiger Aktivitäten

Malware Prevention

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

Stoppt Malware & zielgerichtete Angriffe

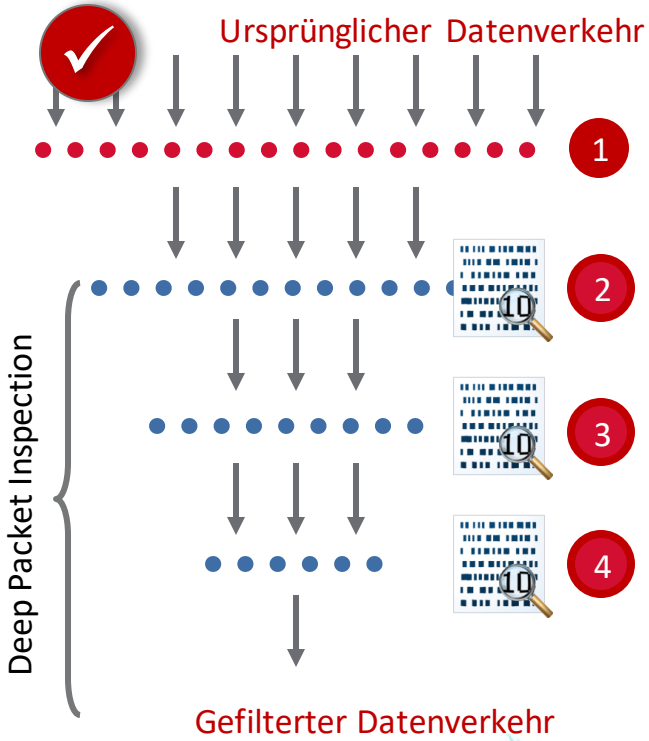
Umgebungen



Betriebssysteme

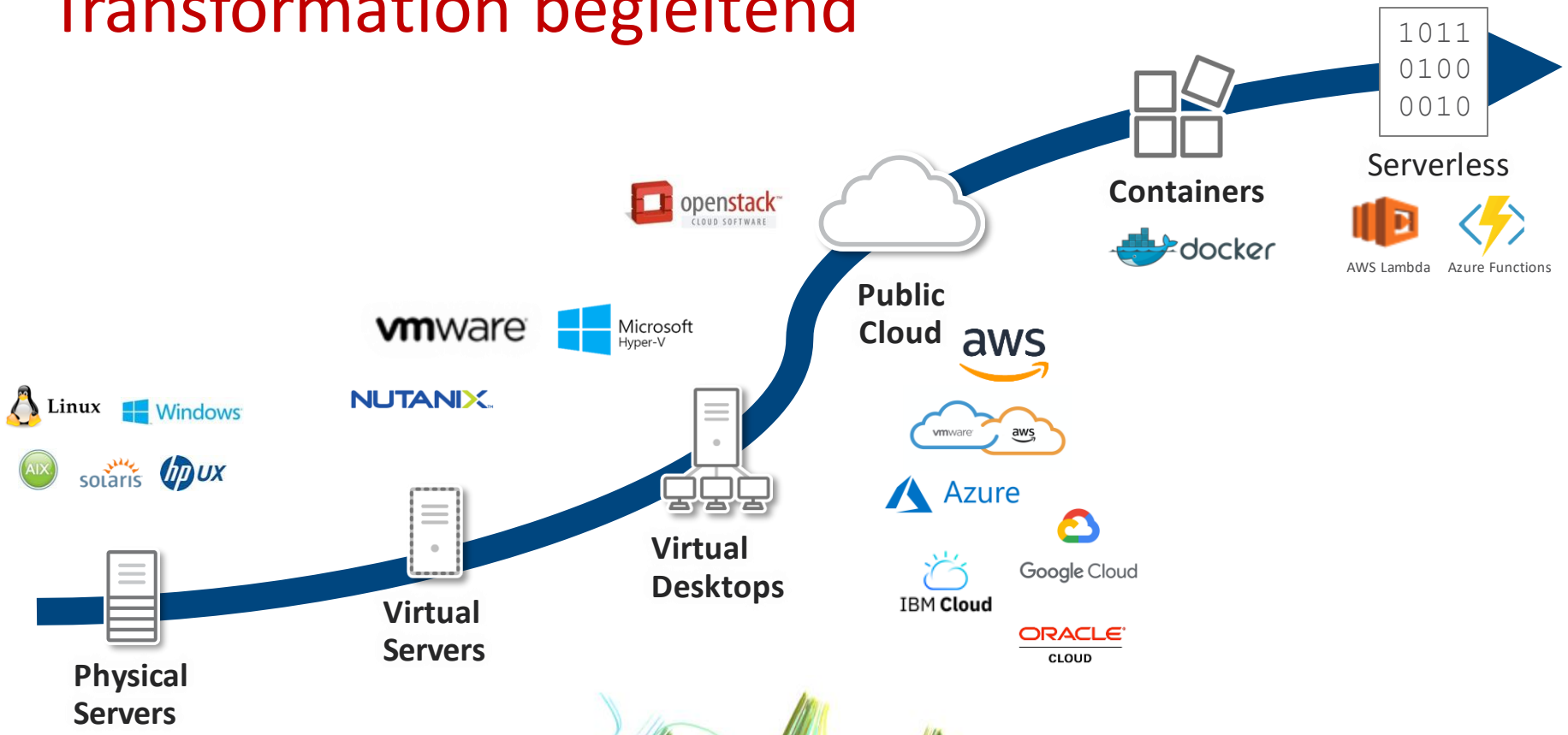
API & Integrationen

Virtuelles Patching mit Deep Security



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

Transformation begleitend



Fazit:

#1 Schwachstellen abschirmen

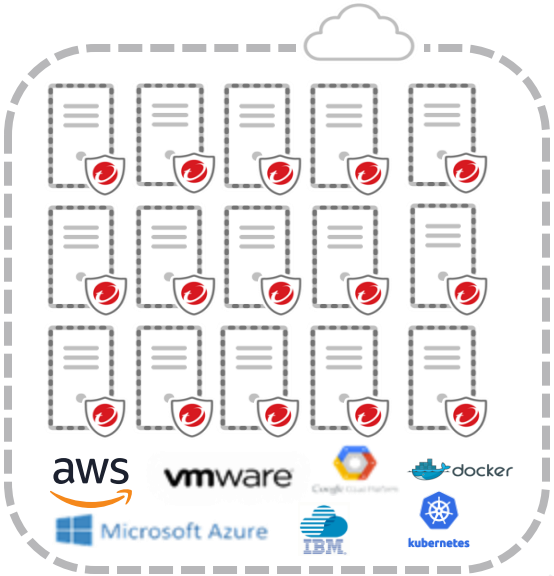
#2 Systeme segmentieren

#3 umfassende Sichtbarkeit schaffen

Sicherung der Business Transformation

Deep Security

Eine einzige Security Management Konsole mit umfassender Übersicht über physikalische, virtuelle, cloud und Container Umgebungen. Entfernen Sie die Komplexität aus Ihren Security Systemen.



Zertifiziert für Schlüsselumgebungen UND für 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

Sicherheit bedeutet im Idealfall…

Kraftvoll sein

Schützt gegen Schwachstellen, Malware & Unauthorisierte Änderungen

Einfach sein

Umfassender Schutz und Übersicht. Optimiert für alle Bereiche Ihrer Hybriden Cloud

Automatisiert sein

Verbundene Sicherheit, die sich nahtlos auch in Entwicklungs- und Betriebs Umgebungen einbauen läßt- um Reibungsverluste zu minimieren & die Einführung zu erleichtern

TREND MICRO™

Endpoint threats detected and blocked globally in 2018 by Trend Micro. **Created with real data by artist** Stefanie Posavec.