

Webcast

Hafnium – Sprechstunde 10.03.2021

Frank.Carius@netatwork.de

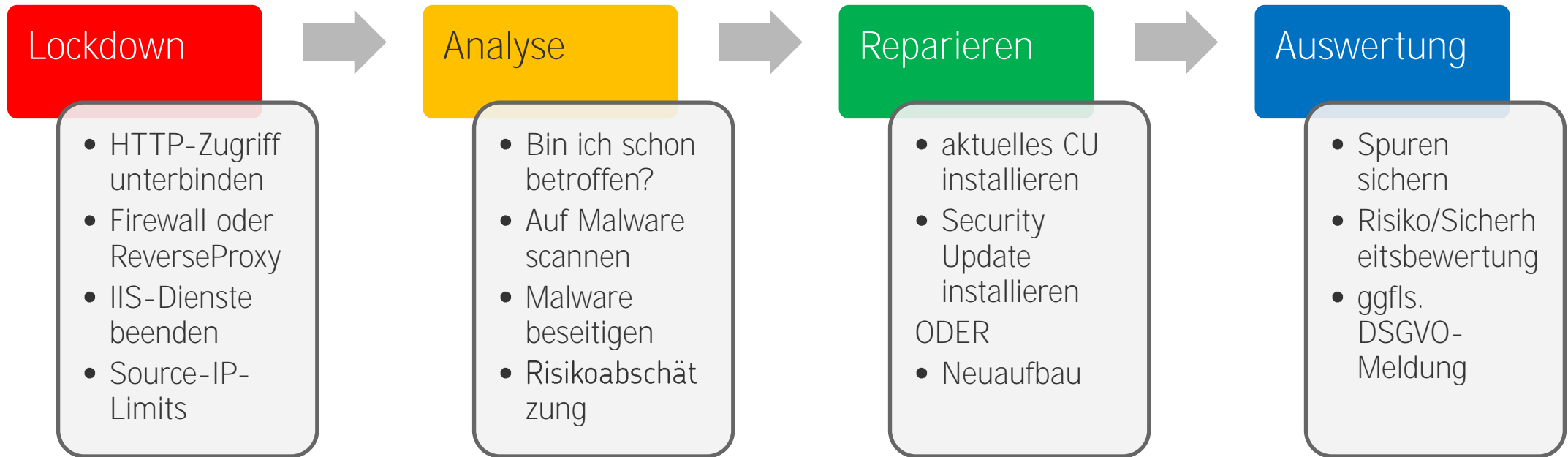
Weckruf

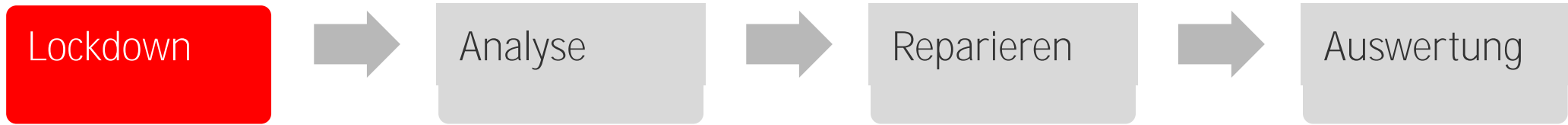


- **Exchange 2013/2016/2019 Server haben kritische Lücken**
 - › Vektor: Anonymer Zugriff per HTTPS auf Exchange Dienste (EWS, OAB, OWA, EAS etc.)
 - › CVE-2021-26855: Ohne Anmeldung kann man sich Zugangsdaten beschaffen für weitere Angriffe
 - › CVE-2021-26857: Bug in UM erlaubt ausführen von Code als System mit Anmeldedaten
 - › CVE-2021-26858/CVE-2021-27065: erlaubt das Schreiben von Daten mit Anmeldung
- **Schadmöglichkeiten**
 - › Angreifer kann Inhalte aller Mailboxen lesen -> Datenverlustrisiko, DSGVO-Verletzung/Meldung
 - › Angreifer kann Dateien ins Dateisystem des Exchange Server schreiben
-> Webshell („China Chopper“, erstmals 2012 entdeckt)
 - › Angreifer kann Befehle als „LocalSystem“ und „Exchange Trusted Subsystem“ ausführen
-> Exchange Konfiguration ändern, Postfach Export, weitere Angriffe als Sprungserver
- **Timeline**
 - › Dez 2020 erste Meldung an Microsoft durch DEVCORE
<https://proxylogon.com/#timeline> und <https://www.youtube.com/watch?v=SvjGMo9aMwE>
 - › Jan 2020 Erste „In the Wild“- Meldung durch Volexity
<https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/>
 - Feb 2021 Zunahme der Angriffe
 - › 2. März 2021 Updates durch Microsoft öffentlich



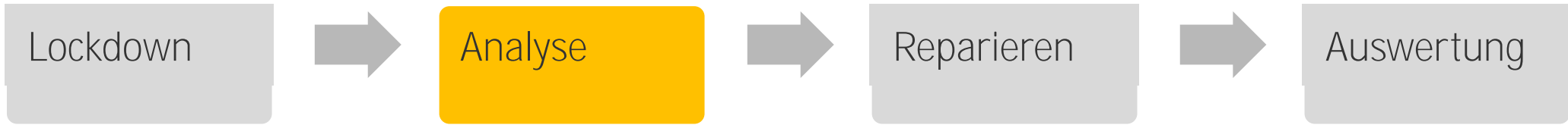
Was ist JETZT tun sollten:





- HTTPS Zugriff unterbinden
 - > Firewall-Regeln
 - > Reverse-Proxy
 - > IIS beschränken
 - > Auch ausgehenden Verkehr unterbinden (Webshell) !!
- Beschränkter Schutz
 - > „ExchangeMitigations.ps1“
<https://github.com/microsoft/CSS-Exchange/blob/main/Security/README.md>





- MSERT.EXE

<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download>
Scannt UND beseitigt erkannte Backdoors

- Test-ProxyLogon.ps1

<https://github.com/microsoft/CSS-Exchange/blob/main/Security/README.md>

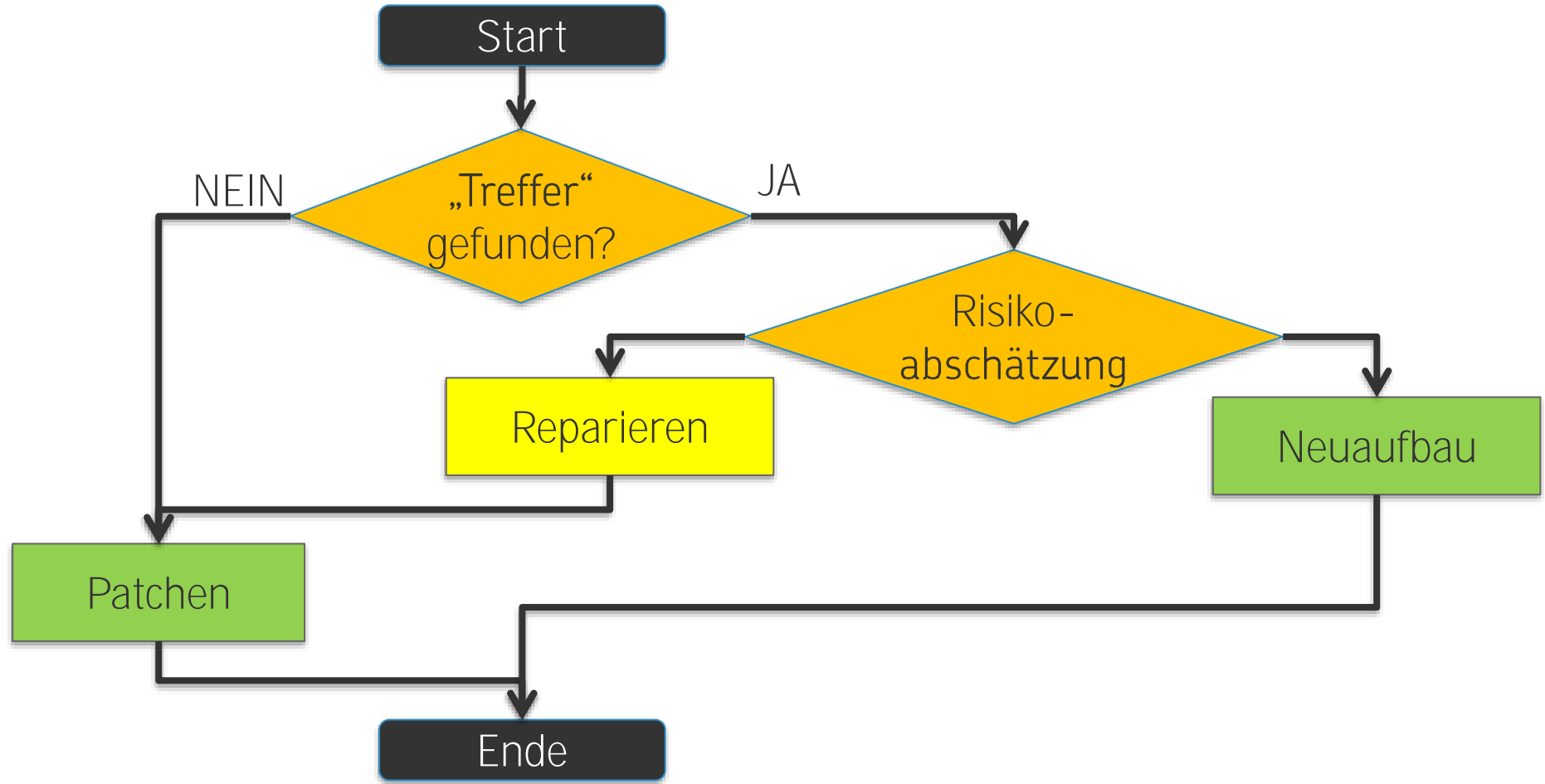
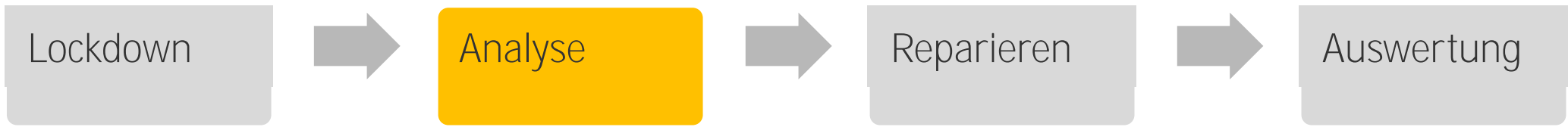
Analysiert

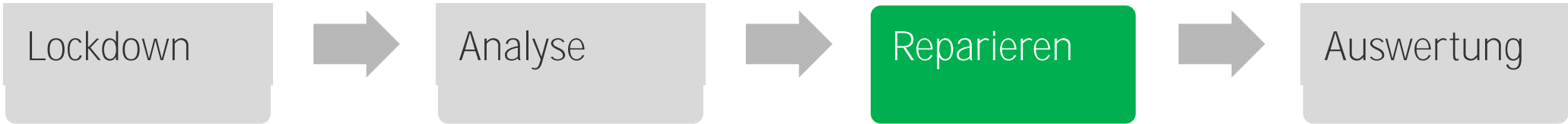
- > IIS-Logs
 - > ECP Log
 - > OAB-Log
 - > UM Eventlogs
 - > ASPX-Dateien
- 3rd Party Malware-Scanner

```
Administrator: Windows PowerShell
PS C:\hafnium> .\Test-ProxyLogon.ps1
Get-ChildItem : Access to the path 'C:\Windows\temp\%1spbq%' is denied.
At C:\hafnium\Test-ProxyLogon.ps1:175 char:39
+ ~~~~~
+   foreach ($file in Get-ChildItem -Recurse -Path "$env:WINDIR\ ..
+   ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Windows\temp\%1spbq:String) [Get-ChildItem], UnauthorizedAccessE
xception
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

ProxyLogon Status: Exchange Server EX01
Log age days: Oabgen Ecp Autod Eas EcpProxy Ews Mapi Oab Owa OwaCal Powershell RpcHttp
Report exported to: C:\hafnium\Test-ProxyLogonLogs\EX01-LogAgeDays.csv
Nothing suspicious detected
PS C:\hafnium> _
```







My Exchange Server is supported by original March 2021 security releases:

- Exchange Server 2010 SP 3 or later
- Exchange Server 2013 CU 23
- Exchange Server 2016 CU 19 or CU 18
- Exchange Server 2019 CU 8 or CU 7

Install March 2021 Security Updates

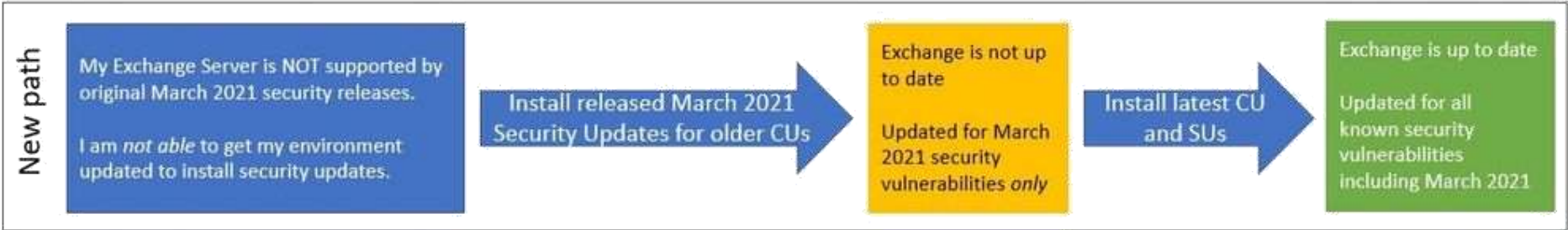
Exchange is up to date
Updated for all known security vulnerabilities including March 2021

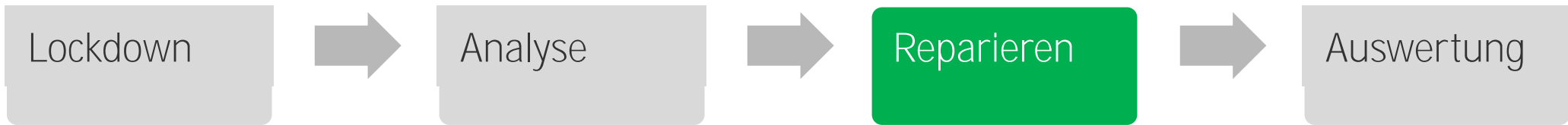
KB5000871 für 2013/2016/2019
KB5000978 für Exchange 2010!

My Exchange Server is NOT supported by original March 2021 security releases.
I am getting my environment supported to install security updates.

Install latest CU / RU → Install March 2021 Security Updates

Exchange is up to date
Updated for all known security vulnerabilities including March 2021





Kontrolle

- Nicht geeignet
 - > Get-ExchangeServer
 - > Get-Hotfix
 - > OWA-Parsing
- Besser
 - > Windows Update GUI
 - > Windows Explorer
- Build-Nummern
 - > Exchange mit
2. Mrz Security Update

```

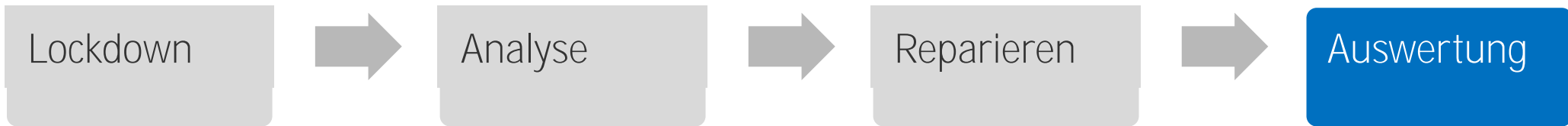
[PS] C:\>Get-ExchangeServer | Format-List Name, Edition, AdminDisplayVersion
Name                : EX16
Edition              : Standard
AdminDisplayVersion : Version 15.1 (Build 2176.2)
  
```

C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\Owa

Name	Date modified	Type
15.1.2176.2	08.12.2020 23:45	File folder
15.1.2176.4	07.02.2021 01:57	File folder
15.1.2176.9	03.03.2021 01:57	File folder

Exchange	2019	2016	2013	2010 SP3
Aktuell	CU8: 15.2.792.10	CU19: 15.1.2176.9	CU23: 15.0.1497.12	RU32: 14.3.513.0
N-1	CU7: 15.2.721.13	CU18: 15.1.2106.13		
N-2	CU6: 15.2.659.12	CU17: Missing		
N-3	CU5: 15.2.595.8	CU16: 15.1.1979.8		
N-3	CU4: 15.2.529.13	CU15: 15.1.1913.12		
N-4		CU14: 15.1.1847.12		





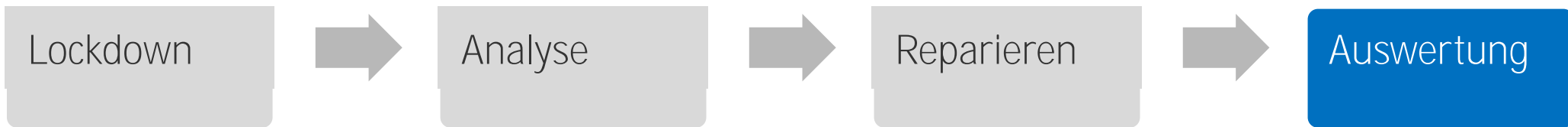
Schadcode gefunden und entfernt – alles OK?

- Welche Rechte hat „Exchange Trusted Subsystem“?
 - › Weniger Rechte ab Ex2019CU1, Ex2016CU12, Ex2013CU22
 - › Cluster File Share Witness?
- Welche Rechte hat „LocalSystem“?
 - › Anmeldung als Admin auf dem Server
 - › LSASS-Dump, Mimikatz
 - › Sprunghost auf andere Server
- „Webshell“?
 - › ASPX, PHP, o.a. Datei, die Code ausführt
 - › Parameter enthält Code
- Unbekannte Malware?

DETECTION	DETAILS	COMMUNITY
CAT-QuickHeal	① CVE-2021-26855:WebShell.41350	Kaspersky ① HEUR:Exploit.Script.CVE-2021-26855.a
Microsoft	① Exploit:ASRCVE-2021-27065.Bldha	Sophos ① Troj/WebShel-L
ZoneAlarm by Check Point	① HEUR:Exploit.Script.CVE-2021-26855.a	Acronis ② Undetected

Analysis - Post-Exploitation from Microsoft Exchange HAFNIUM <https://www.youtube.com/watch?v=rn-6t7OygGk>





- Mein Exchange ist nicht oder nur per VPN erreichbar
 - > Sind sie sicher ?
 - > Wie kommen ihre ActiveSync Geräte zu Exchange ?
 - > Wie funktioniert Exchange Hybrid Mode (Free/Busy; Migration)
- Ich habe eine Pre-Authentifizierung?
 - > Klingt gut. Aber für alle URLs?
 - > MAPI/HTTP mit PreAuth?
- MDM Proxy (MobileIron u.a.)
 - > Reverse Proxy für ActiveSync. EAS ist gesichert
 - > Aber was ist mit EWS und anderen Diensten ?
- Sonstiges
 - > Was ist mit internen Angriffen?
- Applocker, Splunk, Azure Sentinel, Defender ATP, LAPS, KRBRollover, ...



Vielen Dank für Ihre Aufmerksamkeit.

Aktuelle Informationen:

<https://www.msxfaq.de/exchange/update/hafnium-exploit.htm>

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
frank.carius@netatwork.de

Building IT-Excellence.
www.netatwork.de

