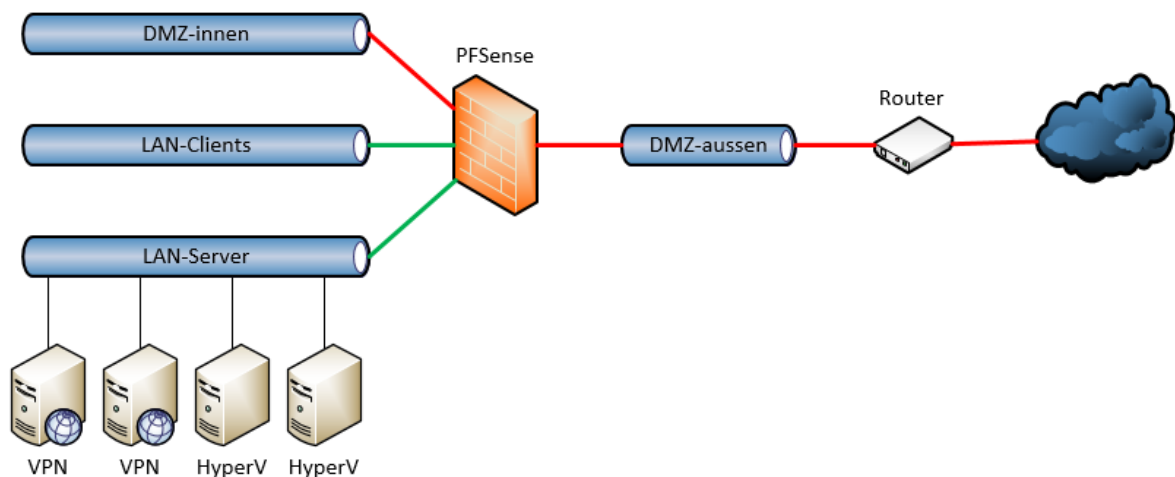


Inhalt

| | |
|--------------------------------------|----|
| Vorgeschichte | 1 |
| Der Angriff | 2 |
| Die Schwachstelle | 2 |
| Der Sicherheitsvorfall | 3 |
| Die Reaktion auf den Angriff | 4 |
| Möglichkeiten der Erkennung | 10 |
| Das Versagen von Microsoft ATA | 10 |
| Lockouts | 11 |
| Eventlog-Analyse | 11 |
| Zusammenfassung | 13 |

Vorgeschichte

Meine Infrastruktur wurde im Laufe der Zeit immer komplexer. Anfangs standen alle Clients und Server direkt hinter dem Internetrouter. Später schaltete ich eine PFSense dazwischen, um die Datenströme zu filtern und somit die Sicherheit zu erhöhen:

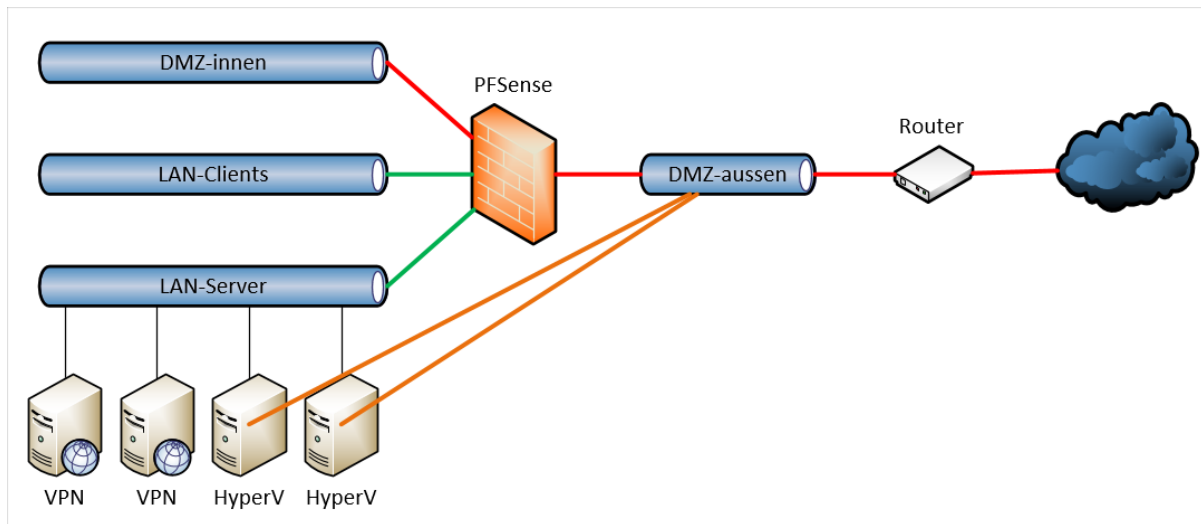


Die PFSense-Firewall sollte kostengünstig und ausfallsicher sein. Also installierte ich sie in eine virtuelle Maschine auf meinem Hyper-V-FailoverCluster, der aus 2 Servern bestand. Sollte einer der Server ausfallen, dann würde die VM auf dem anderen weiterlaufen bzw. wieder gestartet werden.

Für die Administration und den Zugriff auf Daten von unterwegs setzte ich 2 VPN-Server ein. Dieser waren im Netz „LAN-Server“ angeschlossen – also hinter der Firewall. Im Normalbetrieb ist das kein Problem. Aber was wäre, wenn die PFSense nicht funktioniert? Richtig: Dann wäre auch kein VPN-Zugriff und damit kein TroubleShooting möglich!

Natürlich hätte ich auch die beiden VPN-Server in die „DMZ-aussen“ platzieren können. Aber die Verteilung der Verbindungen auf beide Server übernimmt ein HAProxy – ein Zusatzmodul in der PFSense, denn mein Router kann kein PortForwarding mit 1:n. Somit hätte ich nur einen VPN-Server einsetzen können. Und dann wäre das Problem mit der Verfügbarkeit nur verschoben.

So entschied ich mich, den beiden HyperV-Servern einen Zugang zum Netz „DMZ-aussen“ zu konfigurieren:



So konnte ich auf meinem Router direkt ein PortForwarding auf den RDP-Port 3389 einrichten (Hinweis: mach das bloß nicht nach!). Damit es nach außen nicht so offensichtlich ist habe ich für extern einen anderen Port gewählt (Security by Obscurity == FacePalm):

| Freigabe bearbeiten | |
|------------------------------|--|
| Bezeichnung | <input type="text" value="RDP-HV1"/> |
| Protokoll | <input type="text" value="TCP"/> |
| Port an Gerät | <input type="text" value="3389"/> bis Port <input type="text" value="3389"/> |
| Port extern gewünscht (IPv4) | <input type="text" value="39328"/> |

So konnte ich von außen im Notfall direkt auf meine HyperV-Server zugreifen und die VM PFSense reparieren bzw. starten. Und wer scannt schon die higher Ports...

Mittlerweile verwende ich 2 PFSense-VMs, die als CARP-Cluster alle Funktionen für den Netzwerkschutz übernehmen. Je eine läuft auf einem HyperV-Server. Somit war kein Cluster mehr erforderlich. Nur was soll ich sagen ... die beiden Portfreigaben für den RDP-Zugriff hatte ich einfach vergessen!

Der Angriff

Die Schwachstelle

Aber ich hatte ja eine Menge an **Schutzvorkehrungen** getroffen:

- eine Netzwerksegmentierung mit der PFSense und ihrer sauber konfigurierten Firewall
- ein Geoblocker, der Verbindungen nur aus bestimmten geographischen Regionen zulässt werkelt ebenfalls auf der PFSense
- der Einsatz eines Snort IPS für die Analyse der erlaubten Verbindungen in der PFSense mit einem PowerShell-Monitoring/Alerting per Mail
- eine Vielzahl an Richtlinien zur Absicherung meiner Systeme
- sogar ein Microsoft ATA (Advanced Threat Analytics) war im Einsatz – es sollte Anomalien beim Anmelden und beim Ressourcenzugriff erkennen und melden
- der Zugriff auf die beiden HyperV-Server war durch MFA abgesichert

Nur leider hatte die Konfiguration eine **Schwachstelle**: alle Netzwerkschutzkomponenten wurden von der PFSense ausgeführt. Und meine beiden HyperV-Hosts hatten einen **Bypass**!

Der Sicherheitsvorfall

Eines Tages – ich führte Routinearbeiten an meinen Servern durch – stieß ich dann in den Eventlogs meines DomainControllers auf Unregelmäßigkeiten:

| Ereignistyp | Ereignis... | Quelle | Protokoll | Letzte Stu... | 24 Stunden | 7 Tage |
|--------------------------------|-------------|------------------|------------|---------------|------------|--------------|
| Kritisch | - | - | - | 0 | 0 | 0 |
| Fehler | - | - | - | 0 | 14 | 3.846 |
| Warnung | - | - | - | 0 | 14 | 102 |
| Informationen | - | - | - | 492 | 9.987 | 17.984 |
| Überwachung erfolgreich | - | - | - | 1.791 | 74.185 | 178.087 |
| Überwachung gescheitert | - | - | - | 4 | 5.142 | 8.368 |
| | 4625 | Microsoft Win... | Sicherheit | 0 | 2 | 2 |
| | 4768 | Microsoft Win... | Sicherheit | 0 | 1 | 1 |
| | 4769 | Microsoft Win... | Sicherheit | 4 | 5 | 8 |
| | 4771 | Microsoft Win... | Sicherheit | 0 | 15 | 22 |
| | 4776 | Microsoft Win... | Sicherheit | 0 | 5117 | 8333 |
| | 4822 | Microsoft Win... | Sicherheit | 0 | 2 | 2 |

Ich kenne meine Infrastruktur. Diese Anzahl an AuditFailures ist nicht normal. Also ging ich in die Analyse. Und wurde überrascht:

| Ebene | Datum und Uhrzeit | Quelle | Ereignis-ID | Aufgabenkategorie |
|----------------------|----------------------------|--|-------------|---|
| Informationen | 20.07.2019 18:33:18 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:18 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:16 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:15 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:13 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:11 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:09 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:07 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:06 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:05 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |
| Informationen | 20.07.2019 18:33:03 | Microsoft Windows security audit... | 4776 | Überprüfung der Anmeldeinform... |

Ereignis 4776, Microsoft Windows security auditing.

Allgemein Details

Es wurde versucht, die Anmeldeinformationen für ein Konto zu überprüfen.

Authentifizierungspaket: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Anmeldekonto: **besprechung**
 Arbeitsstation: **MSTSC**
 Fehlercode: **0xC0000064**

Protokollname: Sicherheit
 Quelle: Microsoft Windows security
 Ereignis-ID: **4776**
 Ebene: Informationen
 Benutzer: Nicht zutreffend
 Vorgangscod: Info

Protokolliert: 20.07.2019 18:33:05
 Aufgabenkategorie: Überprüfung der Anmeldeinformationen
 Schlüsselwörter: **Überwachung gescheitert**
 Computer: WS-DC2.ws.its

Und jeder Eintrag listete ein anderes Anmeldekonto. Ganz klar: hier versuchte jemand mit verschiedenen Benutzernamen (und Passwörtern) einen **BruteForce-Angriff** auf meine Infrastruktur!

Die Reaktion auf den Angriff

Wie reagiert man in einem solchen Fall richtig? Durchschlägt man mit der Axt alle Verkabelungen? Oder rennt man wild mit den Armen wedelnd schreiend auf dem Gang umher? ☺ Spass beiseite: überlegt euch bitte VOR einem Sicherheitsvorfall, wie man am besten reagieren kann!

In meinem Fall wusste ich sehr schnell, dass es sich um eine Bruteforce-Angriffe handelte. Dabei werden Benutzernamen und Passwörter durchprobiert, bis es einen Treffer gibt. Mir konnte also nichts passieren, denn:

- mit dem falschen Benutzernamen gibt es keinen Zutritt
- mit dem richtigen Benutzernamen greift die Lockout-Policy nach x fehlerhaften Anmeldungen

Und dann kommen meine zusätzlichen Schutzmaßnahmen.

Ich hatte also Zeit und vor allem die Gelegenheit, mir den Angriff mal etwas näher anzusehen. Zunächst wollte ich herausfinden, welcher Service auf welchem Server für das bruteforcen mißbraucht wurde – der **Patient Null**. Nur leider findet man in dem Eventlog auf dem DomainController keinen Hinweis ab den „Auftragegeber“ der Anmeldeüberprüfung. Aber ich habe ein anderes Script, das mir jeden Tag über alle Server eine Zusammenfassung der letzten 24 Stunden liefert. Und darunter befinden sich auch die kumulierten Eventlogs je Server:




Fr 19.07.2019 04:49
 [Redacted]@ws-its.de
 ServerMonitor

An Logmails
 offen

wichtige Ereignisse (der letzten 24h die Top 30)

| Server | Name | Count |
|---------|--|-------|
| WS-RDS3 | Error, SRMSVC, 2147753989, "Fehler beim Ressourcen-Managerdienst für Dateiserver: Unerwarteter Fehler. Fehlerspezifische Deta" | 8633 |
| WS-DC2 | FailureAudit, Microsoft-Windows-Security-Auditing, 4776, "Es wurde versucht, die Anmeldeinformationen für ein Konto zu überprüfen. Authentifizierungspaket:" | 7673 |
| WS-HV2 | FailureAudit, Microsoft-Windows-Security-Auditing, 4776, "Es wurde versucht, die Anmeldeinformationen für ein Konto zu überprüfen. Authentifizierungspaket:" | 5886 |
| WS-HV2 | FailureAudit, Microsoft-Windows-Security-Auditing, 4625, "Fehler beim Anmelden eines Kontos. Antragsteller: Sicherheits-ID: S-1-0-0 Kontoname: - Ko" | 5886 |
| WS-HV1 | FailureAudit, Microsoft-Windows-Security-Auditing, 4776, "Es wurde versucht, die Anmeldeinformationen für ein Konto zu überprüfen. Authentifizierungspaket:" | 1784 |
| WS-HV1 | FailureAudit, Microsoft-Windows-Security-Auditing, 4625, "Fehler beim Anmelden eines Kontos. Antragsteller: Sicherheits-ID: S-1-0-0 Kontoname: - Ko" | 1784 |
| WS-DPM | Warning, SQLAgent\$DPM, 1073742032, "SQL Server Scheduled Job 'd21d5bec-b1f7-4c3b-838d-d6a892ab6562' (0xB2DEA83C1E435049A8F8836F533FEEB1)" | 48 |
| WS-IPM | 0, Software Protection Platform Service, 1073742726 | 27 |
| WS-FS2 | 0, Software Protection Platform Service, 1073742726 | 27 |
| WS-FS2 | 0, Software Protection Platform Service, 1073742727 | 27 |

2 Treffer sind erkennbar: WS-HV1 und WS-HV2 – meine beiden HyperV-Hosts. Auf diesen fand ich die Eventlogs:



Ereignisanzeige (Lokal)

Übersicht und Zusammenfassung

Übersicht

Zusammenfassung der administrativen Ereignisse

| Ereignistyp | Ereignis... | Quelle | Protokoll | Letzte Stu... | 24 Stunden | 7 Tage |
|---------------------------|-------------|------------------|------------|---------------|------------|--------|
| Kritisch | - | - | - | 0 | 0 | 0 |
| ☒ Fehler | - | - | - | 1 | 20 | 133 |
| ☒ Warnung | - | - | - | 1 | 11 | 70 |
| ☒ Informationen | - | - | - | 33 | 767 | 5.193 |
| ☒ Überwachung erfolgreich | - | - | - | 98 | 2.107 | 18.684 |
| ☒ Überwachung gescheitert | - | - | - | 0 | 0 | 6.398 |
| | 4625 | Microsoft Win... | Sicherheit | 0 | 0 | 3199 |
| | 4776 | Microsoft Win... | Sicherheit | 0 | 0 | 3199 |

| Ereignisanzeige (Lokal) | | | | | | |
|--|-------------|------------------|------------|---------------|------------|--------|
| Übersicht und Zusammenfassung | | | | | | |
| Übersicht | | | | | | |
| Zusammenfassung der administrativen Ereignisse | | | | | | |
| Ereignistyp | Ereignis... | Quelle | Protokoll | Letzte Stu... | 24 Stunden | 7 Tage |
| Kritisch | - | - | - | 0 | 0 | 0 |
| ⊕ Fehler | - | - | - | 1 | 27 | 267 |
| ⊕ Warnung | - | - | - | 1 | 20 | 152 |
| ⊕ Informationen | - | - | - | 26 | 662 | 4.625 |
| ⊕ Überwachung erfolgreich | - | - | - | 117 | 2.468 | 9.101 |
| ⊖ Überwachung gescheitert | - | - | - | 0 | 10.184 | 26.657 |
| | 4625 | Microsoft Win... | Sicherheit | 0 | 5092 | 13329 |
| | 4776 | Microsoft Win... | Sicherheit | 0 | 5092 | 13328 |

Und in den Details gab es die Antwort auf den Ursprung:

 Ereigniseigenschaften - Ereignis 4625, Microsoft Windows security auditing.

Allgemein | Details

Fehler beim Anmelden eines Kontos.

Antragsteller:

- Sicherheits-ID: NULL SID
- Kontoname: -
- Kontodomäne: -
- Anmelde-ID: 0x0

Anmeldetyp: 3

Konto, für das die Anmeldung fehlgeschlagen ist:

- Sicherheits-ID: NULL SID
- Kontoname: besprechung
- Kontodomäne: -

Fehlerinformationen:

- Fehlerursache: Unbekannter Benutzername oder ungültiges Kennwort.
- Status: 0xC000006D
- Unterstatus: 0xC0000064

Prozessinformationen:

- Aufrufprozess-ID: 0x0
- Aufrufprozessname: -

Netzwerkinformationen:

- Arbeitsstationsname: MSTSC
- Quellnetzwerkadresse: 185.175.93.4
- Quellport: 0

Detaillierte Authentifizierungsinformationen:

- Anmeldeprozess: NtLmSsp
- Authentifizierungspaket: NTLM
- Übertragene Dienste: -

Protokollname: Sicherheit

Quelle: Microsoft Windows security | Protokolliert: 20.07.2019 18:33:05

Ereignis-ID: 4625 | Aufgabenkategorie: Anmelden

Ebene: Informationen | Schlüsselwörter: Überwachung gescheitert

Benutzer: Nicht zutreffend | Computer: WS-HV2.ws.its

Die Frage „Wurden auch andere Quell-IP-Adressen verwendet?“ konnten ein paar Zeilen PowerShell-Code beantworten:

```

1 $Logs = Get-WinEvent -FilterHashtable @{ Logname="Security" ; ID=4625 ; Starttime=(Get-Date -Date '20.07.2019') }
2 $Logs |
3   ForEach-Object { $_.message -split "`n`n" | Select-String 'Quelle[netzwerk]adresse' } |
4     Group-Object |
5       Format-Table -Property count,name -AutoSize


```

| Count | Name |
|-------|---------------------------------------|
| 5092 | Quelle[netzwerk]adresse: 185.175.93.4 |

Und wer ist der Angreifer?

https://whoer.net/checkwhois

IP address: 185.175.93.4

| | | | |
|-----------|--|---------------|-------------------------------|
| Location: |  Spain (ES), Europe | Hostname: | N/A→N/A |
| Region: | N/A | IP range: | 185.175.92.0 - 185.175.93.255 |
| City: | N/A | ISP: | Content Generation Media S.I. |
| ZIP: | N/A | Organization: | Content Generation Media S.I. |

| | | | |
|------------|----|--------|-----|
| Blacklist: | No | Zone: | N/A |
| TOR: | No | Local: | N/A |

[Hide](#)

```

inetnum      185.175.93.0 - 185.175.93.255
netname     C1oud-services
descr       C1oud-services Network
country     RU
org         ORG-ISEB2-RIPE
admin-c     KAES4-RIPE
tech-c      KAES4-RIPE
abuse-c     ACRO20239-RIPE
status      ASSIGNED PA
mnt-by      CONTENTGH-MNT
mnt-lower   protonserv-mnt
mnt-domains protonserv-mnt
mnt-routes  protonserv-mnt
created     2019-07-12T11:40:41Z
last-modified 2019-07-12T11:40:41Z
source      RIPE

organisation ORG-ISEB2-RIPE
org-name     IP Kirichenko Andrey Evgenievich
org-type     OTHER
address     398004, Russian Federation, Lipetsk,Teperika str 13
abuse-c     ACRO20239-RIPE
mnt-ref     ru-ip84-1-mnt
mnt-ref     CONTENTGH-MNT
mnt-by      ru-ip84-1-mnt
created     2018-11-12T03:43:05Z
last-modified 2019-07-12T11:35:07Z
source      RIPE # Filtered

person      Kirichenko Andrey Evgenievich
address     398004, Russian Federation, Lipetsk,Teperika str 13
phone       +380689301231
nic-hdl     KAES4-RIPE
mnt-by      ru-ip84-1-mnt
created     2018-11-27T03:11:38Z
last-modified 2019-06-03T05:46:09Z
source      RIPE

route       185.175.93.0/24
origin      AS35582
mnt-by      protonserv-mnt
created     2019-07-12T11:53:34Z
last-modified 2019-07-12T11:53:34Z
source      RIPE

```

Sieht nicht sehr vielversprechend aus: außer einem russischen Namen gibt es keinen Hinweis. Manch einer würde sagen: die Russen waren es. Das würde ich nicht empfehlen. Wir fahren einen Nissan, sind aber keine Asiaten. Und eigentlich spielt es auch keine Rolle, da es sich an der Vorgehensweise bewertet nach einem **gestreuten Angriff** aussieht. Das wird auch deutlich, wenn man sich die verwendeten Benutzernamen anschaut:

```

7 $Logs |
8   ForEach-Object { $_.message -split "`r`n" | Select-String 'Kontoname' } |
9   Group-Object |
10  Sort-Object -Property count |
11  Format-Table -Property count,name -AutoSize

```

```

4  Kontoname:      flowerbis
4  Kontoname:      remote
4  Kontoname:      karlheinz
4  Kontoname:      gemeinde-parsdorf
4  Kontoname:      gws bis user 01
4  Kontoname:      dtz
4  Kontoname:      kimadmin804
4  Kontoname:      kai
4  Kontoname:      abteilung sprantal
5  Kontoname:      reception
5  Kontoname:      austausch-ftp
5  Kontoname:      p raxi s_sc h
5  Kontoname:      openssm
5  Kontoname:      bianca schneider
5  Kontoname:      sap admin
5  Kontoname:      rahim
5  Kontoname:      datevl
5  Kontoname:      dario klisanc
5  Kontoname:      c19999.8
5  Kontoname:      peter fierlinger
5  Kontoname:      rk1
5  Kontoname:      kranz torsten
5  Kontoname:      printer maestro remote
5  Kontoname:      dmitry_kamnev
5  Kontoname:      dorothee glodcner
6  Kontoname:      remousr
6  Kontoname:      support.admin
6  Kontoname:      mbarda
6  Kontoname:      heinz.burtscheidt
6  Kontoname:      jbecker
6  Kontoname:      ramona.krakau

```

Spannend finde ich die Tatsache, dass hier zwischen einigen kryptischen Namen auch deutsche Namen verwendet wurden. Ebenso die typischen Servicenamen „datev“ und „sap“, aber auch „support“ und „admin“ kommen nicht zu kurz. Und die Gemeinde Parsdorf ist auch nicht so weit weg. Ganz offensichtlich versuchen die Angreifer durch zielorientierte Benutzernamen ihre Chancen zu erhöhen!

Zuletzt wage ich noch einen kleinen Blick auf den Angreifer mit nmap (ich sollte mal wieder aktualisieren):

```

PS C:\Program Files (x86)\Nmap> .\nmap -sV -T4 -O -A -v -F -Pn --version-light 185.175.93.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-21 15:44 Mitteleuropäische Sommerzeit
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 11.01s elapsed
Initiating SYN Stealth Scan at 15:45

Scanning 185.175.93.4 [100 ports]
Discovered open port 80/tcp on 185.175.93.4
Discovered open port 21/tcp on 185.175.93.4
Discovered open port 1720/tcp on 185.175.93.4
Discovered open port 3389/tcp on 185.175.93.4
Discovered open port 445/tcp on 185.175.93.4
Discovered open port 135/tcp on 185.175.93.4
Discovered open port 139/tcp on 185.175.93.4
Discovered open port 5800/tcp on 185.175.93.4
Discovered open port 9999/tcp on 185.175.93.4
Discovered open port 5432/tcp on 185.175.93.4
Discovered open port 2121/tcp on 185.175.93.4
Discovered open port 6000/tcp on 185.175.93.4

```

```

Increasing send delay for 185.175.93.4 from 0 to 5 due to max_successful_ryno increase to 5
Discovered open port 3128/tcp on 185.175.93.4
Increasing send delay for 185.175.93.4 from 5 to 10 due to max_successful_ryno increase to 6
Warning: 185.175.93.4 giving up on port because retransmission cap hit (6).
Completed SYN Stealth Scan at 15:45, 14.24s elapsed (100 total ports)
Initiating Service scan at 15:45

Scanning 13 services on 185.175.93.4
Completed Service scan at 15:46, 34.71s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 185.175.93.4
Retrying OS detection (try #2) against 185.175.93.4
Initiating Traceroute at 15:46
Completed Traceroute at 15:46, 3.05s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 15:46
Completed Parallel DNS resolution of 8 hosts. at 15:46, 16.50s elapsed
NSE: Script scanning 185.175.93.4.
Initiating NSE at 15:46
Completed NSE at 15:46, 33.28s elapsed
Initiating NSE at 15:47
Completed NSE at 15:47, 0.01s elapsed
Nmap scan report for 185.175.93.4
Host is up (0.060s latency).
Not shown: 48 filtered ports, 39 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp?
80/tcp    open  tcpwrapped
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title.
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1720/tcp  open  tcpwrapped
2121/tcp  open  tcpwrapped
3128/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
|_ ssl-cert: Subject: commonName=WIN-60DSI8SGOL6
|_ Issuer: commonName=WIN-60DSI8SGOL6
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2019-04-17T16:14:17
| Not valid after: 2019-10-17T16:14:17
| MD5: 5f51 ef08 008c 93b9 9bf5 c506 c4c9 a467
|_SHA-1: 99d7 19d3 6400 6b9e 29d6 7f76 a73e 816b 2415 5969
|_ssl-date: 2019-07-21T13:46:25+00:00; -1s from scanner time.
5432/tcp  open  tcpwrapped
5800/tcp  open  tcpwrapped
6000/tcp  open  tcpwrapped
|_x11-access: ERROR: Script execution failed (use -d to debug)
9999/tcp  open  tcpwrapped
OS fingerprint not ideal because: Host distance (12 network hops) is greater than five
No OS matches for host
Network Distance: 12 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -2s

```



```

| nbstat: NetBIOS name: WIN-60DSI8SGOL6, NetBIOS user: <unknown>, NetBIOS MAC: 18:66:da:a2:9c:ea
(Dell)
| Names:
|   WIN-60DSI8SGOL6<20>  Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
|_  WIN-60DSI8SGOL6<00>  Flags: <unique><active>
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-07-21 15:46:25
|_  start_date: 2019-04-29 09:38:14

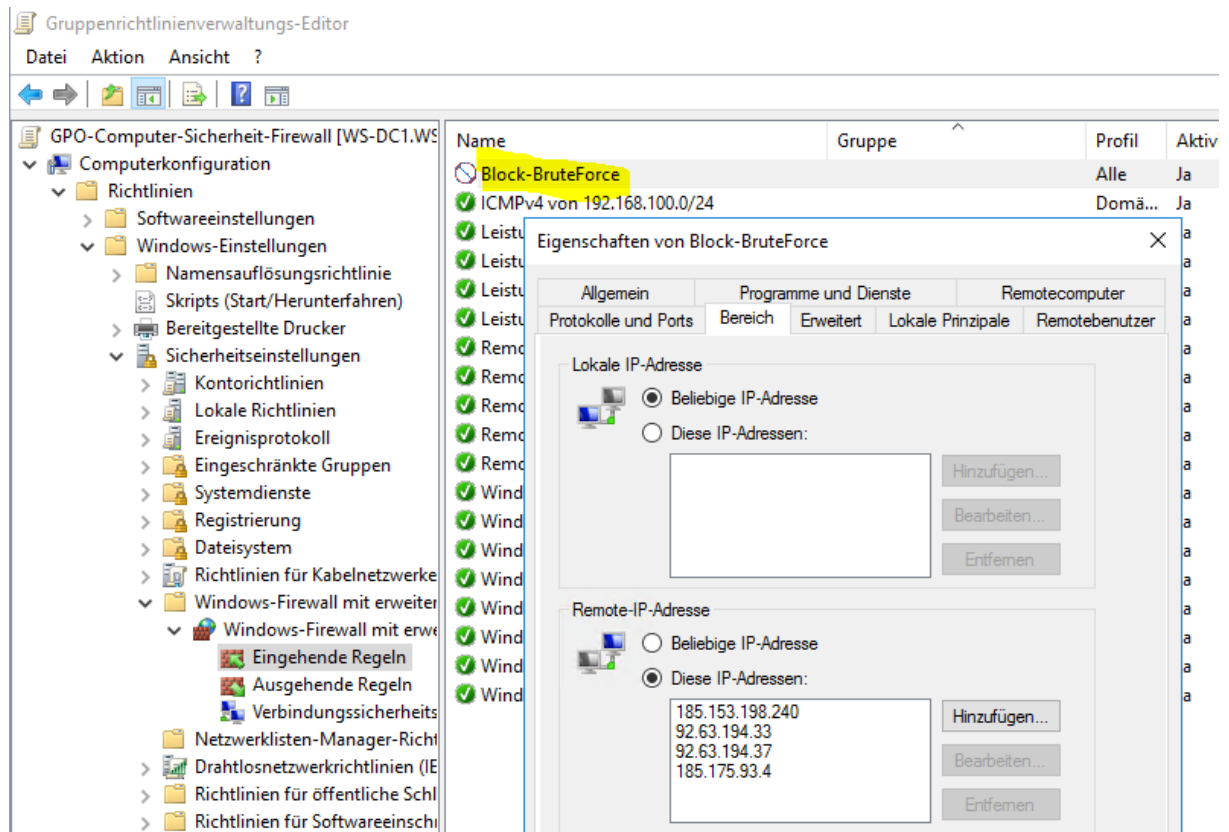
TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   2.00 ms   192.168.43.230
2   ...
3   29.00 ms  10.218.33.61
4   35.00 ms  10.218.35.137
5   37.00 ms  10.218.34.26
6   ... 7
8   46.00 ms  de-cix1.RT.ACT.FKT.DE.retn.net (80.81.192.73)
9   70.00 ms  ae0-1.RT.TLP.SOF.BG.retn.net (87.245.232.126)
10  65.00 ms  GW-BelCloud.retn.net (87.245.248.211)
11  ...
12  68.00 ms  185.175.93.4

NSE: Script Post-scanning.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 136.47 seconds
      Raw packets sent: 499 (24.424KB) | Rcvd: 181 (8.216KB)

```

Hier zeigt sich, dass die Maschine auf der anderen Seite mal so richtig viele offene Ports hat. Und alleine die Ports 135, 3389, 445 genügen mir für eine Vermutung: das ist ein Windows Rechner, der direkt am Internet hängt. Und dieser wurde wahrscheinlich über SMB (445) oder RDP (3389) kompromittiert und soll mich nun als Bot weiter infizieren.

Somit werde ich gar nicht direkt angegriffen und eine weitergehende Forensik oder gar eine Anzeige gegen unbekannt erscheint sinnfrei. Also beende ich den Angriff durch eine hübsche GPO:



Ein gpupdate später war Ruhe. 😊

Möglichkeiten der Erkennung

Das Versagen von Microsoft ATA

Was mich neben der Tatsache, dass ich mit der Freigabe des Ports für RDP eine fehlerhafte Konfiguration vorgenommen hatte, besonders nerfte: Ich hätte den Angriff eigentlich durch Microsoft ATA mitbekommen sollen. Denn dieses Tool hat sich an alle meine DomainController angeschlossen und sollte die „Unregelmäßigkeit“ der Anmeldungen erkennen und melden. Doch ich bekam keine Warnung. Und im offiziellen ATA-Handbuch von Microsoft fand ich dann die Erklärung dazu:

<https://docs.microsoft.com/de-de/advanced-threat-analytics/suspicious-activity-guide>

Verdächtige Authentifizierungsfehler

Beschreibung

Bei einem Brute-Force-Angriff versucht ein Angreifer, sich mit vielen verschiedenen Kennwörtern für verschiedene Konten anzumelden, bis ein korrektes Kennwort für mindestens ein Konto gefunden wird. Sobald eines gefunden wurde, kann sich der Angreifer mit diesem Konto anmelden.

In dieser Erkennung wird eine Warnung ausgelöst, wenn viele Authentifizierungsfehler mit Kerberos oder der integrierten Windows-Authentifizierung auftreten. Dies kann entweder horizontal mit einem kleinen Satz von Kennwörtern für viele Benutzer oder vertikal mit einem großen Satz von Kennwörtern für wenige Benutzer geschehen. Auch eine beliebige Kombination dieser beiden Optionen ist möglich. **Der Mindestzeitraum, bevor eine Warnung ausgelöst werden kann, beträgt eine Woche.**

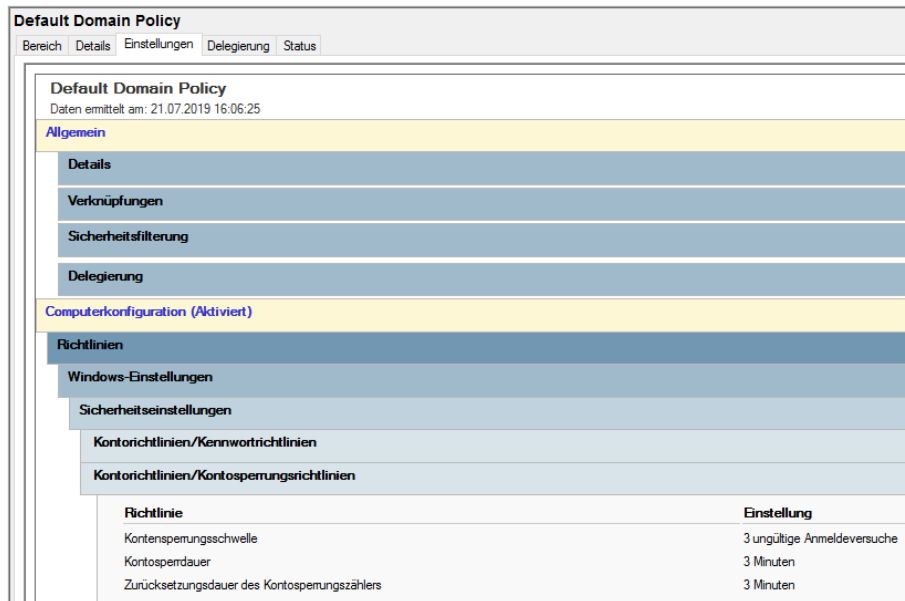
Ich kanns nicht fassen! Eine Woche würde ATA einfach schweigen. Bei der Angriffswelle wurde im Schnitt eine Anmeldung pro Sekunde versucht. Das macht dann 604.800 Anmeldeversuche, bevor eine Warnung aufploppt!!!

Hinweis: die Software des Hackers war nicht besonders clever, denn man kann an den Antwortzeiten einer Anmeldung erkennen, ob der Benutzername existiert oder nicht. Somit könnte in einer ersten Welle ein gültiger Anmeldename gesucht werden und in einer zweiten würde man dann alle möglichen Passwörter versuchen – natürlich vorsortiert nach deren Häufigkeit für eine bestimmte Zielgruppe. Und nun überlegen wir mal, an welcher Stelle in dieser Liste die Passwörter der Benutzer stehen. Vielleicht vor Nummer 604.800? ...

Meine PFSense konnte mir nicht helfen, denn diese hatte ich ja selber umgangen. Was kann also helfen?

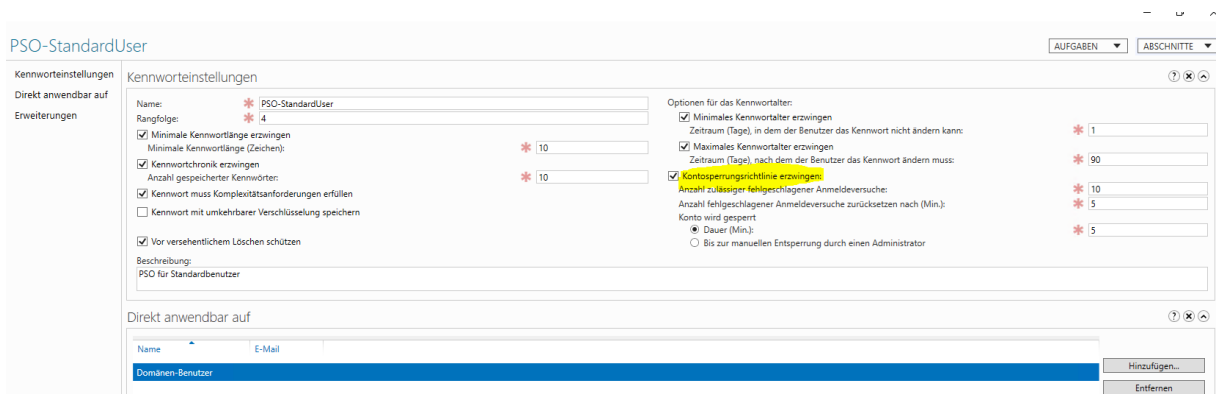
Lockouts

Ganz klar: fehlgeschlagene Anmeldungen von gültigen Benutzerkonten müssen nach dem Überschreiten einer Mindestanzahl zu einer Kontosperrung führen. Dieses Lockout-Feature ist fester Bestandteil der Kennwortrichtlinie in einer AD-Infrastruktur. Man muss es nur sinnvoll konfigurieren. Traditionell gibt es die Variante mit der Gruppenrichtlinie:



| Richtlinie | Einstellung |
|---|-----------------------------|
| Kontensperungsschwelle | 3 ungültige Anmeldeversuche |
| Kontosperrdauer | 3 Minuten |
| Zurücksetzungsdauer des Kontosperrungszählers | 3 Minuten |

Seit Windows Server 2008 gibt es aber auch die Password Setting Objects (PSO) oder auch Finegrained Password Policies:



In meinem Fall wird ein Standardkonto nach 10 Fehlversuchen für 5 Minuten gesperrt. Damit ist kein Bruteforce-Angriff möglich. 😊

Eventlog-Analyse

Viel eleganter ist es aber, wenn man den Angriff aktiv gemeldet bekommt. Dazu habe ich mir ein PowerShell-Script geschrieben. Dieses überwacht die Security-Eventlogs aller meiner DomainController auf bestimmte fehlgeschlagene Audits und trägt die Informationen in CSV-Dateien zusammen. Aus diesen Informationen kann das Script Anomalien ableiten und dann per Mail Alarm schlagen.

Allein an den CSV-Dateien kann man schon Angriffe erkennen:

SecEv-Monitor > CSV

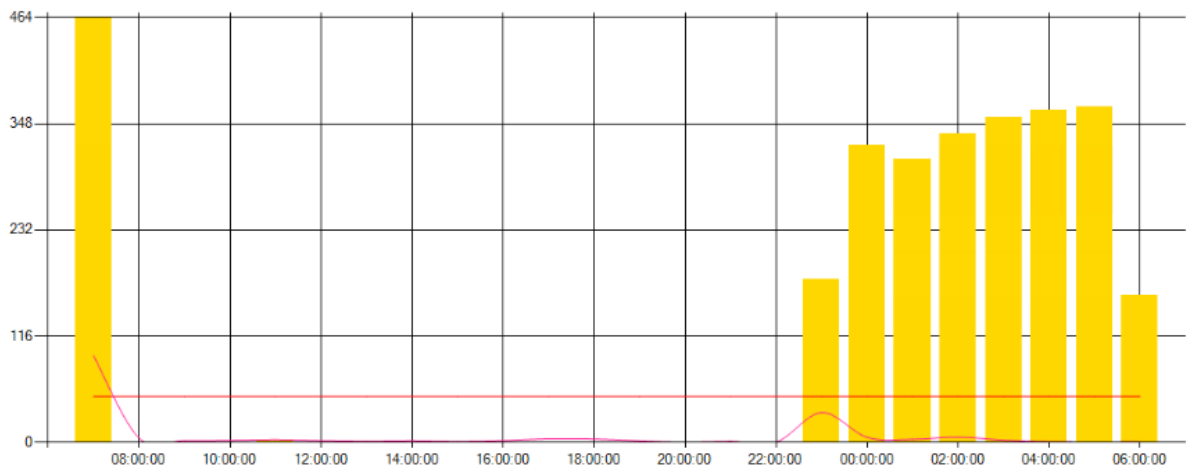
| Name | Änderungsdatum | Typ | Größe |
|----------------|------------------|-----------|----------|
| 2019-06-17.csv | 17.06.2019 23:51 | CSV-Datei | 17 KB |
| 2019-06-18.csv | 18.06.2019 23:53 | CSV-Datei | 17 KB |
| 2019-06-19.csv | | | |
| 2019-06-20.csv | | | |
| 2019-06-21.csv | | | |
| 2019-06-22.csv | | | |
| 2019-06-23.csv | | | |
| 2019-06-24.csv | | | |
| 2019-06-25.csv | | | |
| 2019-06-26.csv | | | |
| 2019-06-27.csv | | | |
| 2019-06-28.csv | | | |
| 2019-06-29.csv | | | |
| 2019-06-30.csv | | | |
| 2019-07-01.csv | | | |
| 2019-07-02.csv | | | |
| 2019-07-03.csv | | | |
| 2019-07-04.csv | | | |
| 2019-07-05.csv | | | |
| 2019-07-06.csv | | | |
| 2019-07-07.csv | 07.07.2019 22:47 | CSV-Datei | 22 KB |
| 2019-07-08.csv | 08.07.2019 23:27 | CSV-Datei | 47 KB |
| 2019-07-09.csv | 09.07.2019 23:49 | CSV-Datei | 28 KB |
| 2019-07-10.csv | 10.07.2019 23:48 | CSV-Datei | 22 KB |
| 2019-07-11.csv | 11.07.2019 23:59 | CSV-Datei | 17 KB |
| 2019-07-12.csv | 12.07.2019 23:47 | CSV-Datei | 25 KB |
| 2019-07-13.csv | 13.07.2019 23:15 | CSV-Datei | 39 KB |
| 2019-07-14.csv | 14.07.2019 17:23 | CSV-Datei | 18 KB |
| 2019-07-15.csv | 15.07.2019 22:55 | CSV-Datei | 81 KB |
| 2019-07-16.csv | 16.07.2019 23:45 | CSV-Datei | 15 KB |
| 2019-07-17.csv | 17.07.2019 23:52 | CSV-Datei | 1.510 KB |
| 2019-07-18.csv | 18.07.2019 23:59 | CSV-Datei | 2.872 KB |
| 2019-07-19.csv | 19.07.2019 08:38 | CSV-Datei | 472 KB |
| 2019-07-20.csv | 20.07.2019 18:36 | CSV-Datei | 786 KB |
| 2019-07-21.csv | 21.07.2019 16:00 | CSV-Datei | 8 KB |

2019-07-20.csv - Editor

```

Datei Bearbeiten Format Ansicht ?
"2019-07-20 14:57:34";"WS-DC2";"";"service-ata";"4004";"";"NTLM-Auth to target ' WS-CM' blocked";"
"2019-07-20 15:51:10";"WS-DC2";"";"service-ata";"4004";"";"NTLM-Auth to target ' WS-NAS1' blocked".
"2019-07-20 16:09:48";"WS-DC2";"";"af admin";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:09:50";"WS-DC2";"";"brotzeit";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:09:52";"WS-DC2";"";"asafonova";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:09:53";"WS-DC2";"";"barth-rieder";"4776";"0xC0000064";"Es wurde versucht, die Anmel-
"2019-07-20 16:09:55";"WS-DC2";"";"elgar";"4776";"0xC0000064";"Es wurde versucht, die Anmeldeinform-
"2019-07-20 16:09:57";"WS-DC2";"";"hj.sontag";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:09:59";"WS-DC2";"";"at."; "4776";"0xC0000064";"Es wurde versucht, die Anmeldeinforma-
"2019-07-20 16:10:00";"WS-DC2";"";"within the it and is security policy. this stipulation is manda-
"2019-07-20 16:10:02";"WS-DC2";"";"gunmen >";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:10:04";"WS-DC2";"";"schukraftdieter";"4776";"0xC0000064";"Es wurde versucht, die Anr-
"2019-07-20 16:10:05";"WS-DC2";"";"hboehmer";"4776";"0xC0000064";"Es wurde versucht, die Anmeldein-
"2019-07-20 16:10:07";"WS-DC2";"";"ann hollingshead";"4776";"0xC0000064";"Es wurde versucht, die An-
"2019-07-20 16:10:09";"WS-DC2";"";"cschlieker";"4776";"0xC0000064";"Es wurde versucht, die Anmelde-
"2019-07-20 16:10:10";"WS-DC2";"";"leanaa adyanacueaa";"4776";"0xC0000064";"Es wurde versucht, die
    
```

Besonders spannend ist aber die Darstellung und die Interpretation mit der PowerShell:



Die gelben Stapel repräsentieren die Anzahl der Events einer bestimmten Kategorie je Stunde. Die geschwungene Linie ist der Mittelwert der Events der gleichen Kategorie aus den letzten 4 Wochen – natürlich nur vom gleichen Wochentag (das musste einfach sein ☺). Und die rote horizontale Linie ist mein persönlicher Schwellwert für den Alarm. Und dieser ging dann per Mail auch ein. Hier ein Beispiel vom 17.07.2019. Der Angriff startete 20:03 und die erste Mail kam 20:06:



Mi 17.07.2019 20:06

ad@ws.its

SecEV-Monitor - Alarm!

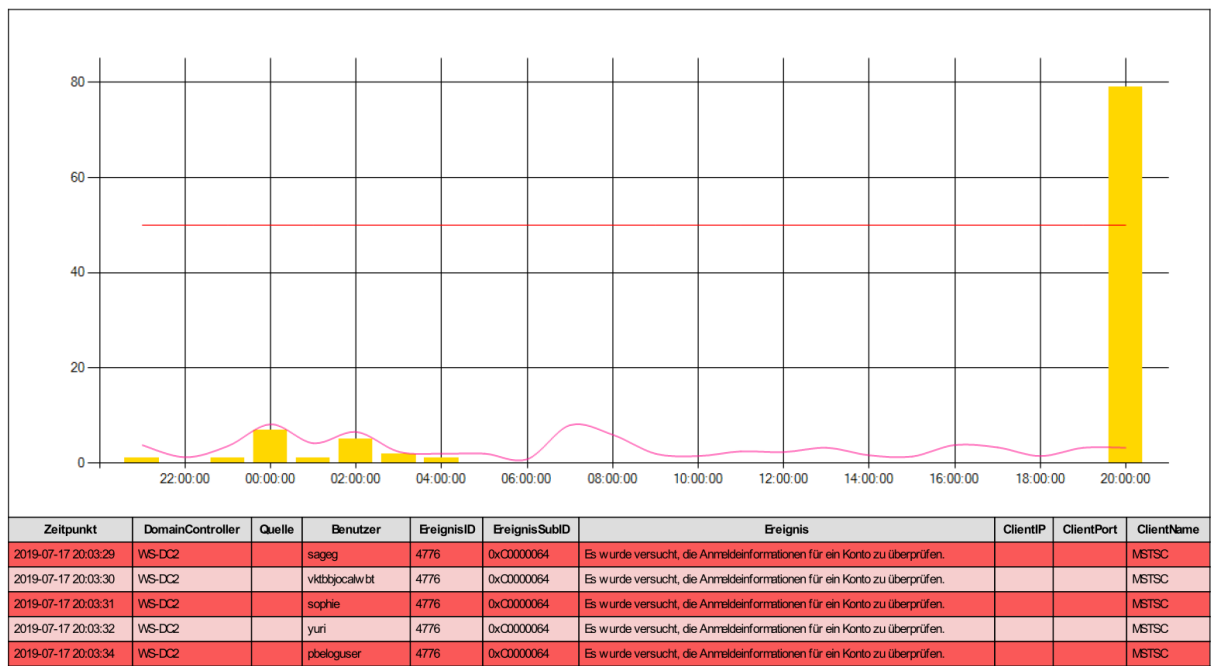
An Logmails

offen



| EventID | Titel | aktuell | Statistik | Limit |
|---------|---|---------|-----------|-------|
| 4740 | Account Lockout | 0 | 0 | 50 |
| 4625 | Account Logon Failure | 0 | 1 | 50 |
| 4776 | BadNTLM | 79 | 3 | 50 |
| 4771 | Kerberos pre-authentication failed | 0 | 1 | 50 |
| 4004 | NTLM-Authentication | 0 | 1 | 10 |
| 4732 | User Added to Sensitive global Group | 0 | 0 | -1 |
| 4728 | User Added to Sensitive Local Group | 0 | 0 | -1 |
| 4756 | User Added to Sensitive universal Group | 0 | 0 | -1 |

61 neue Events: 4776 - BadNTLM



Das Monitoring kann die Angriffsversuche nicht aktiv verhindern – aber der Mailempfänger (also der admin == ich) kann zeitnah reagieren!

Zusammenfassung

Angriffe gehören in unserer vernetzten Welt zum Alltag. Es geht zu bestimmt 99% nicht um euch oder eure Firma. Fast immer sind es automatisierte und gesteuerte Angriffe. Wählt also aus der breiten Palette von Schutzmaßnahmen großzügig aus. Testet und schult euch und eure Kollegen. Baut euch ein Monitoring auf. Und ganz wichtig: überlegt euch schon heute eine Antwort auf die Frage „Wie reagiere ich richtig?“

Stay tuned,
Stephan