Das kleine 1x1 wie und warum ein Unternehmen gehackt wird

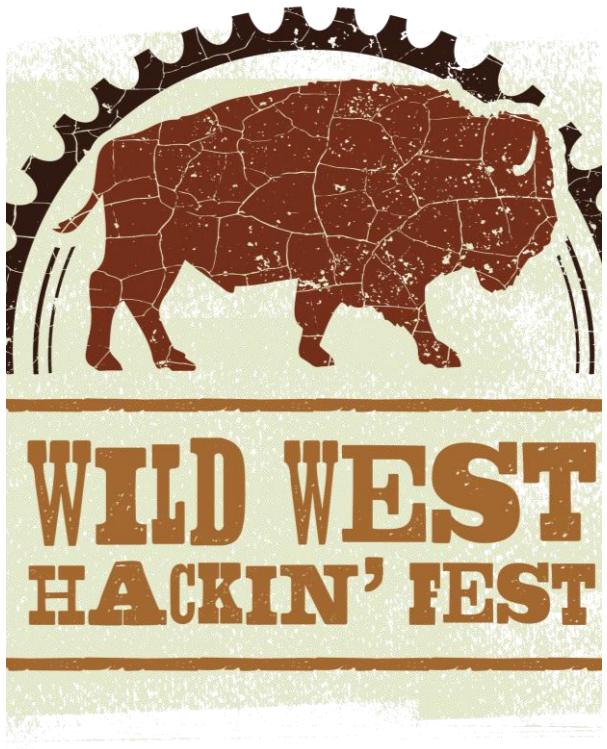
TEMS SECURITY SERVICES

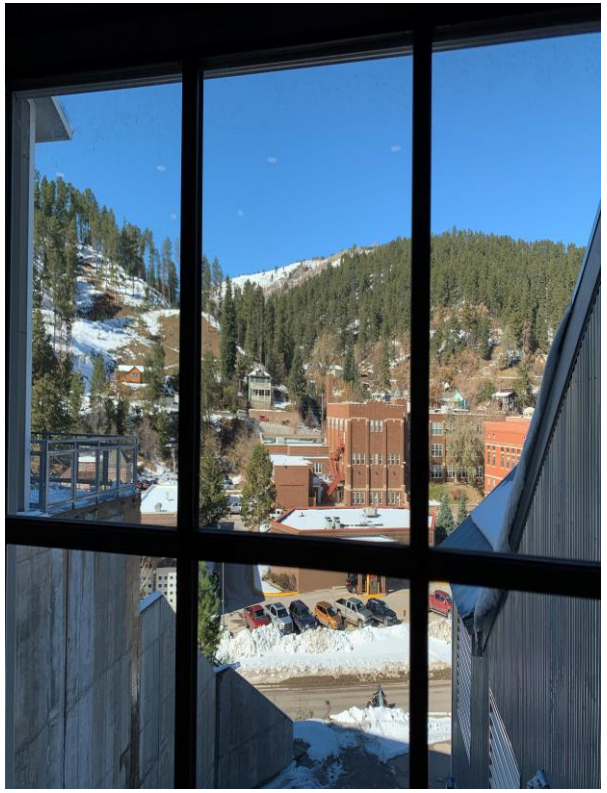
Work smarter
Not harder

Wie sehen wir den IT-Security Wilden Westen

2019 | 2023 (IN 19 TAGEN)

DEADWOOD, SD USA





Wie kann man dem Hacker zum schnellen Erfolg verhelfen

- Sicherung mit dem Domänen Admin einrichten
- Lokale Administratorenrechte für alle, die behaupten es zu benötigen.
- Ein Tier Modell ist einfach zu aufwendig
- Admintätigkeiten vom Arbeitsrechner aus ausführen.

Agenda

- 0 | 1
- Huhn-oder-Ei-Problem des Hackers
- Phishing Methoden
- Cybervorfall 1
- Cybervorfall 2
- Cybervorfall 3
- Cybervorfall 4
- Cybervorfall 5
- Zusammenfassung

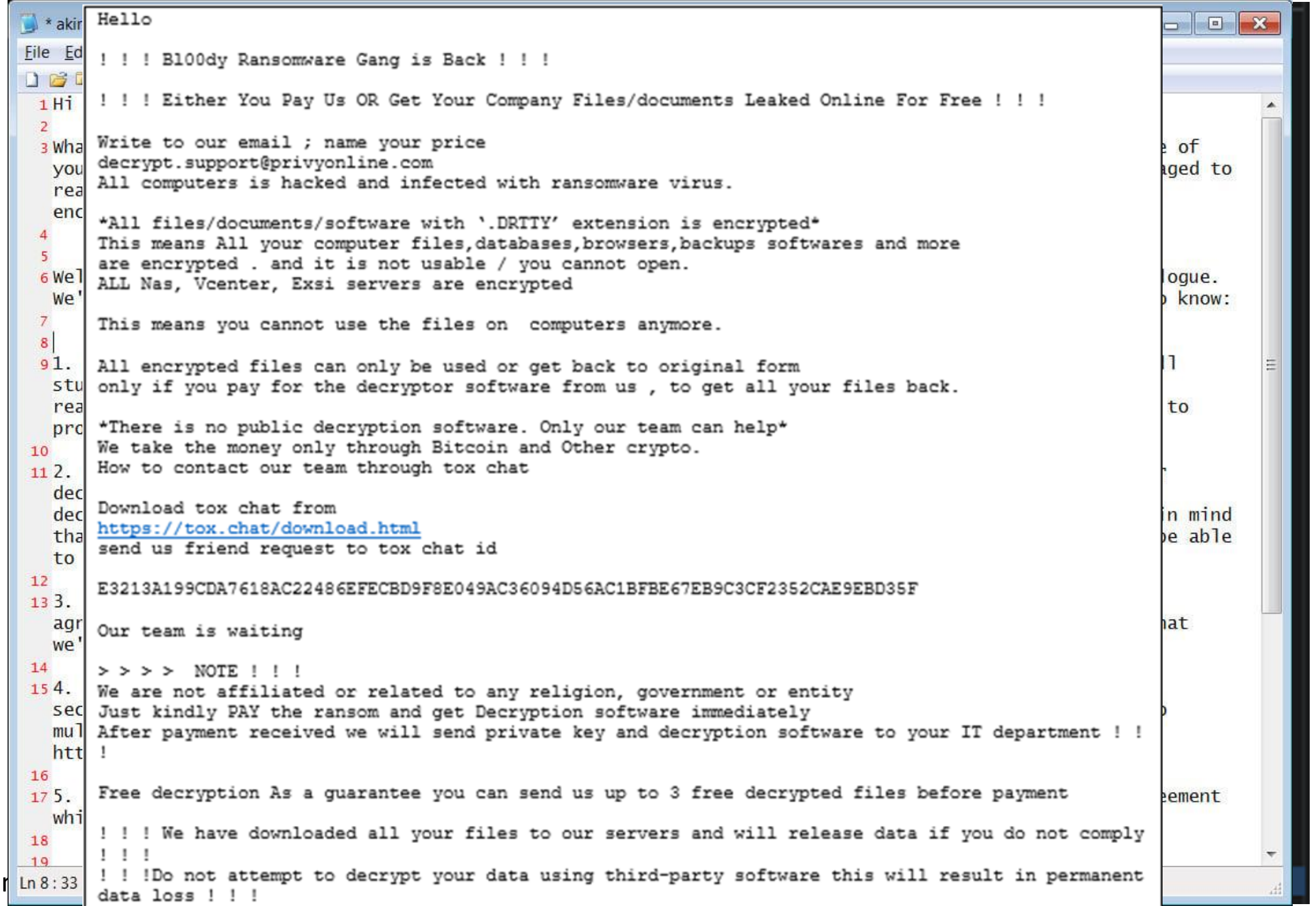
tems security

0 | 1

- Eine Fehlkonfiguration eines Systems
- Ausnutzen einer Schwachstelle einer Software

- **Woraus besteht eigentlich eine Malware / Schadsoftware?**

- Programmteil: Ausnutzen einer Schwachstelle einer Software
- Programmteil: Ausführen von eigener Malware/Schadcode



```
Hello

! ! ! Bl00dy Ransomware Gang is Back ! ! !

! ! ! Either You Pay Us OR Get Your Company Files/documents Leaked Online For Free ! ! !

Write to our email ; name your price
decrypt.support@privyonline.com
All computers is hacked and infected with ransomware virus.

*All files/documents/software with '.DRTTY' extension is encrypted*
This means All your computer files,databases,browsers,backups softwares and more
are encrypted . and it is not usable / you cannot open.
ALL Nas, Vcenter, Exsi servers are encrypted

This means you cannot use the files on  computers anymore.

All encrypted files can only be used or get back to original form
only if you pay for the decryptor software from us , to get all your files back.

*There is no public decryption software. Only our team can help*
We take the money only through Bitcoin and Other crypto.
How to contact our team through tox chat

Download tox chat from
https://tox.chat/download.html
send us friend request to tox chat id

E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F

Our team is waiting

> > > >  NOTE ! ! !
We are not affiliated or related to any religion, government or entity
Just kindly PAY the ransom and get Decryption software immediately
After payment received we will send private key and decryption software to your IT department ! !
!

Free decryption As a guarantee you can send us up to 3 free decrypted files before payment

! ! ! We have downloaded all your files to our servers and will release data if you do not comply
! ! !
! ! !Do not attempt to decrypt your data using third-party software this will result in permanent
data loss ! ! !
```

Quelle: In

Hacking
1x1

tems security

Hacking 1x1

1. Cyber Kill Chain

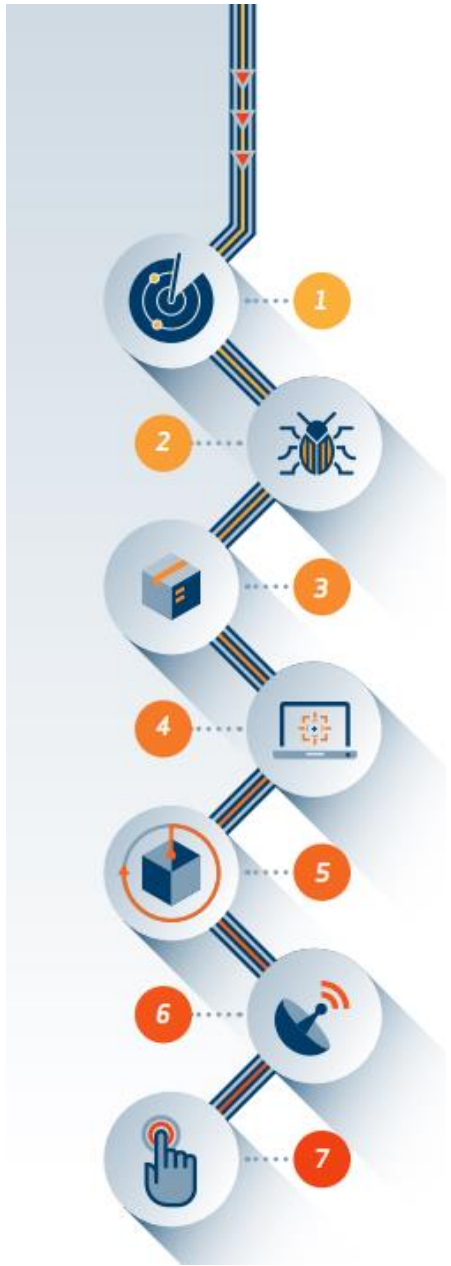
tems security

Hacking workflow

WEAPONIZATION

EXPLOITATION

COMMAND & CONTROL (C2)



RECONNAISSANCE

DELIVERY

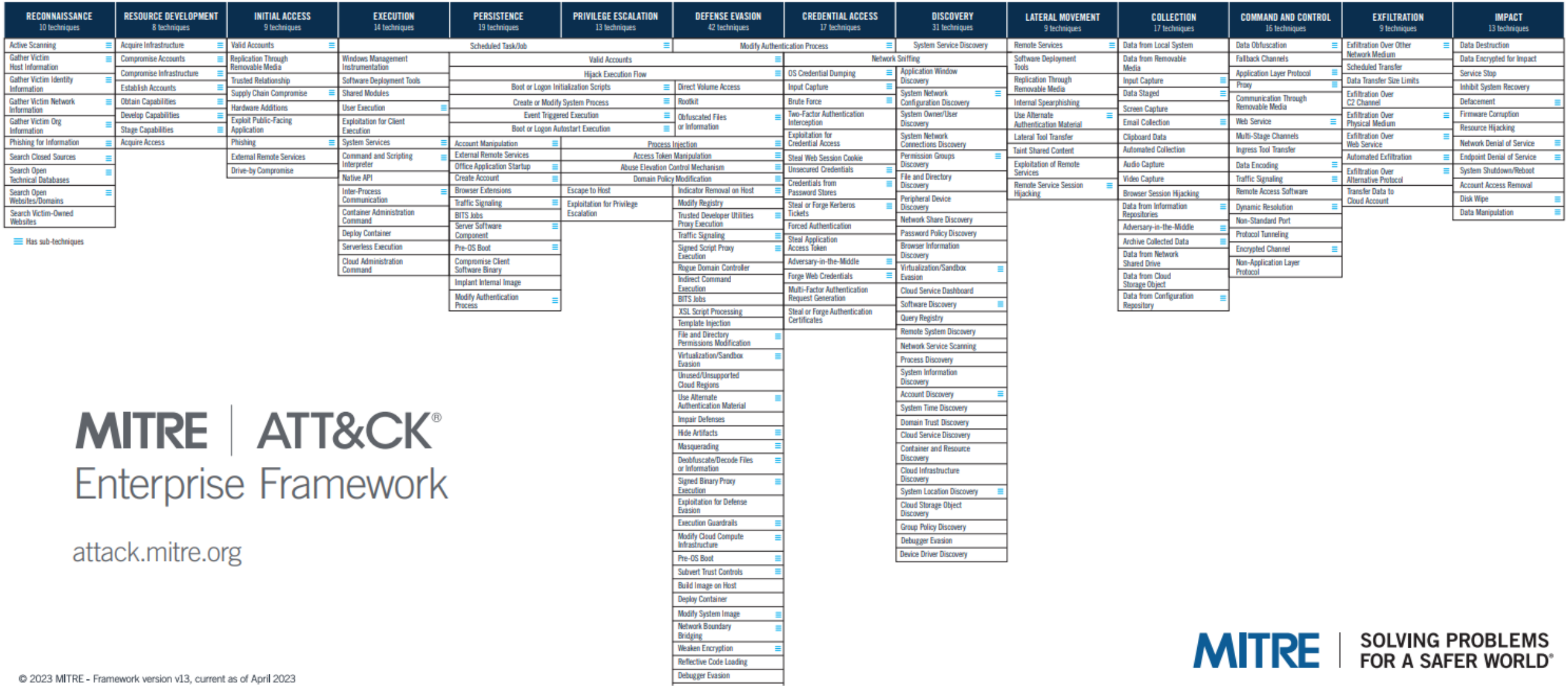
INSTALLATION

ACTIONS ON OBJECTIVES (what`s next?)

Source: https://www.lockheedmartin.com/

THE LOCKHEED MARTIN CYBER KILL CHAIN ®

MITRE ATT&CK Framework



MITRE | ATT&CK®

Enterprise Framework

attack.mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Hacking 1x1

2. Wie finde ich verwundbare Systeme?

tems security

Huhn oder Ei

https://crt.sh/

https://dnsdumpster.com/

https://www.shodan.io/

https://www.exploit-db.com/

https://www.cvedetails.com/vulnerability-list/

Passwörter

tems security

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

tems security

Fall 1

tems security

Fall 1

- Großes Unternehmen
- Über 5000 Mitarbeiter
- Auf 3 Kontinenten

7 von 12

- Zentrales Backup zerstört
- Fileserver verschlüsselt
- E-Mail Server verschlüsselt
- Alle Business Applikationen verschlüsselt

- 14 Tage ohne IT (weltweit)
- 60 Tage keine E-Mails
- >270 Tage bis Normalbetrieb

- IT war schon immer schlecht
- Mit allen Kosten, die über Jahre eingespart wurden, hatte man externe Consultant gefüttert
- Keine wesentliche Verbesserung nach dem Hackangriff

Fall 2

tems security

Fall 2

5 von 12

- Großes Unternehmen
- Über 1000 Mitarbeiter
- Europa

- Teilweise das Backup zerstört
- Fileserver verschlüsselt
- E-Mail Server verschlüsselt
- Viele Business Applikationen verschlüsselt

- >10 Tage ohne IT
- >20 Tage keine E-Mails
- >60 Tage bis Normalbetrieb

- Gute und solide IT
- Eine IT-Hausaufgabe nicht vollständig ausgeführt.
- Hat aus dem Vorfall gelernt

Fall 3

tems security

Fall 3

4 von 12

- kleines Unternehmen
- 15 Mitarbeiter
- Österreich

- Backup war nicht betroffen
- Fileserver verschlüsselt
- Keine E-Mails verschlüsselt
- Keine Business Applikationen verschlüsselt

- >2 Tage ohne IT
- >2 Tage keine E-Mails
- 4 Tage bis Normalbetrieb

- Gute und solide IT
- Remote Desktop war nach außen offen.
- Hat aus dem Vorfall gelernt

Fall 4

tems security

Fall 4

4 von 12

- kleines Unternehmen
- 7 Mitarbeiter
- Österreich

- Alles auf einem Server
- Alle E-Mails verschlüsselt

- >10 Tage ohne IT
- >10 Tage keine E-Mails
- >20 Tage bis Normalbetrieb

- Server vermietet für Hackangriffe
- Anschließend einfach verschlüsselt
- Hat aus dem Vorfall gelernt

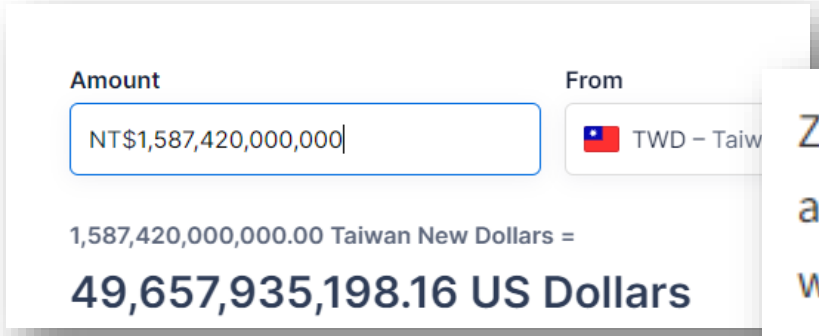
Fall 5

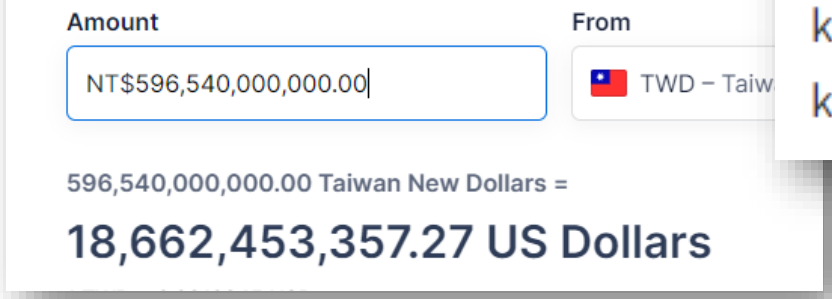
tems security

Fall 5 - Sommer 2023

65.000 Mitarbeiter

Die Lockbit-Cybergang ist eine der umtriebigsten kriminellen Vereinigungen. Ende Juni hat die Gruppierung etwa nach einem Einbruch bei einem TSMC-Zulieferer 70 Millionen US-Dollar Lösegeld vom Chipfertiger gefordert. Mitte März





Zu dem Zeitpunkt ging das Unternehmen davon aus, dass die Sicherheitssoftware auch den Abfluss von Daten verhindert hätte. Dem Unternehmen sei noch unklar, welche Informationen genau kopiert wurden, möglicherweise lediglich Daten von dem verwundbaren PC. Es bestehe jedoch das Risiko, dass Daten vom Server kopiert wurden. Das Unternehmen glaube, dass rund 10 Gigabyte an Daten kopiert wurden, was weniger als ein Prozent der gespeicherten Daten sei.

Zusammenfassung

tems security

Die Herausforderung für die Hacker

Sicheres Backup	Keine lokalen Administratoren	Umsetzung Tier-Level-Modell	Spezielle Admin-Workstation für Admins
Aktives Client-Patch Management	Kein Internetzugriff für Server	Systemhärtungen durchführen	Ausnahmslose MFA Umsetzung
Passwörteränderungen auch von Systemkonten	Windows Rechner PW Änderung alle 3 Tage	Erweitertes Logging in Windows aktivieren	Installation von smarten Honeybots

Nützliche Hilfe mit PDF-Dokumenten

- Bei unbedenklichen PDF-Dokumenten
  - https://www.virustotal.com
- Online PDF-Viewer
  - https://smallpdf.com/pdf-reader
- Online PDF-Analyse
  - https://pdfux.com/inspect-pdf/

Aber Vorsicht, sobald Sie ein PDF-Dokument hochgeladen haben, ist es im Internet veröffentlicht.

Vorsicht bei “vermeintlich” vertraulichen PDF-Dokumenten

tems security

Einfache IT-Security Spielregeln

- Der Hacker **benötigt nur eine Schwachstelle** oder Fehlkonfiguration, und der Hacker hat Zugriff auf ein Unternehmensnetzwerk.
- Ein Unternehmen kann den Hacker **nur durch Befehl oder falsche Anmeldung** innerhalb des Netzwerks durchführen, und wir sind in der Lage, den Hacker zu erkennen.

Fortbildung und Wissensaufbau sind Schlüsselfaktoren für den Erfolg.

tems security

Know your limit

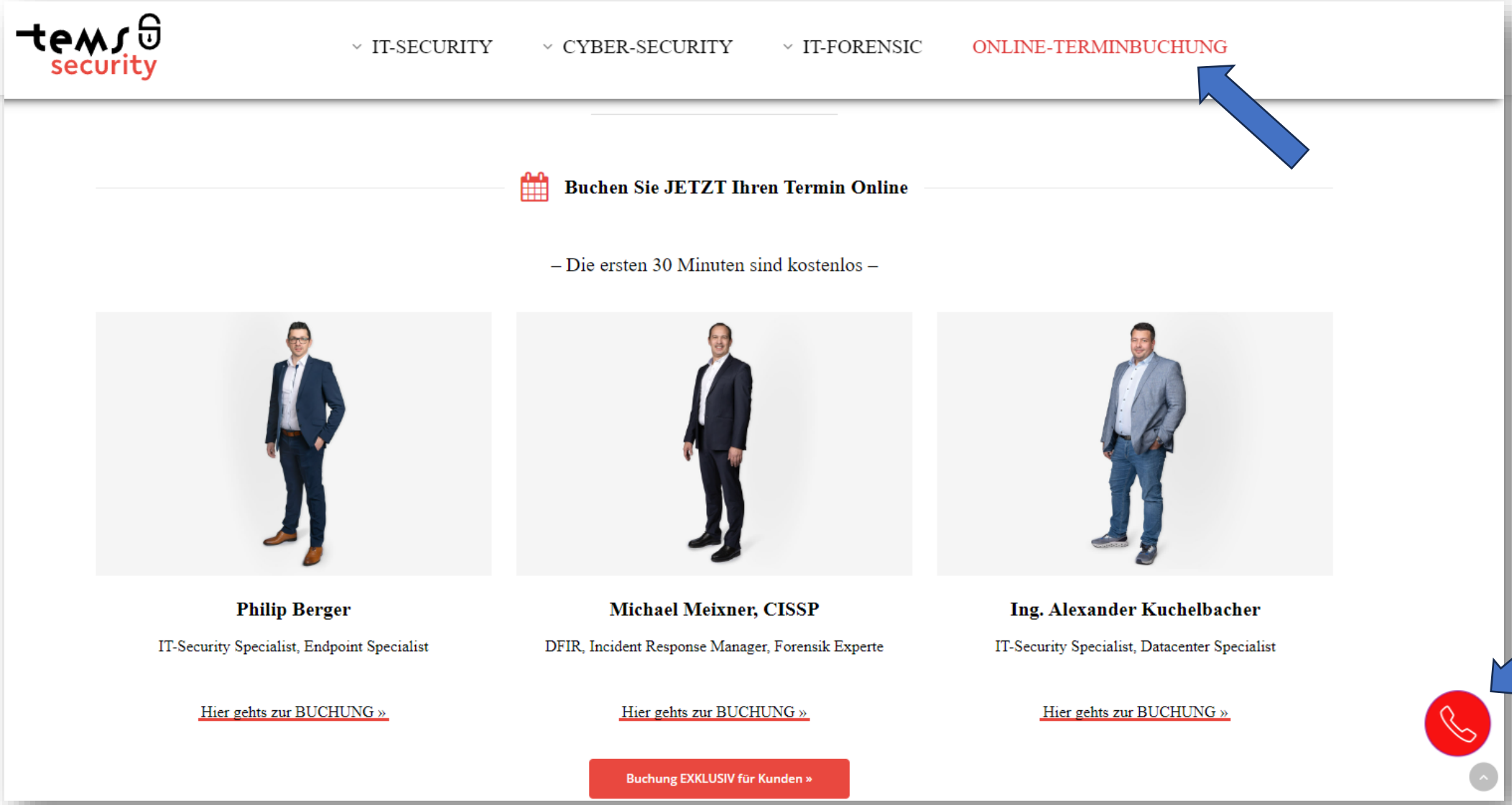
Work smarter
Not harder

Source: Internet

tems security

Ihr Weg zu einem Expertenteam

https://tems-security.at *https://tems.at*



Get in contact with us

Philip Berger
Managing Director
+43(664) 343 8644
Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director
+43(664) 1453328
Michael.meixner@tems-security.at