a.team rocks
CONSULTING & MANAGED DEFENSE

BlueShield

Cybersecurity heute und morgen: Sicherheitskonzepte für die nächste Generation von Cyber-Bedrohungen

AVI KRAVITZ

24.04.2024

Who am I?

Avi Kravitz | avi@a-team.rocks

Founder @ A-Team Rocks Consulting
Co-Founder @ Active Cyber Defense Center / ACDC
Co-Founder @ Founders of Europe

Advisory Board @ T3K Forensics
Advisory Board @ HTL-Spengergasse
Advisory Board & Partner @ Blue-Shield Security

Senior Security Consultant & Trainer

IT-Security seit 1999 (Offensive Security)

Spezialisierung seit 2011 auf Wirtschafts- und Industriespionage

Von 100 Unternehmen – wie viele kannst du hacken?

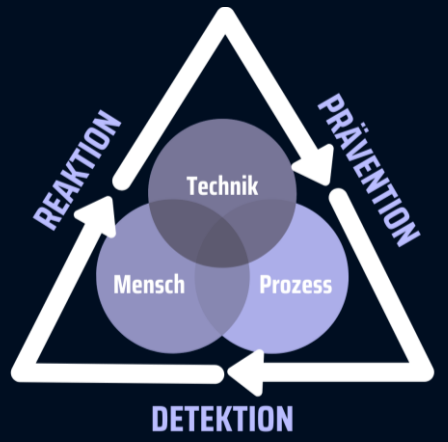
Mythen rund um Cyber-Security

- „Ich habe doch eine Firewall und ein Antivirenprogramm!“
- > 50% der erfolgreichen Angriffe verwenden neuartige Lücken

- „Wer will schon was von mir/uns?“
- > 90% aller Cyberangriffe sind opportunistisch

Mythen rund um Cyber-Security

- „Unsere IT kümmert sich darum.“
- Cyber-Security funktioniert nur ganzheitlich



- „Wir haben eh eine Cyber-Versicherung abgeschlossen“
- Reputation, Betriebsunterbrechung, Sorgfaltspflicht, vertragliche Ausschlussgründe, Strafen,…

Größten (sichtbaren) Bedrohungen 2024

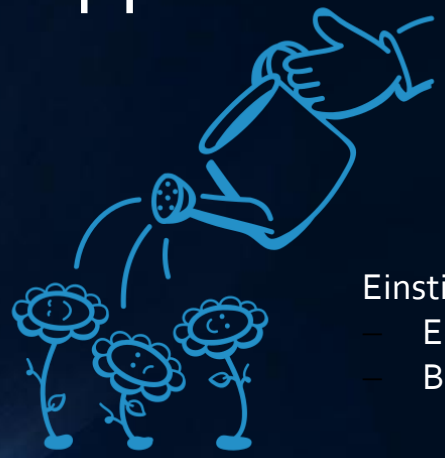
1. Identitätsdiebstahl
2. Erpressung (1.1 Mrd. USD in 2023)
3. Angriffe über die Lieferkette (seit 2021: +650%)

Cyber-Angriffe – die Akteure

opportunistisch VS zielgerichtet

Cyber-Angriffe – die Akteure

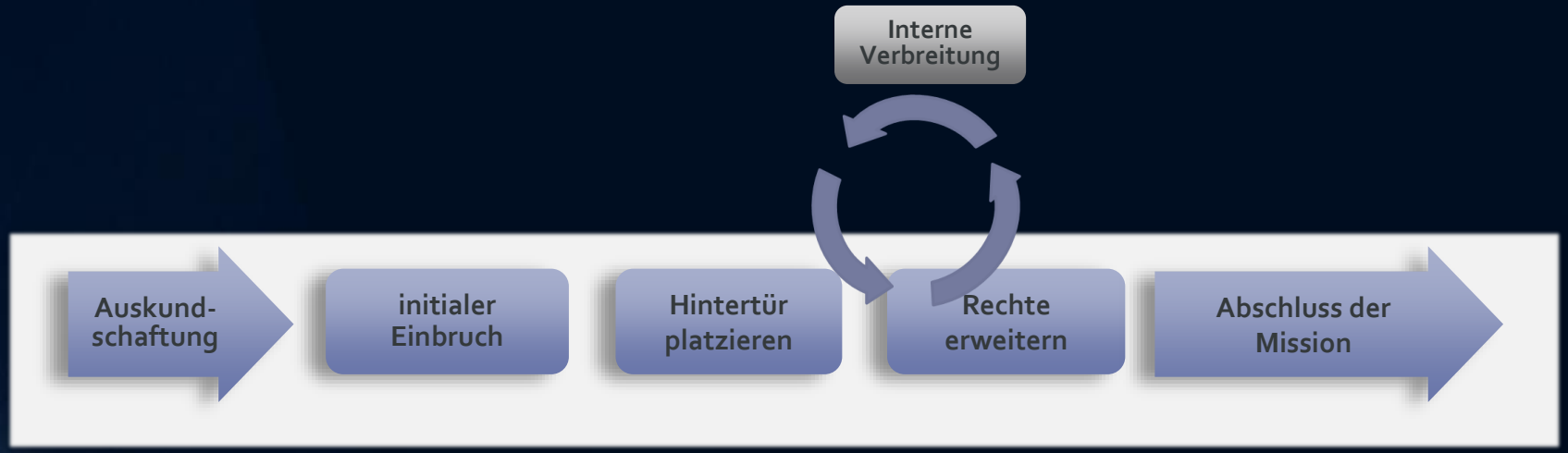
opportunistisch VS zielgerichtet



Einstieg meist:

- E-Mail (z.B. Phishing, Attachments,…)
- Browser (z.B. Malvertising)

Die Anatomie eines fortgeschrittenen Angriffes



Quelle: Lockheed Martin & Mandiant

Die (häufigsten) Eintrittsvektoren:

- E-Mail / Phishing (+76% zu 2021)
- Nicht aktuell gehaltene & exponierte Systeme/Software
- Unzureichend gesicherte Fernzugänge
- **Most Trending**: Angriffe über die Lieferketten
- **Hottest newcomer**: Malvertising

Malvertising

Kofferwort aus Malware und Advertising:

- Malvertising nutzt Online-Werbung, um Malware einzuschleusen

Warum gefährlich?

- Hochwirksam - Nutzer müssen nichts aktiv machen
- Weite Verbreitung - kann auf jeder Webseite erscheinen
- Schwierig zu erkennen -
  Malware kann wie reguläre Werbung aussehen –
  Webseitenbetreiber haben wenig bis keinen Einfluss darauf!

2710 requests to 129 third-party hosts during a single visit to spiegel.de

Testing by Wolfie Christl, 11.10.2022, Firefox, no tracking protection, Vienna

smartadserver.com	602
casalemedia.com	156
openx.net	142
doubleclick.net	134
pubmatic.com	83
emsservice.de	79
amazon-adsystem.com	75
yahoo.com	69
bidswitch.net	66
adnxs.com	61
bidr.io	55
simpli.fi	53
adform.net	52
turn.com	52
quantserve.com	49
adsrvr.org	45
criteo.com	39
mathtag.com	35
rfihub.com	35
adition.com	34
contextweb.com	33
1rx.io	32
rlcdn.com	31
omnitagjs.com	30
sharethrough.com	30
unrulymedia.com	30
yieldlab.net	28
blismedia.com	23
mrpdata.net	22
dyntrk.com	22
lijit.com	22
demdex.net	20
opecloud.com	17

rubiconproject.com	17
adobedtm.com	16
tribalfusion.com	16
doubleverify.com	16
ad4m.at	15
adroll.com	14
emxdgt.com	13
googletagservices.com	13
loopme.me	12
xplosion.de	11
zemanta.com	11
onaudience.com	11
ipredictive.com	11
teads.tv	11
taboola.com	10
conative.network	10
omny.fm	8
viralize.tv	8
everesttech.net	8
justpremium.com	7
adrtx.net	7
dotomi.com	7
facebook.com	7
sparwelt.click	7
adalliance.io	6
nmrodam.com	6
sitescout.com	6
w55c.net	6
googlesyndication.com	6
stackadapt.com	6
creative-serving.com	6
google.com	5
stickyadstv.com	5

erne.co	5
admedo.com	5
crwdcntrl.net	5
aaroaj.com	4
blubroid.de	4
ioam.de	4
acuityplatform.com	4
criteo.net	3
bing.com	3
mxcdn.net	3
facebook.net	3
outbrain.com	3
mookie1.com	3
emetriq.de	3
google.at	3
sascdn.com	3
gammaplatform.com	3
betweendigital.com	3
2mdn.net	3
zeotap.com	3
eyeota.net	3
indexww.com	2
technical-service.net	2
akamaihd.net	2
cwi.re	2
nativendo.de	2
dnacdn.net	2
sportradarserving.com	2
richaudience.com	2
avct.cloud	2
fwmrm.net	2
de17a.com	2
nrich.ai	2

exelator.com	2
scoota.co	2
avads.net	2
admixer.net	2
theadex.com	2
fiftyt.com	2
audrte.com	2
gstatic.com	2
weborama.fr	2
adobetarget.com	1
googletagmanager.com	1
gumgum.com	1
ads-twitter.com	1
t.co	1
digitaleast.mobi	1
vtracy.de	1
twitter.com	1
resetdigital.co	1
clickagy.com	1
ctnsnet.com	1
linkedin.com	1
mfadsrvr.com	1
serving-sys.com	1
semasio.net	1
exactag.com	1
admob.com	1
conative.de	1
cloudflare.com	1
googleapis.com	1
adscale.de	1

Beliebte Webseiten in DE

1. **google.com**
Internet-Suchmaschine

2. **youtube.com**
Video-Portal

3. **google.de**
Internet-Suchmaschine

4. **facebook.com**
Soziales Netzwerk

5. **amazon.de**
Amerikanischer Onlineversandhändler

6. **ebay.de**
Online-Auktionen

7. **wikipedia.org**
Online-Enzyklopädie

8. **ebay-kleinanzeigen.de**
Kostenlose Kleinanzeigen bei eBay

9. **web.de**
E-Mail-Anbieter

10. ***
"Erwachsenen-Webseite"

- Quelle: https://www.die-besten-aller-zeiten.de/internet/beliebteste-webseiten-in-deutschland.html

Beispiel “Erwachsenen-Webseite” (20.7.2023)

www.google-analytics.com: 2
fs.ypncdn.com: 17
fi1.ypncdn.com: 2
ss.phncdn.com: 3
stats.g.doubleclick.net: 2
di1.ypncdn.com: 2
di.phncdn.com: 5
di2.ypncdn.com: 1
fi1-ph.ypncdn.com: 17
fi2.ypncdn.com: 1
fi2-ph.ypncdn.com: 1
bi.phncdn.com: 1
ads2.contentabc.com: 1
cdn.engine.phn.doublepimp.com: 1 (BLOCKED)
cdn1-smallimg.phncdn.com: 2
etahub.com: 1
hw-cdn.contentabc.com: 1
hw-cdn.trafficjunky.net: 1
media.trafficjunky.net: 2
s1.static.cfgr1.com: 1
syndication.exoclick.com: 1
vz-cdn.contentabc.com: 1
vz-cdn.trafficjunky.net: 1
www.afgr1.com: 1
85otw.voluumtrk3.com: 1
ads.exoclick.com: 1
engine.phn.doublepimp.com: 1
static.exoclick.com: 1
www.you-porn.com: 2
www.googletagmanager.com: 1
static.trafficjunky.com: 4
www.rtalabel.org: 1
www.pornhub.com: 2
www.redtube.com: 2
www.tube8.com: 2
www.pornmd.com: 2
www.thumbzilla.com: 1
www.youporngay.com: 1
youpornshop.com: 1
www.youpornpremium.com: 7
guppy.link: 2
black77854.com: 1
ei.phncdn.com: 7
help.getadblock.com: 1
twitter.com: 1
www.instagram.com: 1

Insgesamt 46 externe Domains nachgeladen, davon 1 geblockt. Gesamtanzahl der Requests: 111

Beispiel “Erwachsenen-Webseite” (20.7.2023)

VirusTotal Hashes

Search Term: cdn.engine.phn.doublepimp.com

source of data: VirusTotal

TStamp	Detection	SHA256 Hash
2023-07-20 04:53:23	56 of 75	91bc6d221c1a488090c2ecda2529eb5e39fd7171a31602691eaa4062514d01fe
2023-06-29 23:18:44	52 of 75	3c882772d962fa7afe893aab3a477364cadd265e45040c029e23096b250fe85a
2023-05-27 09:59:33	50 of 75	502663d0738d1c42bfd07c0464d9432c3a47bf415753e68f0c86333fbcae7a5b

VT-Datenbank:

(Payload die mit dieser Domäne interagieren)

https://www.virustotal.com/gui/file/91bc6d221c1a488090c2ecda2529eb5e39fd7171a31602691eaa4062514d01fe/detection

https://www.virustotal.com/gui/file/3c882772d962fa7afe893aab3a477364cadd265e45040c029e23096b250fe85a/detection

https://www.virustotal.com/gui/file/502663d0738d1c42bfd07c0464d9432c3a47bf415753e68f0c86333fbcae7a5b/detection

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Scar.C93649
ALYac	Trojan.GenericKD.38921851	Antiy-AVL	Trojan/Win32.Scar
Arcabit	Trojan.Generic.D251E67B	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Dropper.Gen
BitDefender	Trojan.GenericKD.38921851	BitDefenderTheta	AI:Packer.A7BFA33F1E

malvertising

Alle | Bilder | News | Videos | Bücher | Mehr | Suchfilter

Ungefähr 259 Ergebnisse (0,28 Sekunden)

Trojaner-Info

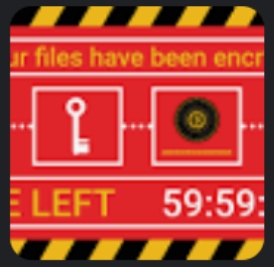
Aktuelle Trends beim betrügerischen Social Engineering: HTML-Phishing und Malvertising

Um Cyber-Crime-Angriffe zu platzieren, sind E-Mail-Anhänge weiterhin bei Betrügern sehr beliebt. Doch Office-Dokumente scheinen als...

vor 2 Tagen

Heise

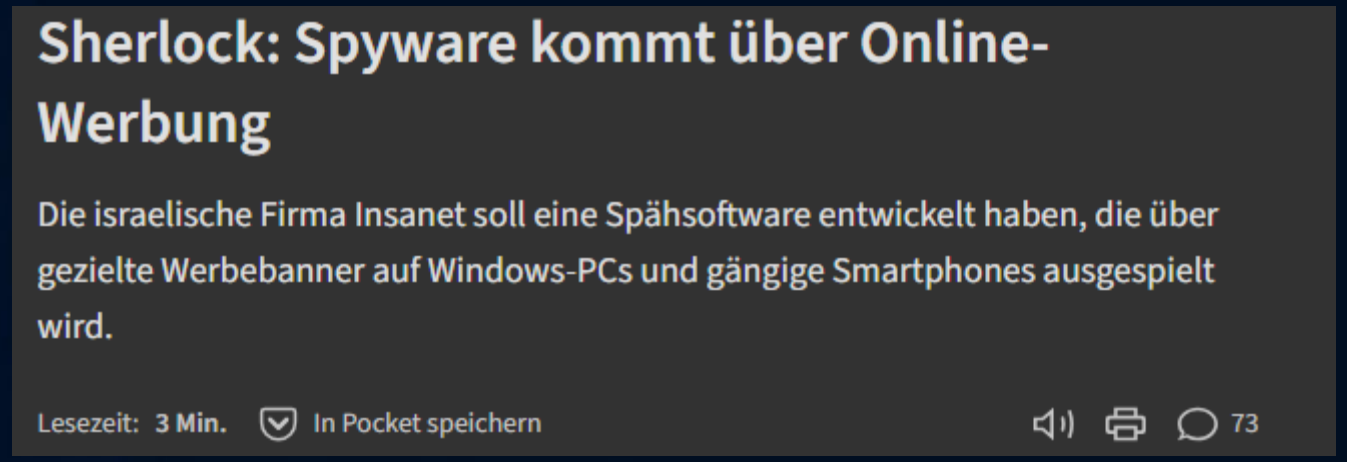
Malvertising: BlackCat-Ransomware versteckt sich hinter Fake-WinSCP-Tool



Die Hintermänner des Verschlüsselungstrojaners BlackCat (aka ALPHV) setzen auf einen weiteren Verbreitungsweg.

vor 2 Wochen

Malvertising – ganz aktuell



Sherlock: Spyware kommt über Online-Werbung

Die israelische Firma Insanet soll eine Spähsoftware entwickelt haben, die über gezielte Werbebanner auf Windows-PCs und gängige Smartphones ausgespielt wird.

Lesezeit: 3 Min. In Pocket speichern 73

Quelle: Heise, 18.09.2023

„Wir analysieren 1.4 Mio. neue Domänen am Tag.

+70% sind gefährlich“

BlueShield

Wir haben initialen Zugang, was nun?

Initial Access Broker

- „Makler für den Erstzugang“

Quelle: Blueliv

Circassian March 24, 2023 01:32 PM

Hi,

RDP USA access
Revenue: $64.3M Zoominfo
Industry: Construction Zoominfo
139 employees. Zoominfo
rights: domain admins
Type access: RDP

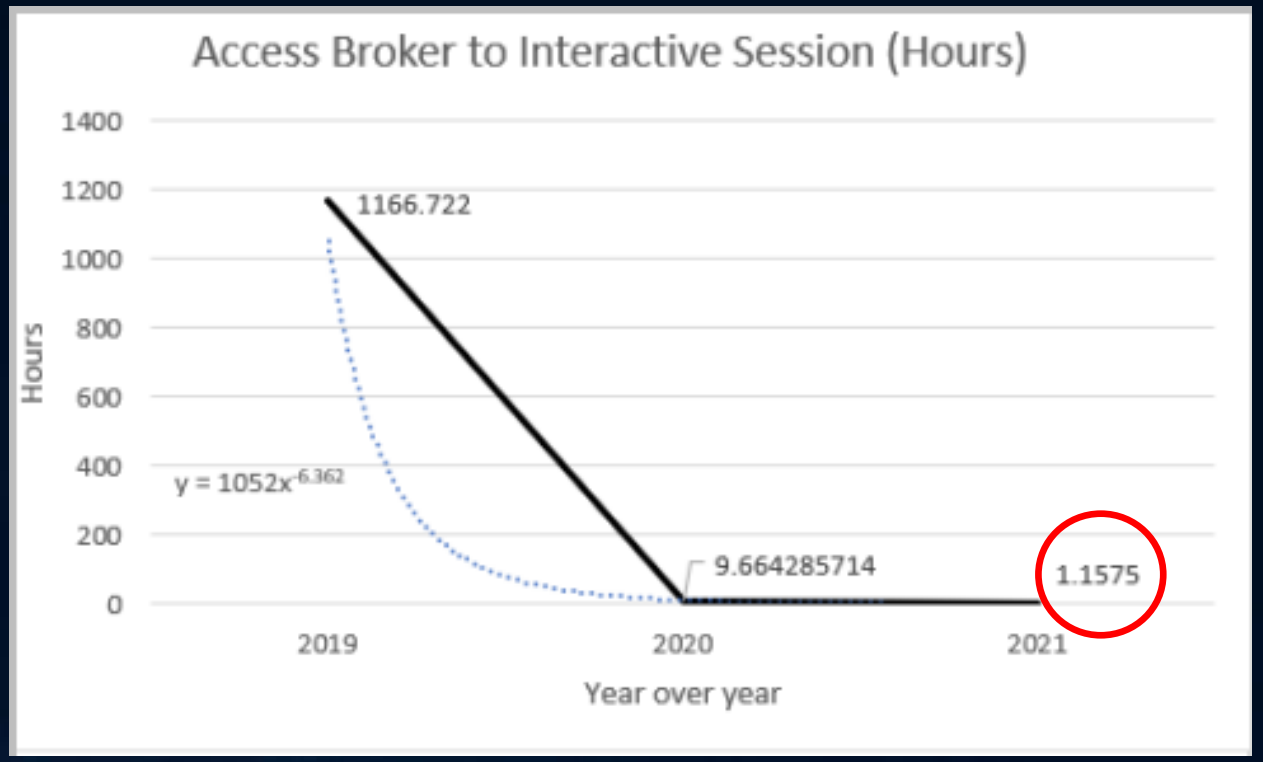
5 Hyper V| AV:Windows Defender | 130 computer Active Directory | 487 User Active Directory

Price : 3000 Usd

I agree to the guarantor.

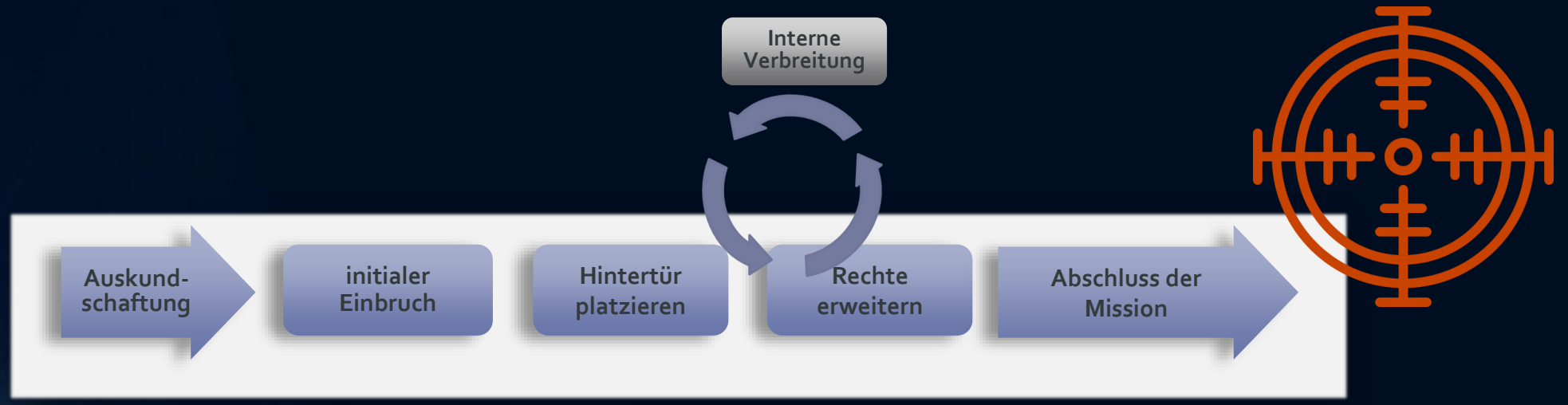
Initiale Infektion – Patient 0

- Dauer bis zum ersten „bösen“ Login:



Quelle: IBM X-Force

Die Anatomie eines fortgeschrittenen Angriffes



Quelle: Lockheed Martin & Mandiant

Angriffe über die Lieferketten

CHRONIK

Hackerangriff auf 34 Firmen

Hackern ist in Oberösterreich ein großangelegter Angriff auf Firmen gelungen. Über eine IT-Firma wurden die Computersysteme von 34 Unternehmen mit einer Schadsoftware infiziert und verschlüsselt. Den Firmen wurden hohe Lösegeldforderungen gestellt.

2. September 2021, 6.11 Uhr

Angriffe über die Lieferketten – Solarwinds Hack 2021

- 18.000 der größten Unternehmen weltweit betroffen
- Unter anderem:
  - Microsoft, CISCO, Intel,…
- Attributierung führt zu Russland

Hintergrund
15.01.2021
Lesedauer ca. 7 Minuten
Drucken
Teilen

SOLARWINDS-HACK

Ein Hackerangriff, der um die Welt geht

Der Angriff auf das Unternehmen SolarWinds gilt als größter Hack seit Jahren. Zehntausende Firmen könnten betroffen sein. Um was geht es, wie gefährlich ist es und wie kann man sich schützen? Antworten auf die wichtigsten Fragen.

von Eike Kühl

Quelle: Spektrum, 15.01.201

Hackerangriffe auf die Ukraine

Die erste Angriffswelle

Die Invasion begann, bevor Raketen einschlugen – mit russischen Hackerattacken. Deren Aktionen beschränken sich nicht auf die Ukraine. Sie können auch den Westen treffen.

Von **Kai Biermann** und **Karsten Polke-Majewski**

24. Februar 2022, 14:45 Uhr / 234 Kommentare /

Quelle: zeit.de, 24.02.2022

Wer ist der größte Lieferant?

Angriffe über die Lieferketten - Microsoft Hack 2023

- *„Bis heute weigert sich der Konzern, die genauen Hintergründe und die sich daraus ergebenden Konsequenzen offenzulegen.“*

Quelle: Heise, 4.8.2023

… und es ging weiter

US-Softwarekonzern

Russische Gruppe hackt Microsoft

Der US-Softwarekonzern Microsoft ist Opfer einer Cyberattacke geworden. Dem Unternehmen zufolge konnten Hacker mit Verbindungen zur russischen Regierung unter anderem Mails ranghoher Mitarbeiter lesen.

21.01.2024, 12.15 Uhr

Quelle: Spiegel.de,12.3.2024

…bis jetzt

Windows-Konzern

Russische Hacker haben sich bei Microsoft Zugriff auf Mails und Quellcodes verschafft

Der Windows-Konzern hat schon vor Wochen kriminelle Zugriffe auf seine Systeme festgestellt – und wird die offenbar russischen Angreifer nicht los. Das hat Folgen.

08.03.2024 - 20:11 Uhr

Quelle: Handelsblatt, 12.3.2024

Ransomware - Verschlüsselungstrojaner

- Ziel: (meist) Lösegeld Erpressung
- Schaden ?
- Alle 11 Sekunden erfolgt ein Ransomware-Angriff

- Durchschnittliche Wiederherstellungszeit: **21 Tage!**

Jedes 6. österreichische Unternehmen war 2022 von Ransomware betroffen
(Quelle: Cyber Security in Österreich 2022 – KPMG/BMI Austria)

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher“ zu sein

“There are only two types of companies: Those that have been hacked and those that will be hacked.”

– Robert S. Mueller, III, former Director of the FBI

Details zum Sicherheitsvorfall

Ausfall | Einbruch

Betr. (Organisation)	CHU Saint-Pierre
Datum (Veröffent.)	13.03.2023
Land	Belgien
Vorfall	Am 11. März 2023 kam es zu einem Cyberangriff auf das Saint-Pierre Universitätskrankenhaus in Brüssel. Der Angriff wurde entdeckt, nachdem IT-Experten eine Verlangsamung interner Server feststellten. Aufgrund der Attacke wurden interne Server und die Notaufnahme für mehrere Stunden heruntergefahren und eintreffende Patienten wurden an andere Krankenhäuser umgeleitet.
Quellen	11.03.2023: Brussels Times 12.03.2023: noticemerica 12.03.2023: BRF

Stephane Odent · 3rd+ + Follow
CIO at CHU Saint-Pierre
23h ·

Opportunity knocks.... Bravo Sophos! In any case, their antivirus did not protect us and seriously weighed us down...

That said, we must indeed take cybersecurity very seriously and protect ourselves against a growing and increasingly aggressive and effective threat.

See translation

Karim Boudekhan 3rd+ + Follow
Enterprise Account Manager
BELUX SOPHOS
5d ·

Do not wait before it's too late!
Another hospital that is the target of cyberattacks.

The CHU Saint-Pierre in Brussels has closed its emergency service due to a cyberattack 🔥🔥🔥.

With our solutions and services from Sophos, this attack would have been neutralized by our dedicated team of experts.

Was haben wir daraus gelernt?

- Ziel Prävention => draußen halten und/oder Zeit gewinnen
- Es gibt kein Schlangenöl um „sicher“ zu sein
- Hausaufgaben erledigen!

“There are only two types of companies: Those that have been hacked and those that will be hacked.”

– Robert S. Mueller, III, former Director of the FBI

Wohin geht die Reise?

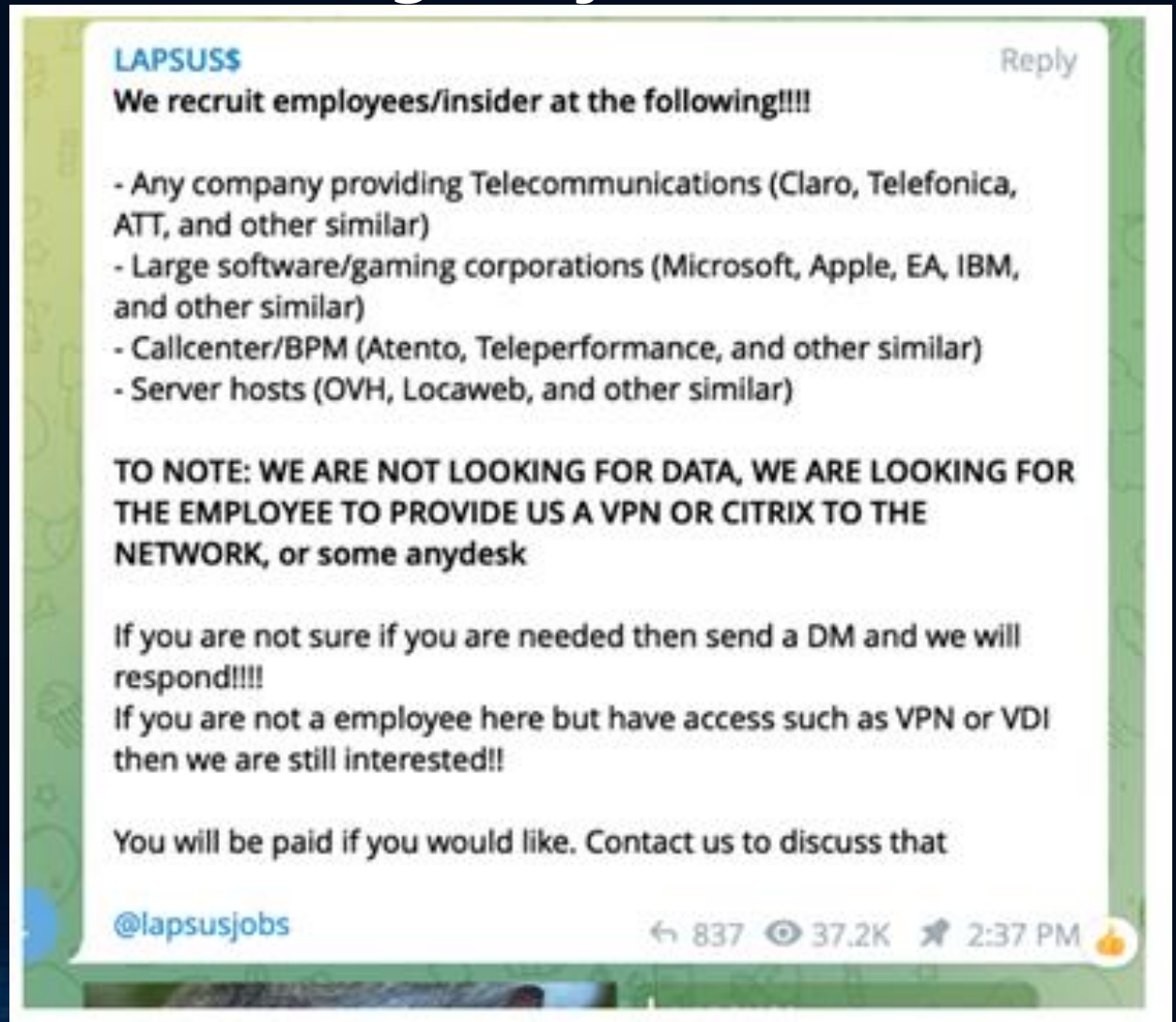
- Cyber-Crime gekommen um zu bleiben!
- Angriffe werden immer schneller
- …und dank KI auch immer besser

- Messlatte für Cyber-Versicherungen steigt

*"Cybersecurity Ventures also reports that cybercrime represents the **greatest transfer of economic wealth in history**. 15% growth every year." (Intrusion, 2021)*

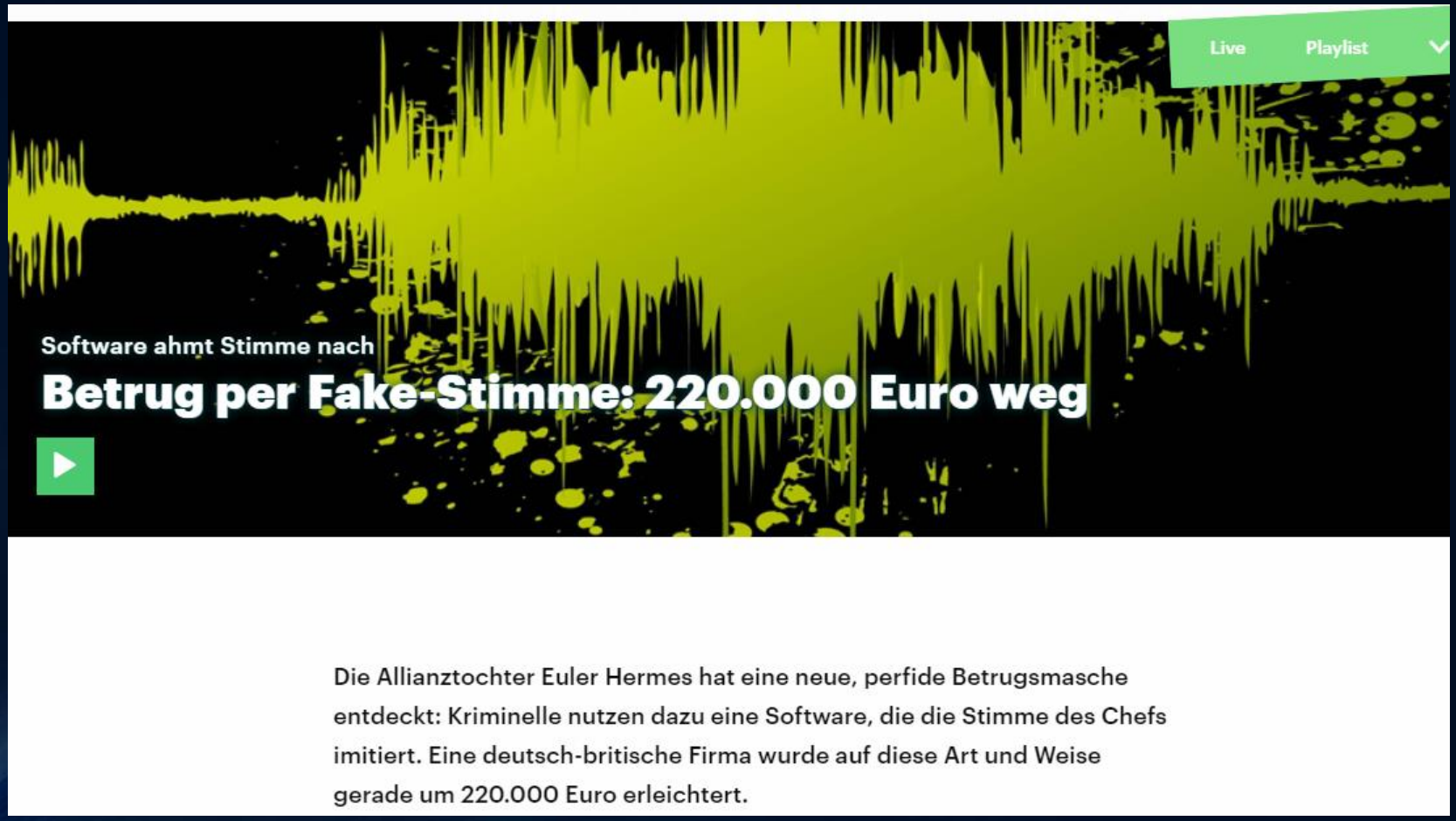
Ransomware - Verschlüsselungstrojaner

- Insider?



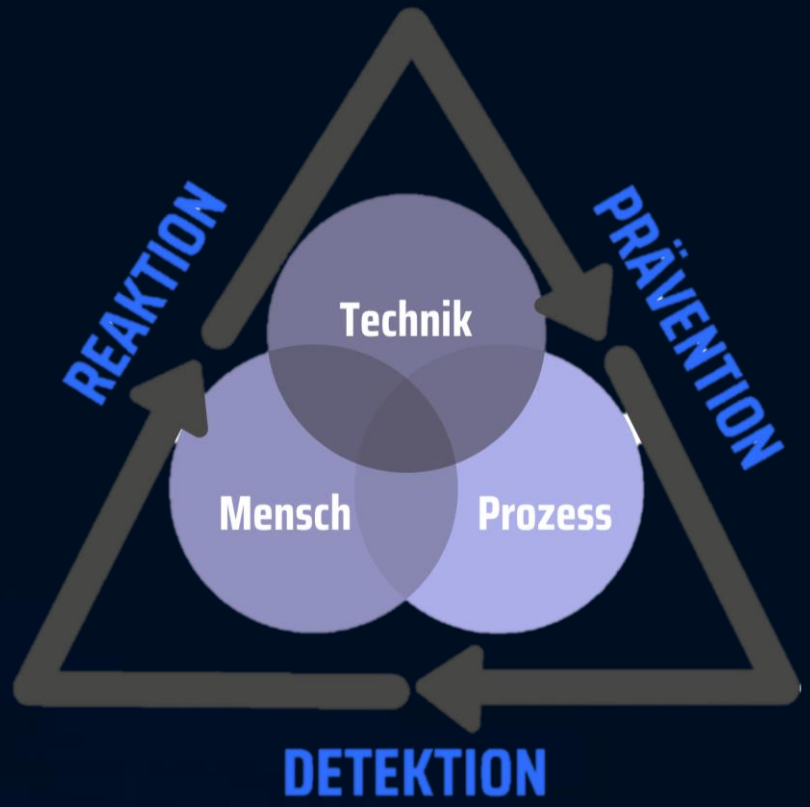
Wohin geht die Reise?

Wohin geht die Reise?



State-of-the-Art Cyber-Security 2024ff

- Cyber-Security ist ein Prozess & kein Projekt
- Multi Vendor Strategie
- Monitoring & schnelle Reaktion ist und wird kriegsentscheidend
- Jede Security-Lösung braucht aktives Monitoring (Threat Hunting)

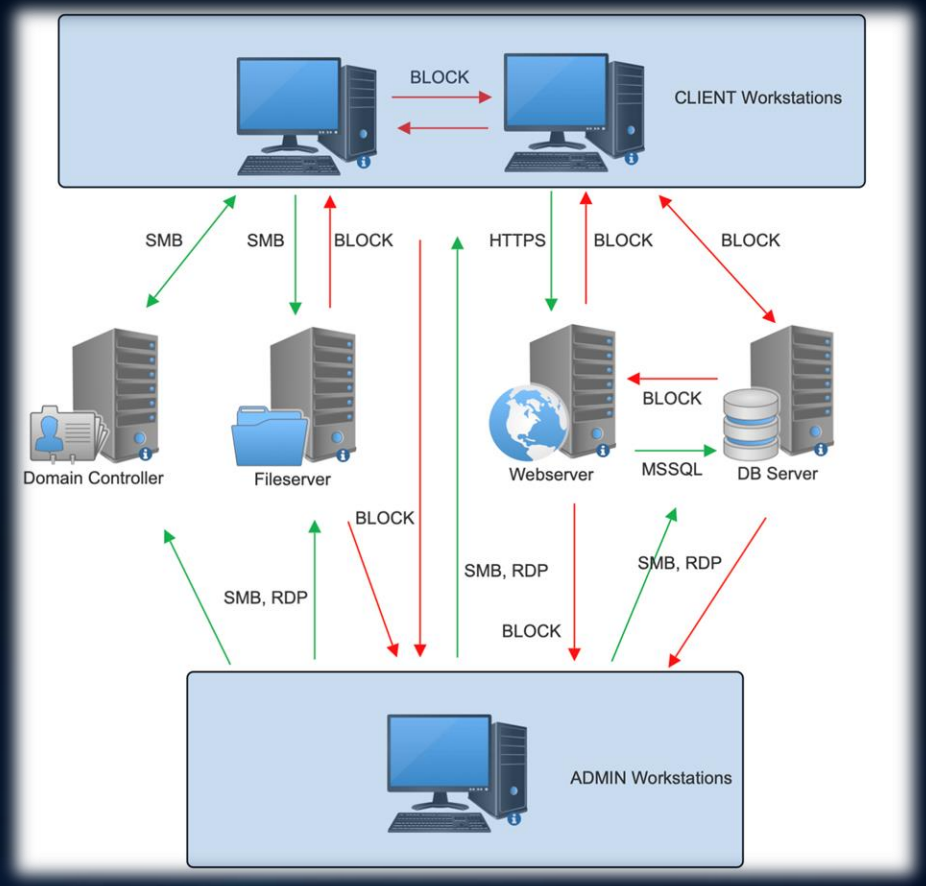


Jedes Unternehmen ist einzigartig!

Cyber-Hygiene - Baseline

- Passwortmanagement & MFA
- Sicherheitsupdates zeitnah (!) einspielen
- Netzwerksegmentierung (zumindest Client zu Client und Client zu Admin unterbinde
- Least Privilege – Zugriffsberichtigungen reviewen, jeder sollte nur auf das Zugriff haben, was er/sie für die Arbeit auch benötigen
- Backups: nicht in die Domäne hängen und möglichst isolieren!
- Awareness Trainings & Kultur etablieren, damit potentielle Sicherheitsvorfälle rasch gemeldet werden

Netzwerksegmentierung



Von 100 Unternehmen – wie viele kannst du hacken?

Vielen Dank!

a-team rocks
CONSULTING & MANAGED DEFENSE

BlueShield

avi@a-team.rocks