AWARE7
full service awareness agency

Live Hacking

Kunden im Dialog

Unser Team – unsere Kompetenz

AWARE7
full service awareness agency

Kreativer & professioneller Dienstleister in der IT-Security Branche

Penetrationstests & Sicherheitsuntersuchungen

- Mehr als 200 PT p.a.
- Internationale Kundschaft
- Hohe Expertise

Live Hacking & Cyber Security Shows

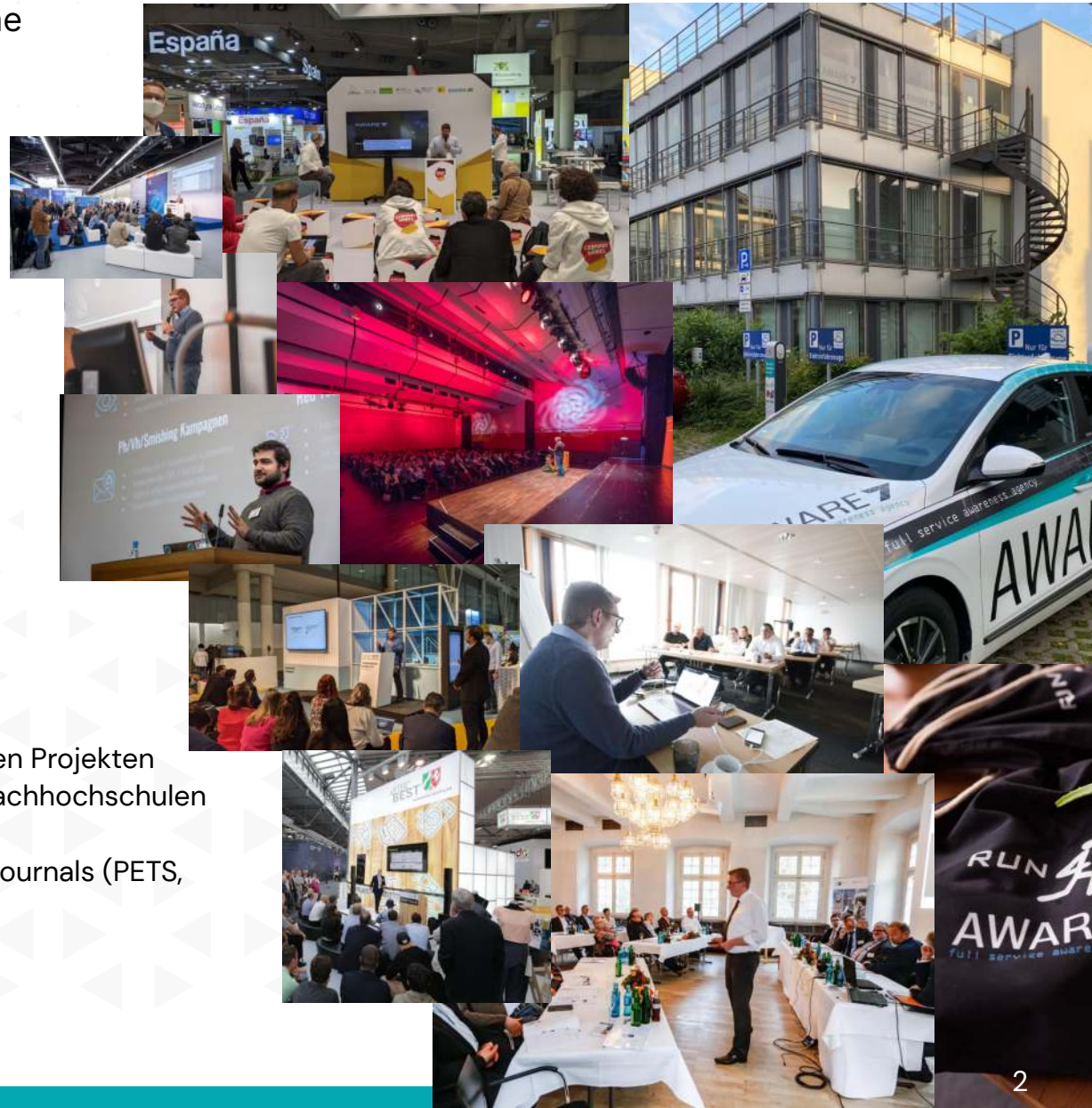
- Projektübergreifender Austausch
- von 30 bis 180 Minuten
- Im Duett und zweisprachig

IT-Sicherheitskonzeption ISO 27001

- Vom Beginn bis zur Zertifizierung
- Partner für internes und zert. Audit
- Bereitstellung von ext. ISBs

Individuelle IT-Security Projekte

- Aus- und Durchführung von individuellen Projekten
- Enge Zusammenarbeit mit Instituten, Fachhochschulen und Universitäten
- Publikationen in Top Konferenzen und Journals (PETS, WWW)



Wer bin ich?

M.Sc. Chris Wojzechowski

Geschäftsführender Gesellschafter der AWARE7 GmbH

- **Bachelor of Science**
  Westfälische Hochschule Bocholt
  Wirtschaftsinformatik

- **Master of Science**
  Westfälische Hochschule Gelsenkirchen
  Internet-Sicherheit

- **IT-Grundschutz Praktiker (TÜV)**
  Auf- und Ausbau von ISMS Systemen nach
  ISO 27001 auf Basis des IT-Grundschutzes

- **IT-Risk Manager (DGI)**
  IT-Risikoanalyse und Bewertung nach ISO 31000

Veröffentlichungen:
Kompass IT-Verschlüsselung
Studie für das Bundesministerium für Wirtschaft und Energie (BMWi)

Meine digitale Sicherheit - Tipps und Tricks für Dummies
Wiley Verlag, 06.10.2021

Wer bin ich?

Dr.-Ing. Matteo Große-Kampmann

Geschäftsführender Gesellschafter der AWARE7 GmbH

- **Bachelor of Science**
  Hochschule Koblenz - Medizintechnik
- **Master of Science**
  Westfälische Hochschule Gelsenkirchen - Internet-Sicherheit
- **Promotion zum Dr.-Ing**
  Ruhr-Universität-Bochum
- **Dozent**
  Digital Business University of Applied Sciences

Aktuelle Veröffentlichungen:
"We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications
Privacy Enhancing Technologies Symposium 2022.3, Sydney, Australia.

Reproducibility and Replicability of Web Measurement Studies
ACM Web Conference 2022, Lyon, France.

Sonstige Tätigkeiten
Mentorenbeirat an der Technischen Hochschule Georg Agricola
Juror und Coach bei versch. Gründungswettbewerben

Daily Struggle

Wie gehen Kriminelle vor?

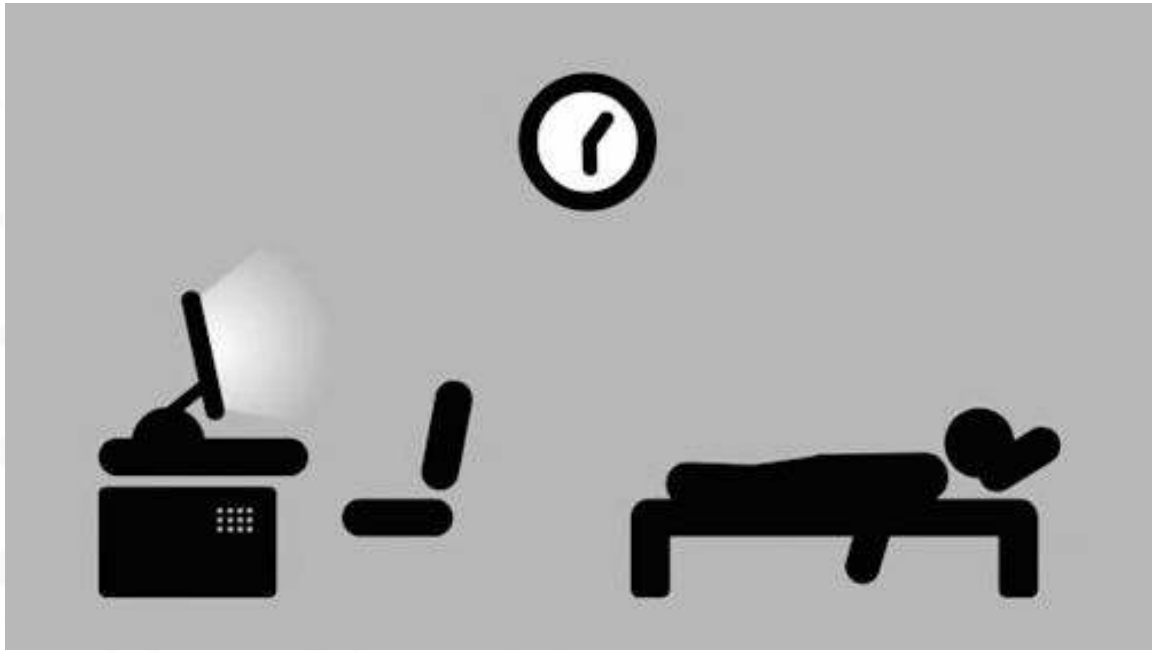
Wir schauen uns die Betrugsmaschen der Kriminellen an, vollziehen sie nach, bauen sie nach um anschließend zu sensibilisieren.

Welche Sicherheitslücken gibt es?

Wir schauen uns Medienphänome an, analysieren diese, schätzen sie ein und arbeiten bei verfügbaren Kapazitäten mit an der Lösung.

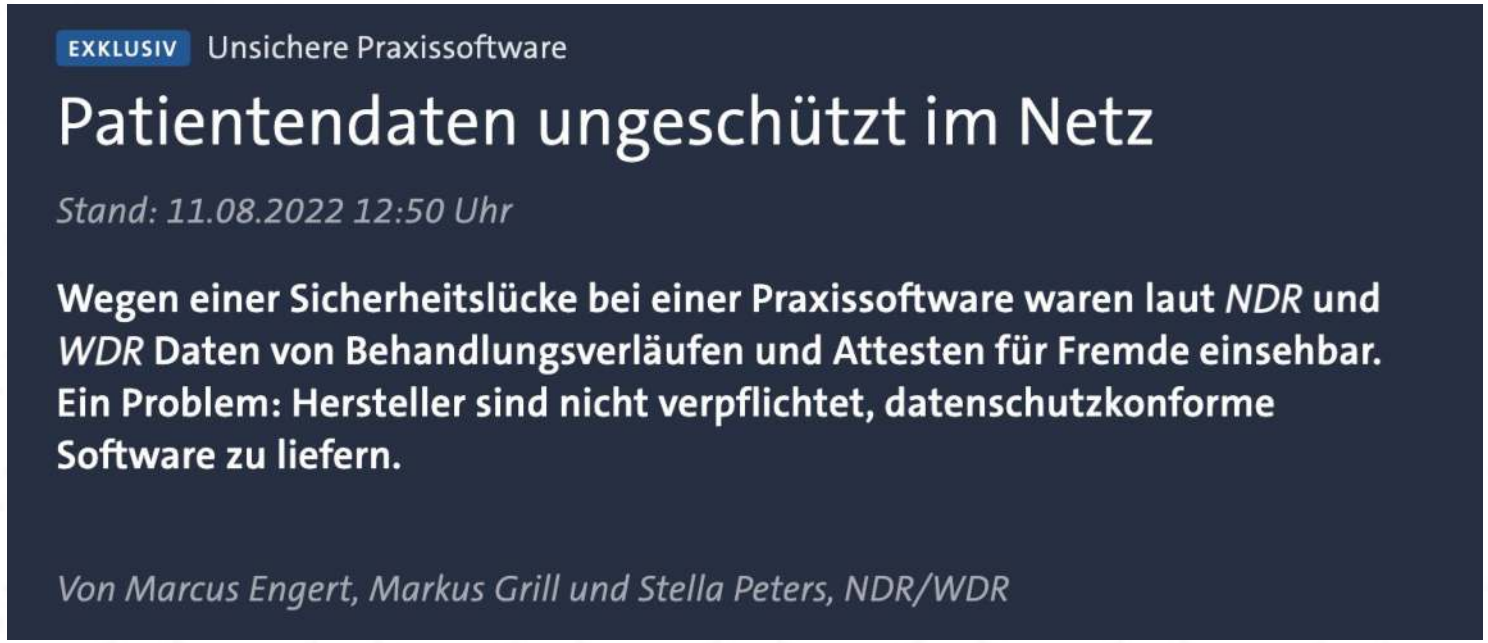
Was ist das tagesaktuelle IT-Geschehen?

Wir sind stets auf dem neuesten Stand der IT-Sicherheit - im Privat, Geschäfts- & Forschungsbereich. Zum Nutzen aller.



Aktuelle Vorfälle

Die zum Nachdenken anregen.
Teilweise hunderte Firmen die gleichzeitig oder zeitnah betroffen sind – Lösegeldforderungen in unbekannten Kryptowährungen oder lediglich über der Verfügbarkeit?



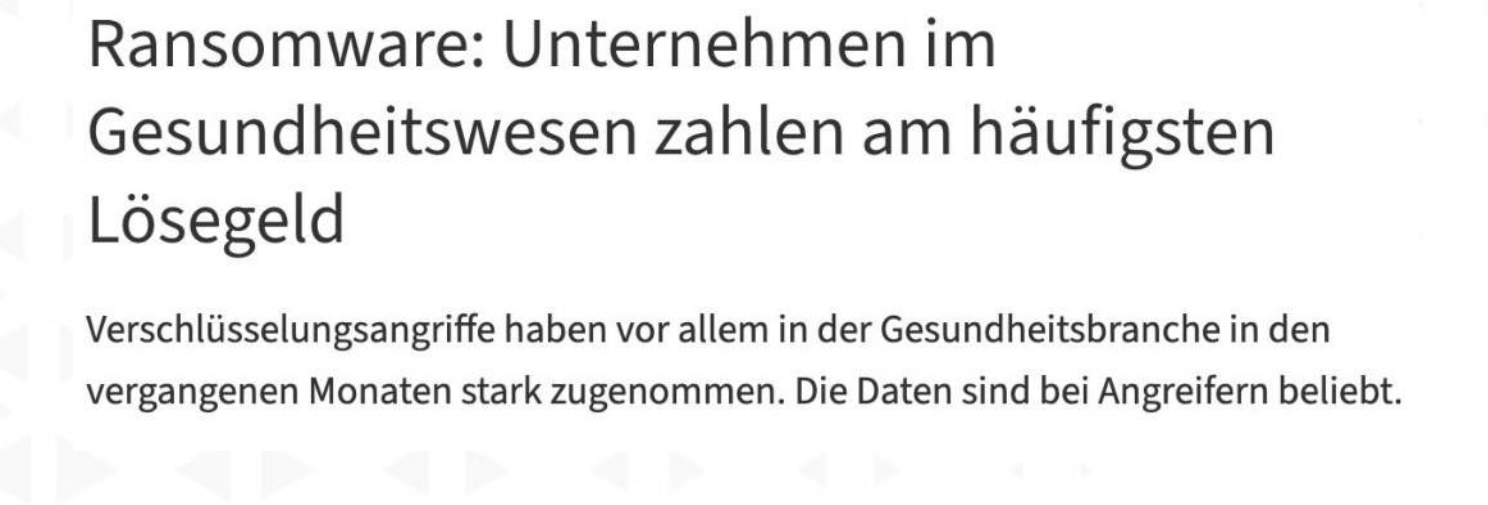
EXKLUSIV Unsichere Praxissoftware

Patientendaten ungeschützt im Netz

Stand: 11.08.2022 12:50 Uhr

Wegen einer Sicherheitslücke bei einer Praxissoftware waren laut *NDR* und *WDR* Daten von Behandlungsverläufen und Attesten für Fremde einsehbar. Ein Problem: Hersteller sind nicht verpflichtet, datenschutzkonforme Software zu liefern.

Von Marcus Engert, Markus Grill und Stella Peters, NDR/WDR



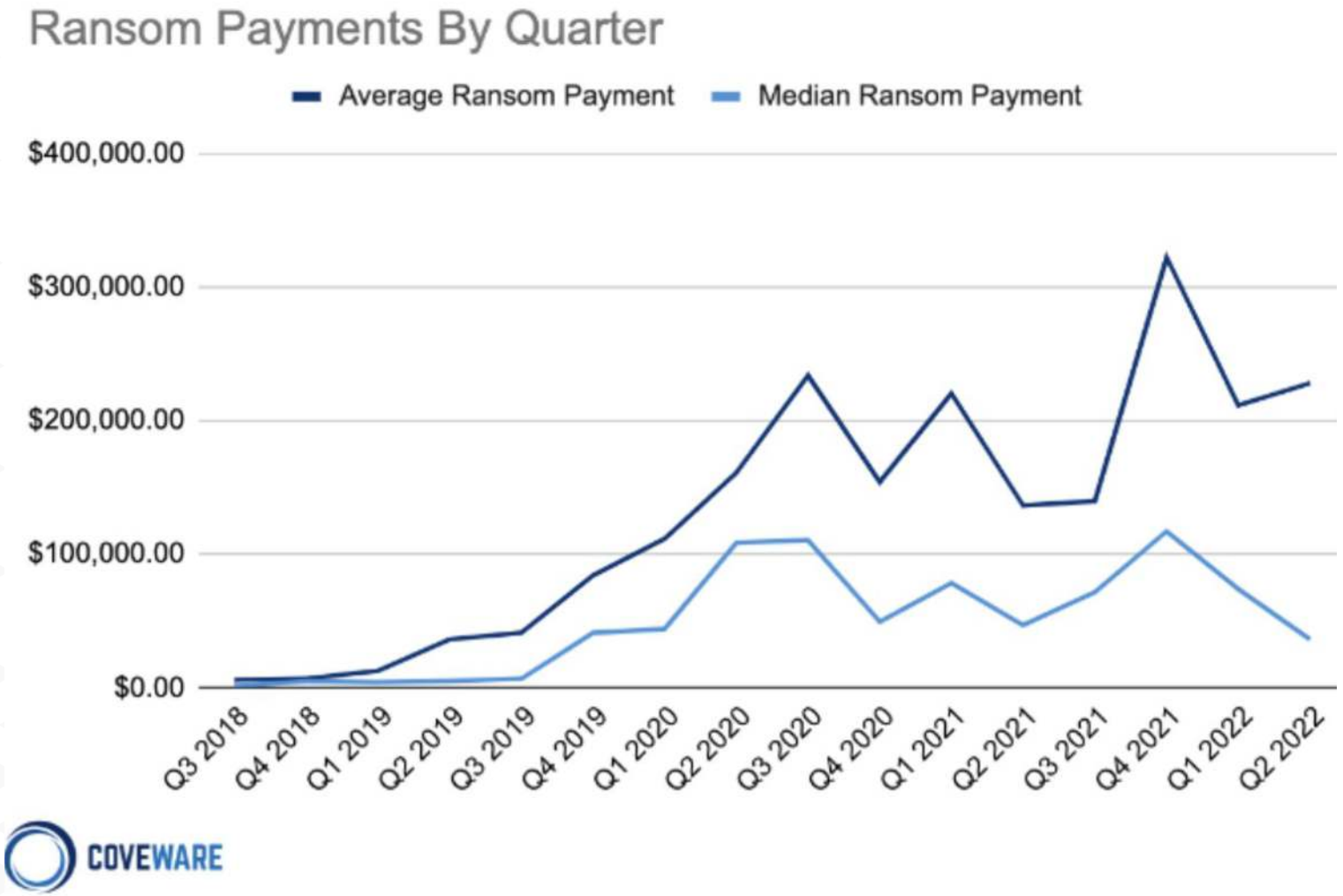
Ransomware: Unternehmen im Gesundheitswesen zahlen am häufigsten Lösegeld

Verschlüsselungsangriffe haben vor allem in der Gesundheitsbranche in den vergangenen Monaten stark zugenommen. Die Daten sind bei Angreifern beliebt.

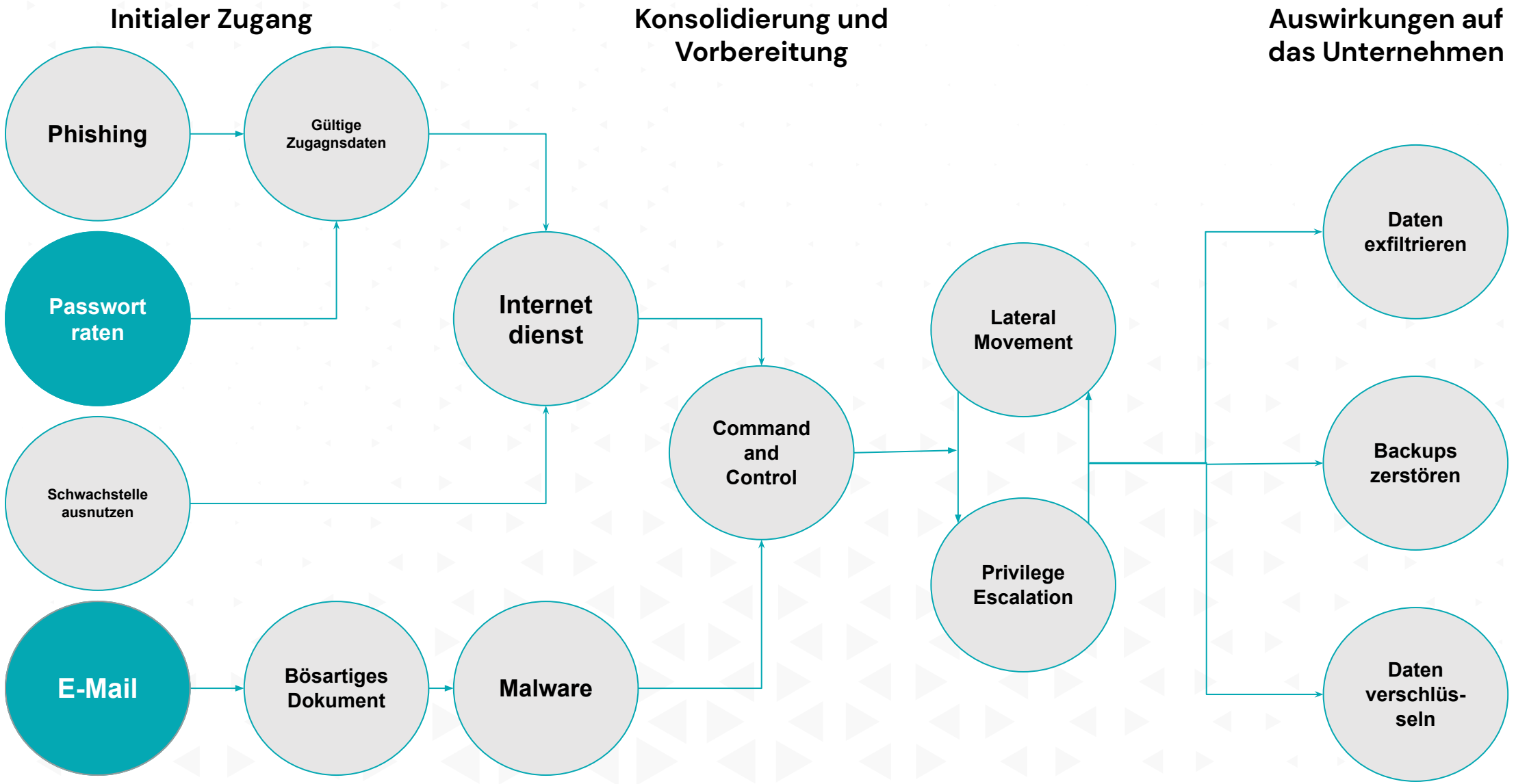
Sicherheitsvorfälle und die Konsequenzen

Ransomware wird teurer

- Die Zeiten in denen Systeme für 5.000 USD entschlüsselt werden konnten sind vorbei
- Verlagerung der Angriffe auf mittelständische Unternehmen
- Ein Ransomware-Befall zieht durchschnittlich einen Monat Ausfall mit sich und verursacht Kosten i.H.v. 1.601.615 EUR

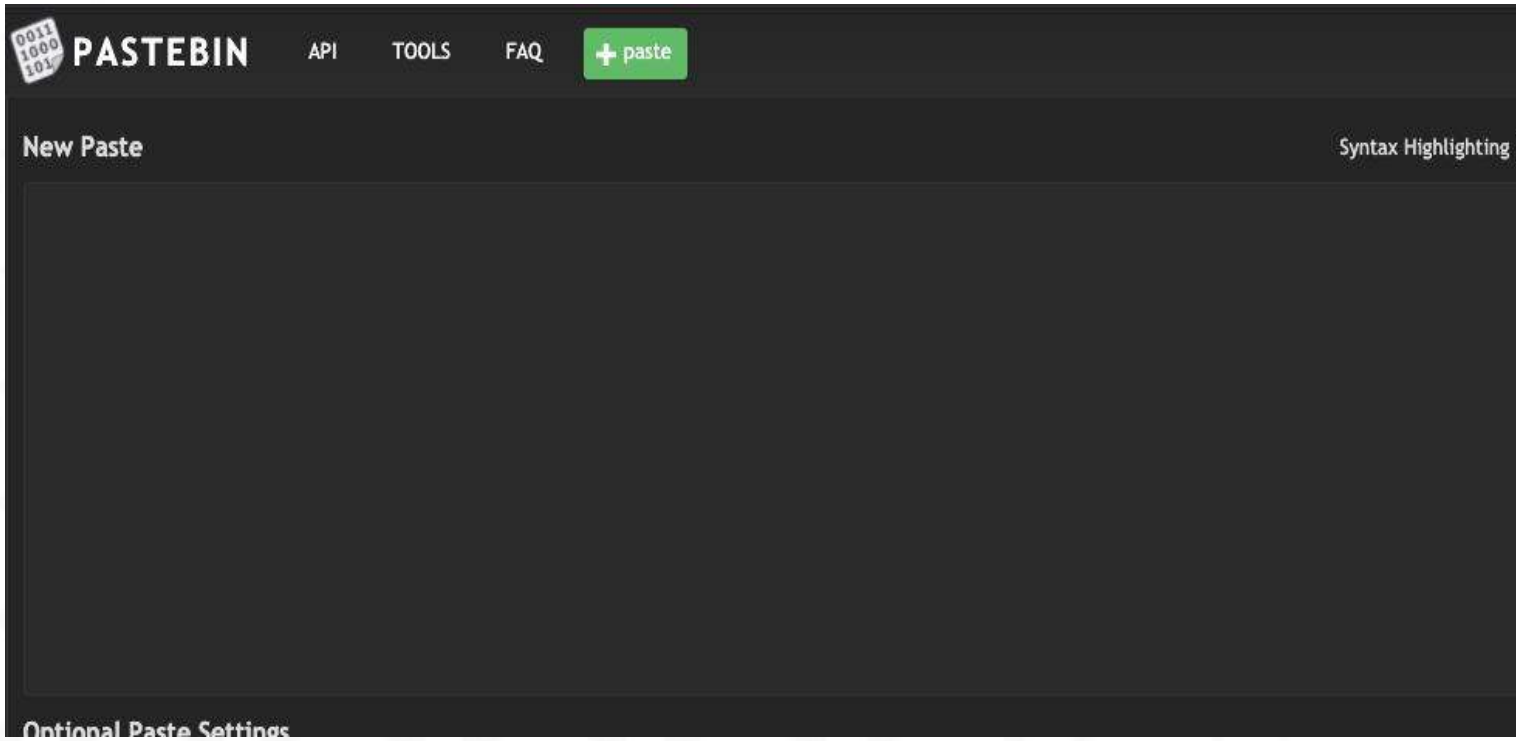


Ablauf eines Ransomware Angriffs



Zielsuche

- Ohne Ziel kein Angriff!
- Suchmaschinen können gute Anlaufstellen für die Zielsuche sein
- Pastebin stellt anonyme Beiträge bereit



Berechenbare IT-Unsicherheit

Datenmissbrauch durch Cambridge Analytica UPDATE 05.04.2018, 12:16 Uhr

Facebook-Skandal betrifft bis zu 310.000 Nutzer aus Deutschland

Hacker-Jackpot: Credit Bureau Equifax gehackt

08.09.2017 07:48 Uhr – Daniel AJ Sokolov

Passwörter im Klartext: 20.000 Euro Bußgeld nach DSGVO gegen Knuddels.de

380.000 Kreditkarten betroffen

Datenpanne bei British Airways

Stand: 07.09.2018 09:42 Uhr

Yahoo verliert bei weiterem Hack Daten von eine Milliarde Nutzerkonten

TOP 5 Passwörter in Deutschland

1. hallo
2. passwort
3. hallo123
4. schalke04
5. passwort1

TOP 5 Passwörter weltweit

1. 123456
2. 123456789
3. 1234
4. 12345
5. 12345678

Malware gibt es auch in PDFs

May 20, 2022 • Category: Threat Research • By: Patrick Schläpfer • Comments: 0

PDF Malware Is Not Yet Dead

For the past decade, attackers have preferred to package malware in Microsoft Office file formats, particularly Word and Excel. In fact, in Q1 2022 nearly half (45%) of malware stopped by HP Wolf Security used Office formats. The reasons are clear: users are familiar with these file types, the applications used to open them are ubiquitous, and they are suited to social engineering lures.

In this post, we look at a malware campaign isolated by HP Wolf Security earlier this year that had an unusual infection chain. The malware arrived in a PDF document – a format attackers less commonly use to infect PCs – and relied on several tricks to evade detection, such as embedding malicious files, loading remotely-hosted exploits, and shellcode encryption.

Figure 1 – Alert timeline in HP Wolf Security Controller showing the malware being isolated.

Der eigene Schutz

#Grundsätzliches

Vorsicht bei E-Mail Anhängen!

Insbesondere bei ZIP-Dateien und
Office Dokumenten (Vorsicht - Makros!)

Software auf allen Geräten aktuell halten!

Schwachstellen werden geschlossen, neue Sicherheits-
mechanismen ermöglicht und freigeschaltet

Legen Sie Backups an!

Egal ob von Ihren virtuellen Maschinen und
Daten.

Schulen Sie sich regelmäßig!

Newsletter, Securitynews, Tagesschau, Websites,
Blogs, Twitter, Facebook, RSS Reader ..

Der eigene Schutz

Sind gefälschte Bewerbungsmails oder andere Kampagnen im Umlauf?

Informieren Sie sich auf einschlägigen Portalen (watchlist-internet.at; mimikama.at; heise.de) über aktuelle Maschen. Alternativ können Sie gezielt bei Google, Bing oder DuckDuckGo nachschauen

Ist der Name öfter im Zusammenhang mit Betrug ggfs. Ransomware aufgetaucht?

Oft werden gleiche Namen in E-Mail Adressen verwendet. Viele Menschen berichten über diese Kampagnen und helfen bei der Aufklärung. Suchen Sie z.B. gezielt nach “Max Mustermann”. Ransomware Beispiel: “Rolf Drescher” (GoldenEye Ransomware)

WLAN und Bluetooth ausschalten!

Wenn Sie die Verbindungen nicht benötigen, kann es sinnvoll sein diese auszuschalten.
Sie sparen Akku und Ihr Smartphone/Tablet/Computer kommuniziert nicht ungewollt.

Vielen Dank

Rückfragen?

AWARE7 GmbH
Munscheidstrasse 14
45886 Gelsenkirchen

49 (0) 209 8830 6760

info@aware7.de