Datenschutz und Datensicherheit

Reinhold Okon

Datenschutzbeauftragter

DSB Okon & Meister (München/Karlsfeld)

Wenn der ET zum Admin wird

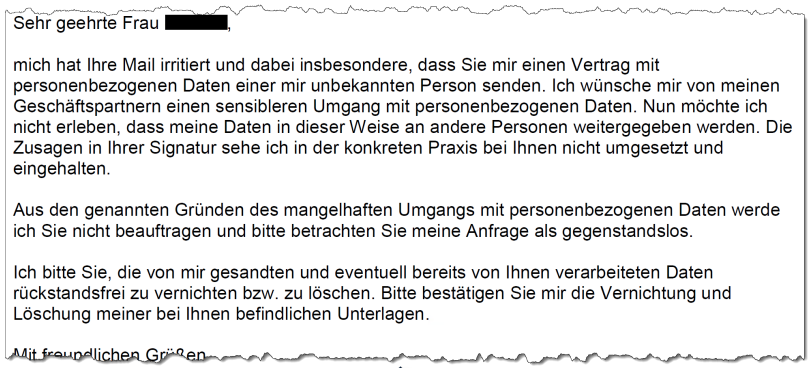
Hallo Hausverwaltung [redacted]
Ich bekomme jetzt zum siebten(!) mal eine Mail von Ihnen, dass ich meine Kontodaten aktualisieren soll. Dass Sie ein Problem in Ihrer EDV haben, ist mehr als offensichtlich. Der Virus schreit förmlich, danach entdeckt zu werden. Sie scheinen das überhaupt nicht zu erkennen. Ich frage mich, was Sie überhaupt können. Ihre Tätigkeit als Verwalter ist unter aller Kanone. Und nun auch noch Kunden in Ihren Wahnsinn, mit einzubeziehen untragbar. Tun Sie endlich was und zwar in beide Richtungen. Kann ja nicht sein, dass das so schwer ist.

Keine freundlichen Grüße

E &V sind keine Freunde mehr

Sie zeige ich an. Ihre Inkompetenz ist extrem gefährlich. Ihr Herr [redacted] ist, genau wie Sie, ein Verbrecher. Wo sind denn jetzt meine Daten hingekommen? Zu den Russen offensichtlich! Nur weil Sie zu blöd sind, muss nun unsere Gemeinschaft um den Fortbestand der Verwaltung bangen. Ihre Blödheit ist unfassbar! ICH ZEIGE SIE AN. Sie haben mit Ansage die Daten vernichtet. Das ist das dritte Mal in 3 Jahren. Ich werde dies mit der Gemeinschaft klären.

Datenschutz wird durch Betroffene geprüft



Sehr geehrte Frau [redacted],

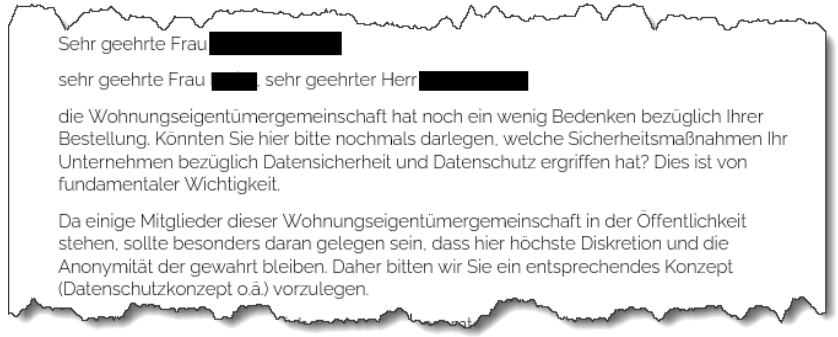
mich hat Ihre Mail irritiert und dabei insbesondere, dass Sie mir einen Vertrag mit personenbezogenen Daten einer mir unbekannten Person senden. Ich wünsche mir von meinen Geschäftspartnern einen sensibleren Umgang mit personenbezogenen Daten. Nun möchte ich nicht erleben, dass meine Daten in dieser Weise an andere Personen weitergegeben werden. Die Zusagen in Ihrer Signatur sehe ich in der konkreten Praxis bei Ihnen nicht umgesetzt und eingehalten.

Aus den genannten Gründen des mangelhaften Umgangs mit personenbezogenen Daten werde ich Sie nicht beauftragen und bitte betrachten Sie meine Anfrage als gegenstandslos.

Ich bitte Sie, die von mir gesandten und eventuell bereits von Ihnen verarbeiteten Daten rückstandsfrei zu vernichten bzw. zu löschen. Bitte bestätigen Sie mir die Vernichtung und Löschung meiner bei Ihnen befindlichen Unterlagen.

Mit freundlichen Grüßen

Datenoffenlegung



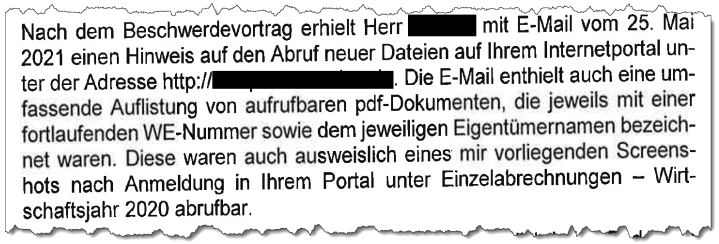
Sehr geehrte Frau [redacted]

sehr geehrte Frau [redacted], sehr geehrter Herr [redacted]

die Wohnungseigentümergemeinschaft hat noch ein wenig Bedenken bezüglich Ihrer Bestellung. Könnten Sie hier bitte nochmals darlegen, welche Sicherheitsmaßnahmen Ihr Unternehmen bezüglich Datensicherheit und Datenschutz ergriffen hat? Dies ist von fundamentaler Wichtigkeit.

Da einige Mitglieder dieser Wohnungseigentümergemeinschaft in der Öffentlichkeit stehen, sollte besonders daran gelegen sein, dass hier höchste Diskretion und die Anonymität der gewahrt bleiben. Daher bitten wir Sie ein entsprechendes Konzept (Datenschutzkonzept o.ä.) vorzulegen.

Verwalterbestellung

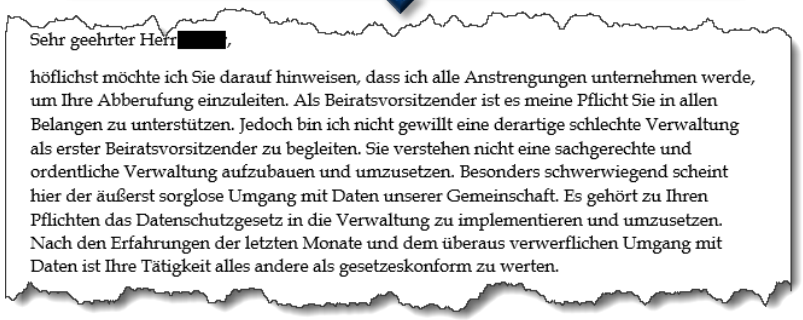


Nach dem Beschwerdevortrag erhielt Herr [redacted] mit E-Mail vom 25. Mai 2021 einen Hinweis auf den Abruf neuer Dateien auf Ihrem Internetportal unter der Adresse http://[redacted]. Die E-Mail enthielt auch eine umfassende Auflistung von aufrufbaren pdf-Dokumenten, die jeweils mit einer fortlaufenden WE-Nummer sowie dem jeweiligen Eigentümernamen bezeichnet waren. Diese waren auch ausweislich eines mir vorliegenden Screenshots nach Anmeldung in Ihrem Portal unter Einzelabrechnungen – Wirtschaftsjahr 2020 abrufbar.

Webportal

Die Realität!

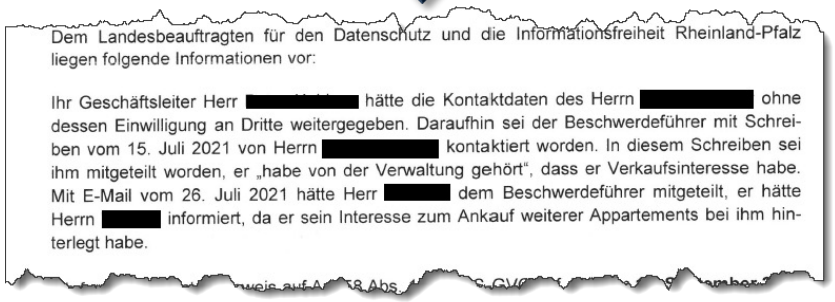
Datenschutzmissachtung



Sehr geehrter Herr [redacted],

höflichst möchte ich Sie darauf hinweisen, dass ich alle Anstrengungen unternehmen werde, um Ihre Abberufung einzuleiten. Als Beiratsvorsitzender ist es meine Pflicht Sie in allen Belangen zu unterstützen. Jedoch bin ich nicht gewillt eine derartige schlechte Verwaltung als erster Beiratsvorsitzender zu begleiten. Sie verstehen nicht eine sachgerechte und ordentliche Verwaltung aufzubauen und umzusetzen. Besonders schwerwiegend scheint hier der äußerst sorglose Umgang mit Daten unserer Gemeinschaft. Es gehört zu Ihren Pflichten das Datenschutzgesetz in die Verwaltung zu implementieren und umzusetzen. Nach den Erfahrungen der letzten Monate und dem überaus verwerflichen Umgang mit Daten ist Ihre Tätigkeit alles andere als gesetzeskonform zu werten.

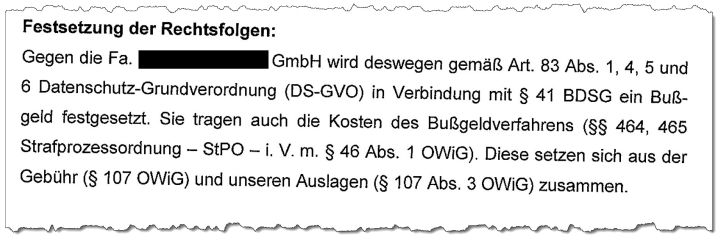
Datenweitergabe



Dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz liegen folgende Informationen vor:

Ihr Geschäftsleiter Herr [redacted] hätte die Kontaktdaten des Herrn [redacted] ohne dessen Einwilligung an Dritte weitergegeben. Daraufhin sei der Beschwerdeführer mit Schreiben vom 15. Juli 2021 von Herrn [redacted] kontaktiert worden. In diesem Schreiben sei ihm mitgeteilt worden, er „habe von der Verwaltung gehört", dass er Verkaufsinteresse habe. Mit E-Mail vom 26. Juli 2021 hätte Herr [redacted] dem Beschwerdeführer mitgeteilt, er hätte Herrn [redacted] informiert, da er sein Interesse zum Ankauf weiterer Appartements bei ihm hinterlegt habe.

Bußgeld



Festsetzung der Rechtsfolgen:

Gegen die Fa. [redacted] GmbH wird deswegen gemäß Art. 83 Abs. 1, 4, 5 und 6 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 41 BDSG ein Bußgeld festgesetzt. Sie tragen auch die Kosten des Bußgeldverfahrens (§§ 464, 465 Strafprozessordnung – StPO – i. V. m. § 46 Abs. 1 OWiG). Diese setzen sich aus der Gebühr (§ 107 OWiG) und unseren Auslagen (§ 107 Abs. 3 OWiG) zusammen.

DSB Okon & Meister

ista

Ein Konzept zur Sicherheit?

Sehr geehrte Frau [redacted]

sehr geehrte Frau [redacted], sehr geehrter Herr [redacted]

die Wohnungseigentümergemeinschaft hat noch ein wenig Bedenken bezüglich Ihrer Bestellung. Könnten Sie hier bitte nochmals darlegen, welche Sicherheitsmaßnahmen Ihr Unternehmen bezüglich Datensicherheit und Datenschutz ergriffen hat? Dies ist von fundamentaler Wichtigkeit.

Da einige Mitglieder dieser Wohnungseigentümergemeinschaft in der Öffentlichkeit stehen, sollte besonders daran gelegen sein, dass hier höchste Diskretion und die Anonymität der gewahrt bleiben. Daher bitten wir Sie ein entsprechendes Konzept (Datenschutzkonzept o.ä.) vorzulegen.

Ransomware 2022 und 2023 eine Erfolgsgeschichte?

Unternehmen	Wann	Was	Quelle
Medizinischer Dienst	Jun 23		CSO
Deutsche Leasing	Jun 23		CSO
Verlagsgruppe VRM	Ende Mai 2023		CSO
Hosting-Dienstleister von Dena	Mai 23	Ransomware	CSO
United Hoster	Mai 23	Ransomware	CSO
Dienstleister von Heineking Media	Mai 23		CSO
Black Cat Networks	Mai 23	Ransomware	CSO
GITAI	Mai 23	Ransomware	CSO
Maxim Group	Anfang Mai2023	Ransomware	CSO
Lux Automation		Ransomware	CSO
Bilstein Gruppe	Ende April 2023	Ransomware	CSO
Stürtz Maschinenbau	22. Apr 23	Ransomware	DSGVO Portal
Badische Stahlwerke	20. Apr 23		CSO
Jobrad		Ransomware	CSO
Bitmarck	Apr 23		CSO
Lürssen	Apr 23	Ransomware	CSO
Evotec	06. Apr 23		CSO
Üstra	31. Mrz 23		CSO
BIG direkt	28. Mrz 23		Ruhr Nachrichten
Materna	25. Mrz 23		CSO
SAF Holland	Mrz 23		CSO
Matthäi	17. Mrz 23	Ransomware	CSO
Energieversorgung Filstal	13. Mrz 23	DDoS	CSO
Rheinmetall, NW	07. Mrz 23	DDoS	CSO
Steico, BY	01. Mrz 23	n.a.	CSO
Smart InsurTech, BE	10. Feb 23	n.a.	Smart InsurTech
Albert Ziegler, BW	09. Feb 23	n.a.	CSO
Unternehmen in Bayern, BY	06. Feb 23	Ransomware	Polizei Bayern
Kapellmann und Partner Rechtsanwälte, NW	03. Feb 23	Ransomware	Kapellmann
Häfele, BW	02. Feb 23	Ransomware	CSO
Stadtwerke Karlsruhe, BW	01. Feb 23	Ransomware	CSO
Dürr, BW	Feb 23	n.a.	CSO
Bayerischer Rundfunk, BY	Feb 23	Phishing	CSO
Geze, BW	Feb 23	n.a.	Geze
Wisag Dienstleistungsholding, HE	Feb 23	n.a.	Frankfurter Allgemeine Zeitung
Flughafen Hamburg, HH	25. Jan 23	DDoS	Hamburger Abendblatt
Plüsch-Tierheim, NW	24. Jan 23	n.a.	CSO
Sky Deutschland, BY	21. Jan 23	n.a.	Digital Fernsehen
Bitmarck, NW	19. Jan 23	n.a.	CSO
Fritzmeier Group, BY	17. Jan 23	n.a.	CSO
Adesso, NW	11. Jan 23	n.a.	CSO
Unternehmen in Kaiserslautern, RP	Jan 23	Social Engineering	

Warum ist Ransomware so erfolgreich?

1. Effektive Taktik
2. Leichte Durchführbarkeit
3. Schwierigkeiten bei der Verfolgung
4. Hohe Profitabilität
5. Mangelnder Schutz

Lösegeldforderungen

253.160 € Lösegeld

war 2021 das durchschnittlich gezahlte Lösegeld von Unternehmen in Deutschland, um Daten, die durch Ransomware verschlüsselt wurden, wieder verfügbar zu machen. Dies zeigt eine neue Sophos-Studie „State of Ransomware 2022“ welche am 27. April 2022 veröffentlicht wurde. Demnach haben 42 % der deutschen Unternehmen ein Lösegeld bezahlt, um wieder in die „Spur der Produktivität“ zurückzukommen.

https://news.sophos.com/de-de/2022/04/27/state-of-ransomware-2022-studie-das-angriffskarussell-dreht-sich-immer-schneller/

Was wird angegriffen?

Die primären „Angriffsziele“
waren 2021 in der Regel die Datensicherung, Systeme zur Datenspeicherung (NAS), Betriebssysteme, Datenbanken und Cloudsysteme.

Nach der „Infektion“ werden die Systeme meist „beobachtet“ um zu lernen. D.h., in den meisten Fällen lässt sich der „Infektionszeitraum“ nur sehr schwer bestimmen. Das macht es dem Admin schwer, das „Einfallstor“ zu finden und zu bestimmen

https://news.sophos.com/de-de/2022/04/27/state-of-ransomware-2022-studie-das-angriffskarussell-dreht-sich-immer-schneller/

Wie kommt der Schädling ins Netz?

Das „Einfallstor“

war 2021 in der Regel die „Gutgläubigkeit“, der „Leichtsinn“ und die „Unwissenheit“ der PC-Nutzer. Meist durch Klick auf Links, E-Mail-Anhänge geöffnet, Websites besucht, die Schwachstellen im Browser ausnutzen und Phishing-Mails beantwortet.

Außerdem sind infizierte Softwareprodukte und kompromittierte Zugangsdaten weitere Wege ins Unternehmensnetzwerk. Auch „Social Engineering“ wir zunehmend zum Problem!

https://news.sophos.com/de-de/2022/04/27/state-of-ransomware-2022-studie-das-angriffskarussell-dreht-sich-immer-schneller/

Die E-Mail nebst Anhang

RAe [redacted].de>

WG: Bewerbung als Rechtsanwaltsgehilfe

An GEON-Systems / Reinhold Okon

Joe Oki

Nachricht Bewerbungsmappe-Schmitt.docm (1 MB)

Oki ich habe das geöffnet, bitte rufe mich an
Andrea

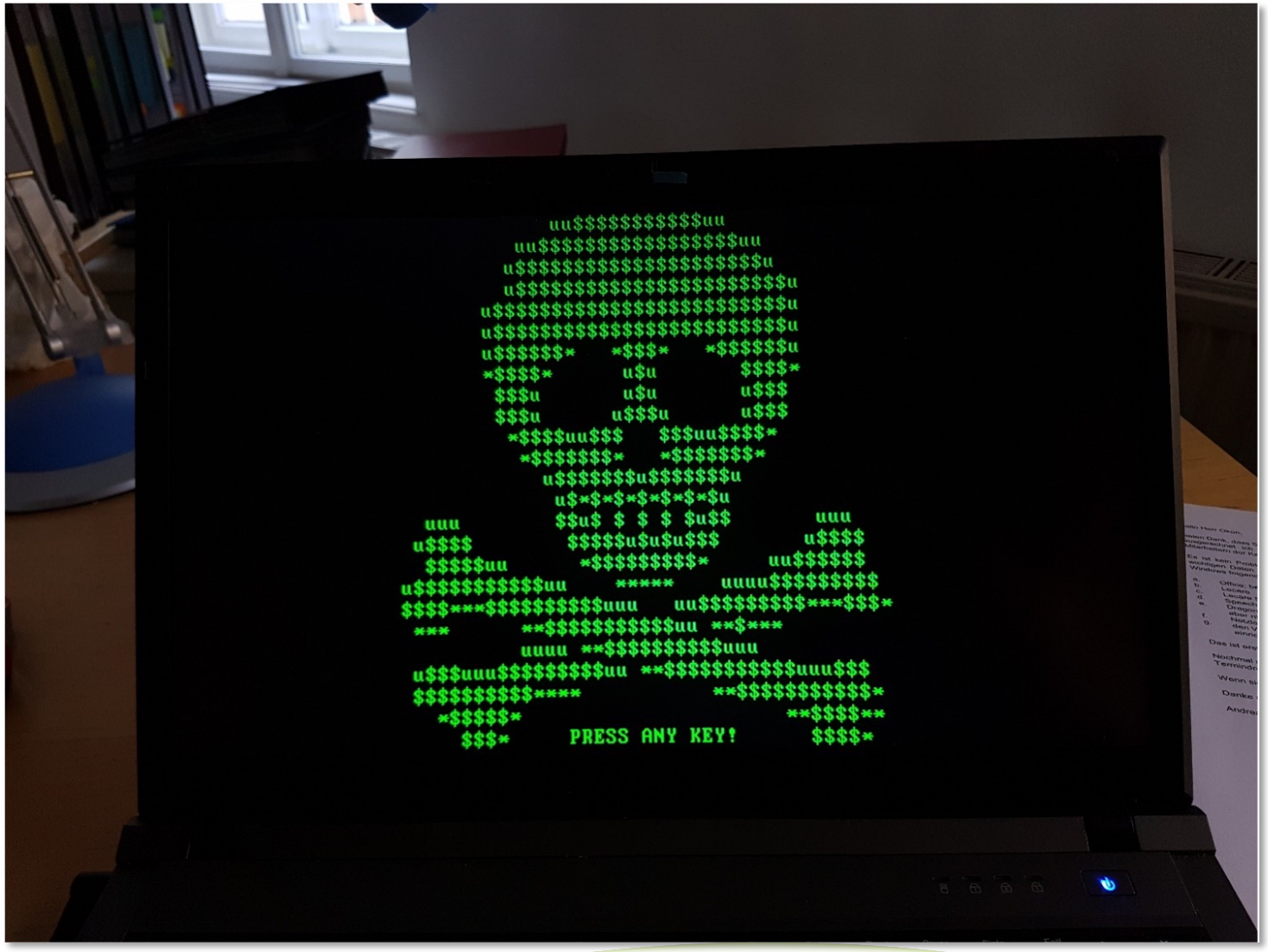
Von: Tobias Schmitt [mailto:t.schmitt@bsz-trier.de]
Gesende[redacted]00:00
An: RAe [redacted]
Betreff: Bewerbung als Rechtsanwaltsgehilfe

Sehr geehrte Damen und Herren,

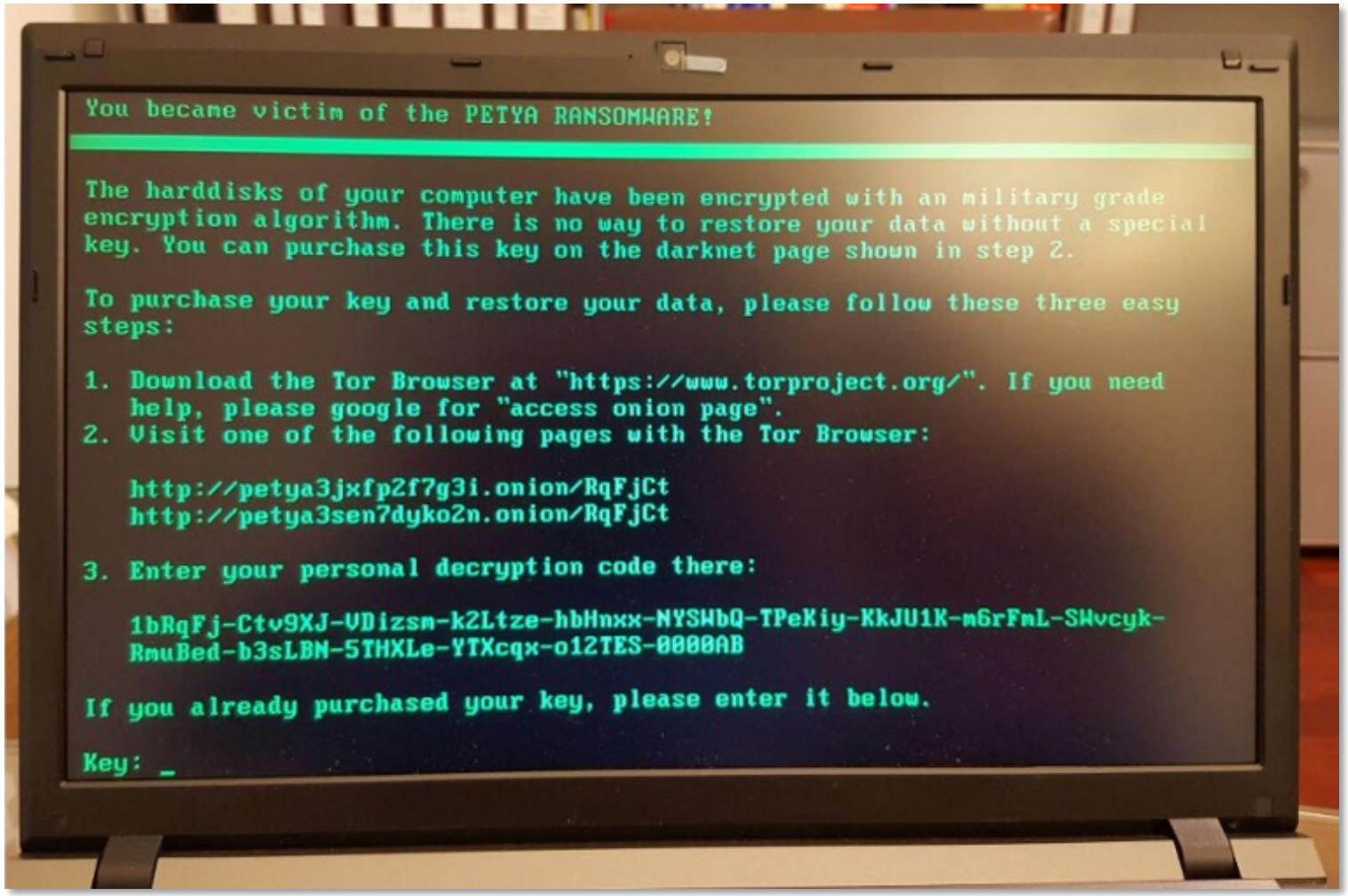
hiermit bewerbe ich mich als Rechtsanwaltsgehilfe bei Ihnen. Anbei finden Sie meine Berwerbungsmappe.

Mit freundlichem Gruß
Tobias Schmitt

Und jetzt?



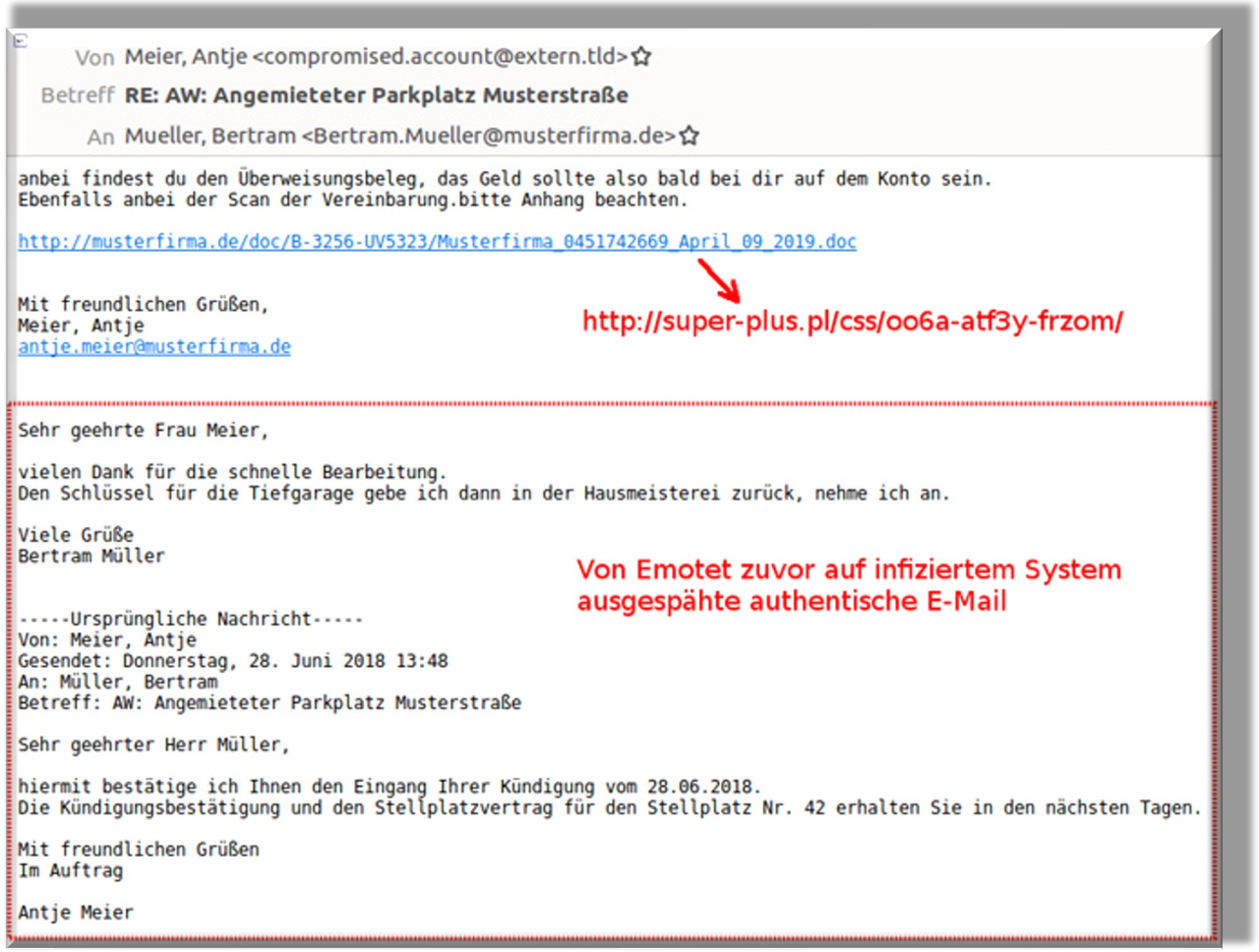
Ich hab´ ja eine Datensicherung



Eine reine Datensicherung reicht hier nicht mehr aus. Arbeitsplatz/PC/Server/Laptop muss wieder in den vorherigen Zustand zurück versetzt werden.

Sämtliche Programme, Einstellungen und Userspezifische Anwendungen müssen wieder hergestellt werden. Die wenigsten Unternehmen beachten dieses große Problem.

Beispiel: „Emotet“



Von Meier, Antje <compromised.account@extern.tld>
Betreff **RE: AW: Angemieteter Parkplatz Musterstraße**
An Mueller, Bertram <Bertram.Mueller@musterfirma.de>

anbei findest du den Überweisungsbeleg, das Geld sollte also bald bei dir auf dem Konto sein.
Ebenfalls anbei der Scan der Vereinbarung.bitte Anhang beachten.

http://musterfirma.de/doc/B-3256-UV5323/Musterfirma_0451742669_April_09_2019.doc

Mit freundlichen Grüßen,
Meier, Antje
antje.meier@musterfirma.de

http://super-plus.pl/css/oo6a-atf3y-frzom/

Sehr geehrte Frau Meier,

vielen Dank für die schnelle Bearbeitung.
Den Schlüssel für die Tiefgarage gebe ich dann in der Hausmeisterei zurück, nehme ich an.

Viele Grüße
Bertram Müller

Von Emotet zuvor auf infiziertem System ausgespähte authentische E-Mail

-----Ursprüngliche Nachricht-----
Von: Meier, Antje
Gesendet: Donnerstag, 28. Juni 2018 13:48
An: Müller, Bertram
Betreff: AW: Angemieteter Parkplatz Musterstraße

Sehr geehrter Herr Müller,

hiermit bestätige ich Ihnen den Eingang Ihrer Kündigung vom 28.06.2018.
Die Kündigungsbestätigung und den Stellplatzvertrag für den Stellplatz Nr. 42 erhalten Sie in den nächsten Tagen.

Mit freundlichen Grüßen
Im Auftrag

Antje Meier

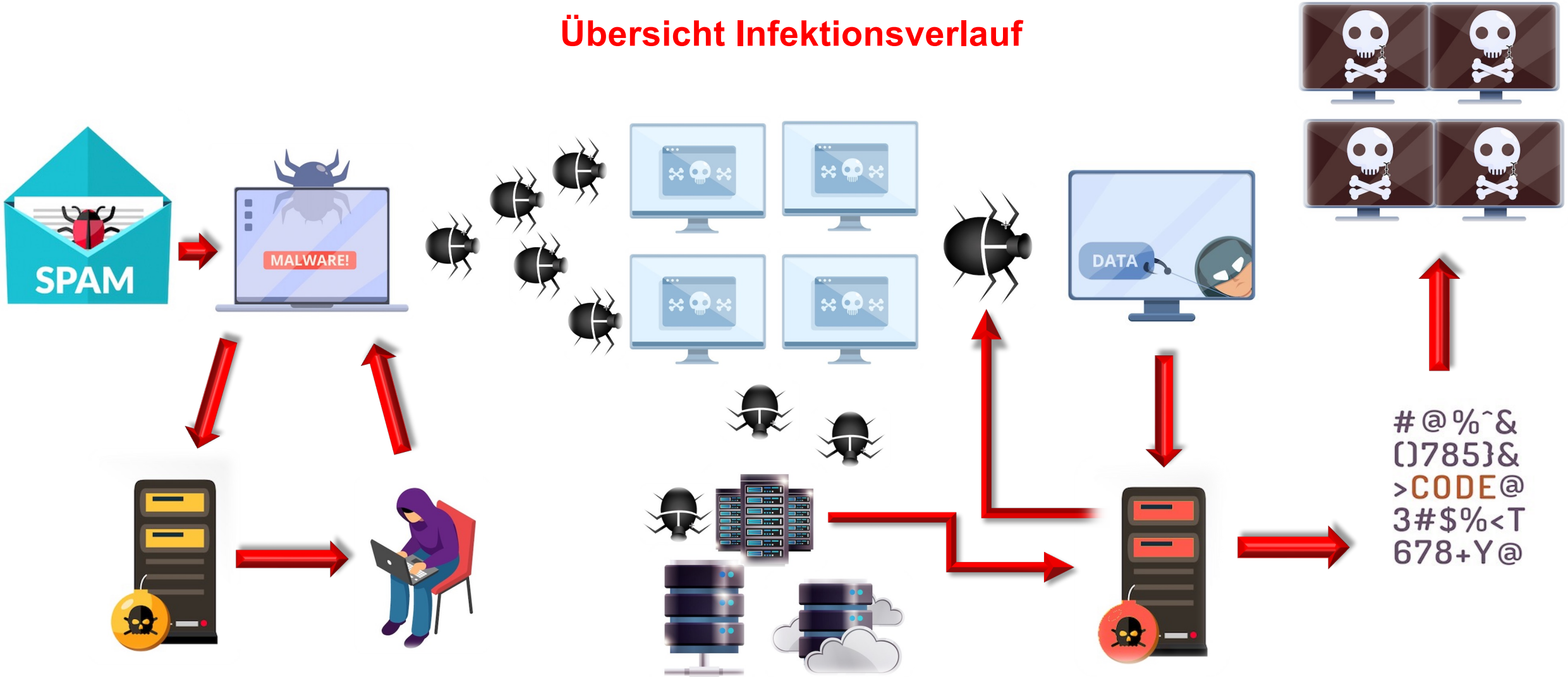
Korrespondenz, die lange nach der ursprünglichen Mail eintrifft

Vorher geführte Korrespondenz

https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/emotet-trojaner-beantwortet-empfangene-emails-und-klaut-anhaenge-35502

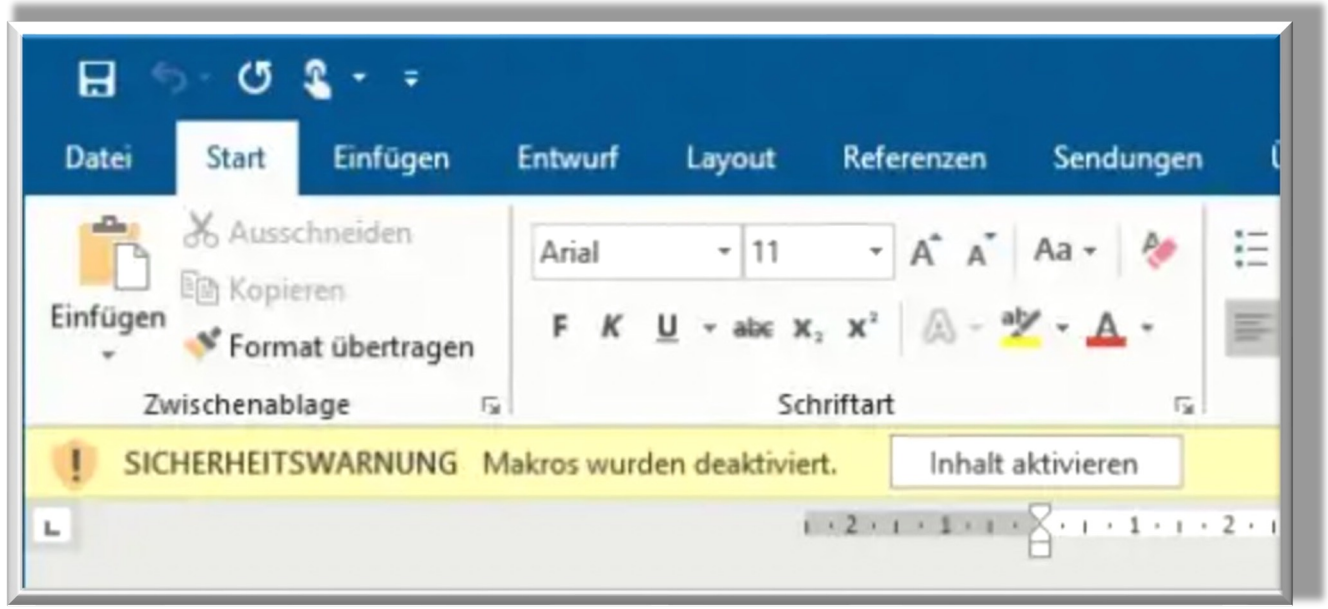
Wie läuft ein Angriff ab?

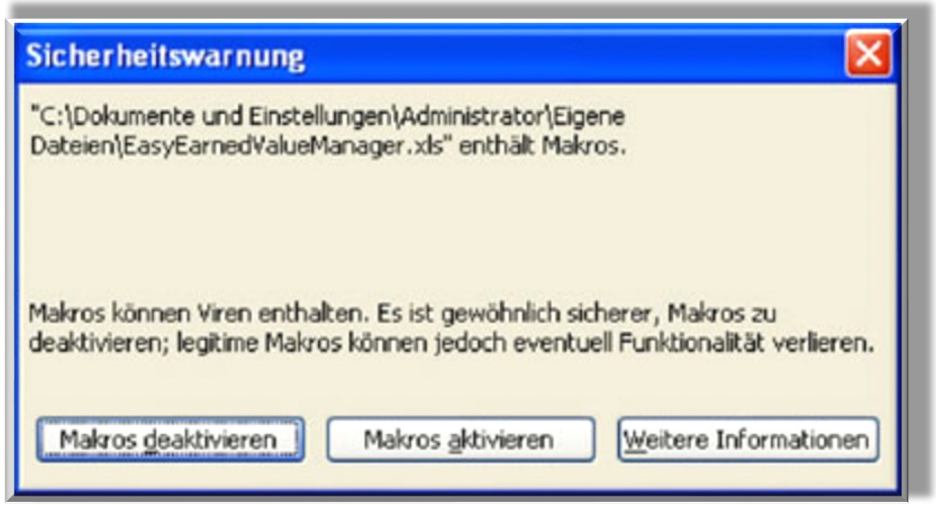
Übersicht Infektionsverlauf



Beispiel Trickbot: Wie wird er scharfgeschaltet?

Das richtige GO ist eigentlich der Klick zur Aktivierung der Makros. Dadurch werden die Skripte geladen und der Verschlüsselungsprozess kann beliebig gestartet und ausgeführt werden.





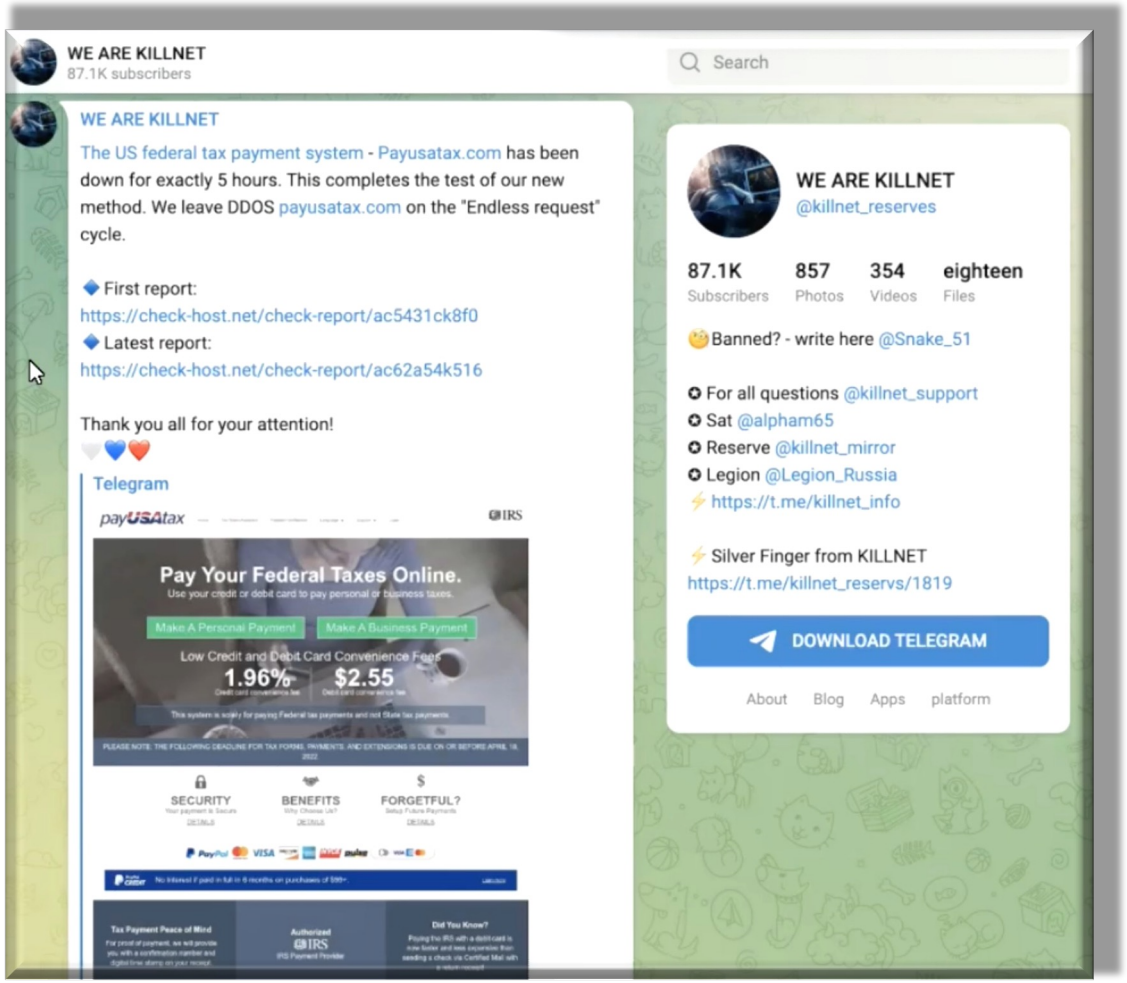
Makro-Blockierung durch Microsoft

Die Verbreitung von Emotet hat etwas nachgelassen. Denn Microsoft hat seit April 2022 bei den Office-Programmen VBA-Makros, die mit Dateien aus dem Internet heruntergeladen werden, standardmäßig blockiert.

Beispiel Trickbot: Was kann er alles?

- Er kann Benutzernamen, Password-Hashs und andere nützliche Informationen stehlen, die später für Seitwärtsbewegung im Netzwerk vom Active Directory und der Registrierdatenbank aus eingesetzt werden können.
- Netzwerkverkehr auf dem infizierten Computer abfangen.
- Er ermöglicht per VNC-Protokoll Bedienungsoperationen über einen entfernten Rechner auszuführen.
- Cookies von Browsern stehlen.
- Zugangsdaten im Registry, der Datenbank von mehreren Anwendungen und Konfigurationsdateien, extrahieren. Darüber hinaus kann er auch private Schlüssel, SSL-Zertifikate und Datendateien für Krypto-Wallets stehlen.
- Autofill-Daten in Browsern und Informationen, die Benutzer in Online-Formularen angeben, abfangen.
- Dateien auf FTP- und SFTP-Servers scannen.
- Schädliche Skripte in Webseiten einbetten.
- Browser-Traffic über einen Proxy umleiten.
- Die APIs, die für die Zertifikatskettenprüfung zuständig sind, für Zertifikat-Spoofing knacken, d. h. gefälschte Zertifikate als glaubwürdig darstellen.
- Zugangsdaten von Outlook-Profilen sammeln, E-Mails im Outlook abfangen und Spam über den E-Mail-Client schicken.
- Nach der Outlook Web App (OWA) suchen und die App knacken.
- Low-Level-Zugriff auf Hardware bekommen.
- Zugriff auf einen Computer auf Hardware-Ebene verschaffen.
- Schwachstellen bei Domains suchen.
- Die Adressen von SQL-Servern ausfindig machen und darüber Suchanfragen durchführen.
- Sich über der Exploits von EternalRomance und EternalBlue verbreiten.
- VPN-Verbindungen herstellen.

Wer greift die großen Unternehmen an?



Ransomware-Angreifer können aus verschiedenen Ländern und Regionen der Welt stammen, da es sich um eine Art von Cyberkriminalität handelt, die von überall aus durchgeführt werden kann. In vielen Fällen handelt es sich um organisierte kriminelle Gruppen oder Einzelpersonen, die darauf aus sind, Geld durch Erpressung zu erpressen.

Einige der Länder, die für Ransomware-Angriffe bekannt sind, sind **Russland, China, Nordkorea und Iran**. Dies liegt daran, dass diese Länder eine relativ schwache Durchsetzung von Cyberkriminalitätsgesetzen haben und oft als sichere Häfen für Cyberkriminelle dienen.

Großer Akteur ist die Pro-russische Hackergruppe Killnet

Diese Gruppe besteht seit ca. März 2022. Sie sind hauptsächlich für DDOS-Angriffe auf kritische Infrastrukturen verantwortlich.

https://www.all-about-security.de/podcast/we-are-killnet-die-pro-russische-hackergruppe-setzt-deutschland-auf-der-abschussliste/

Wer greift die kleinen Unternehmen und Privatpersonen an?

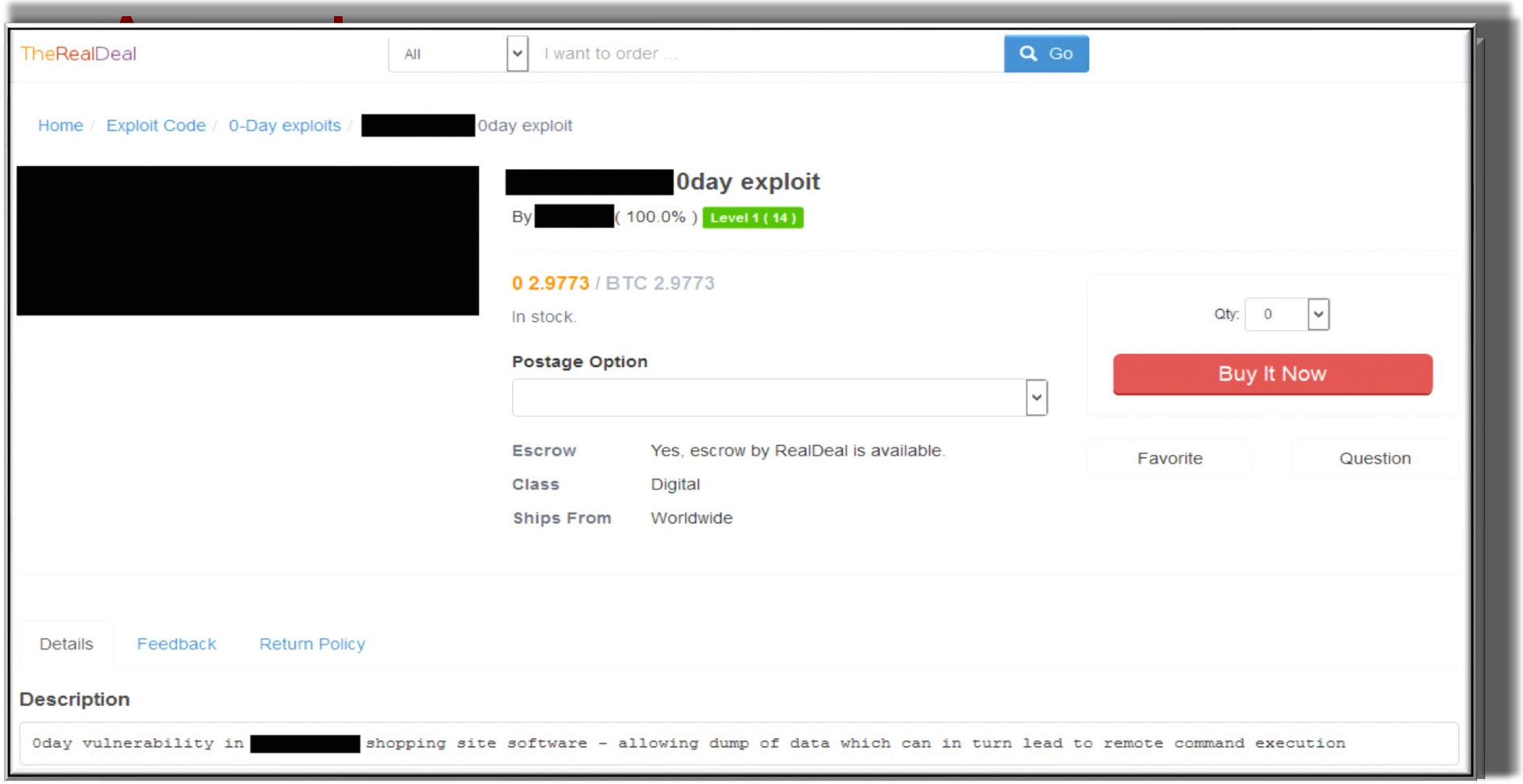
Script-Kiddies, Freizeit-Hacker und „Normalos“

Das **Darknet** bietet eine Fülle von vorgefertigten „Baukästen“, welche schon komplett mit allen Features ausgestattet sind. Es sind nahezu keinerlei Programmierkenntnisse mehr notwendig. Man benötigt lediglich einen schnellen PC, VPN, Torbrowser, einen guten Virenschutz, eine Firewall, etwas Geld und ein wenig Mut.

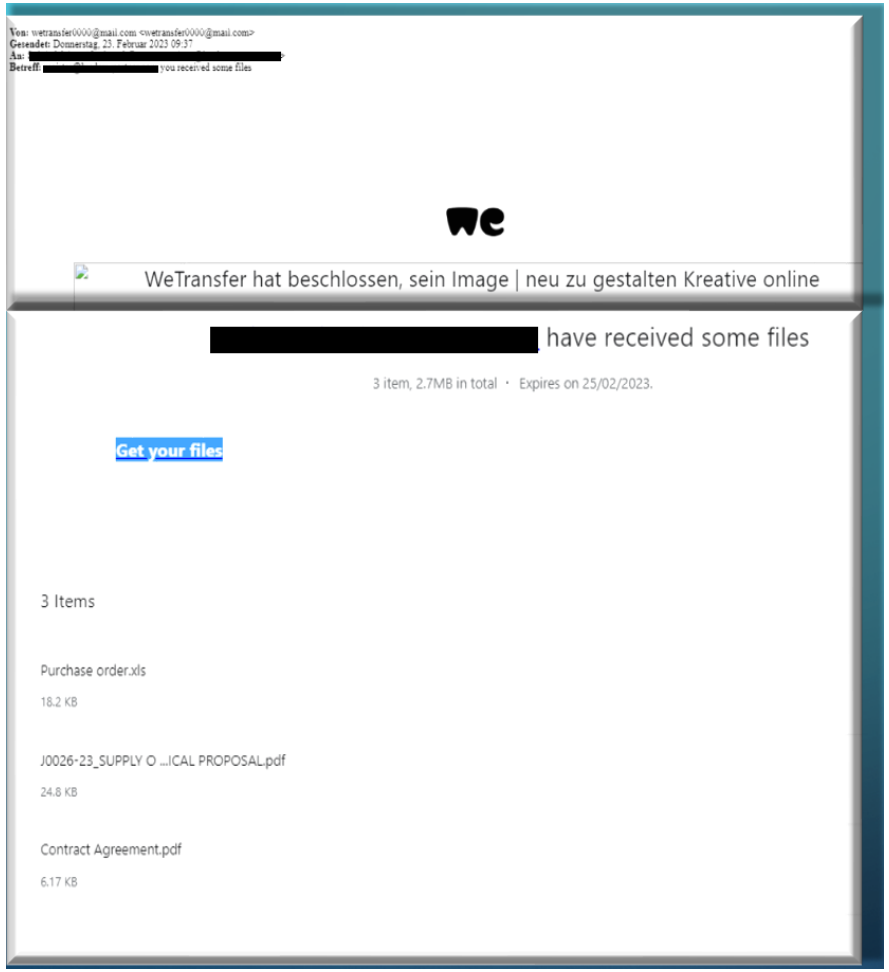
Die Vielfalt ist groß!

Woher bekommt man einen Baukasten?

„TheRealDeal“ Einkaufen wie bei



Welche Produkte funktionieren am besten?

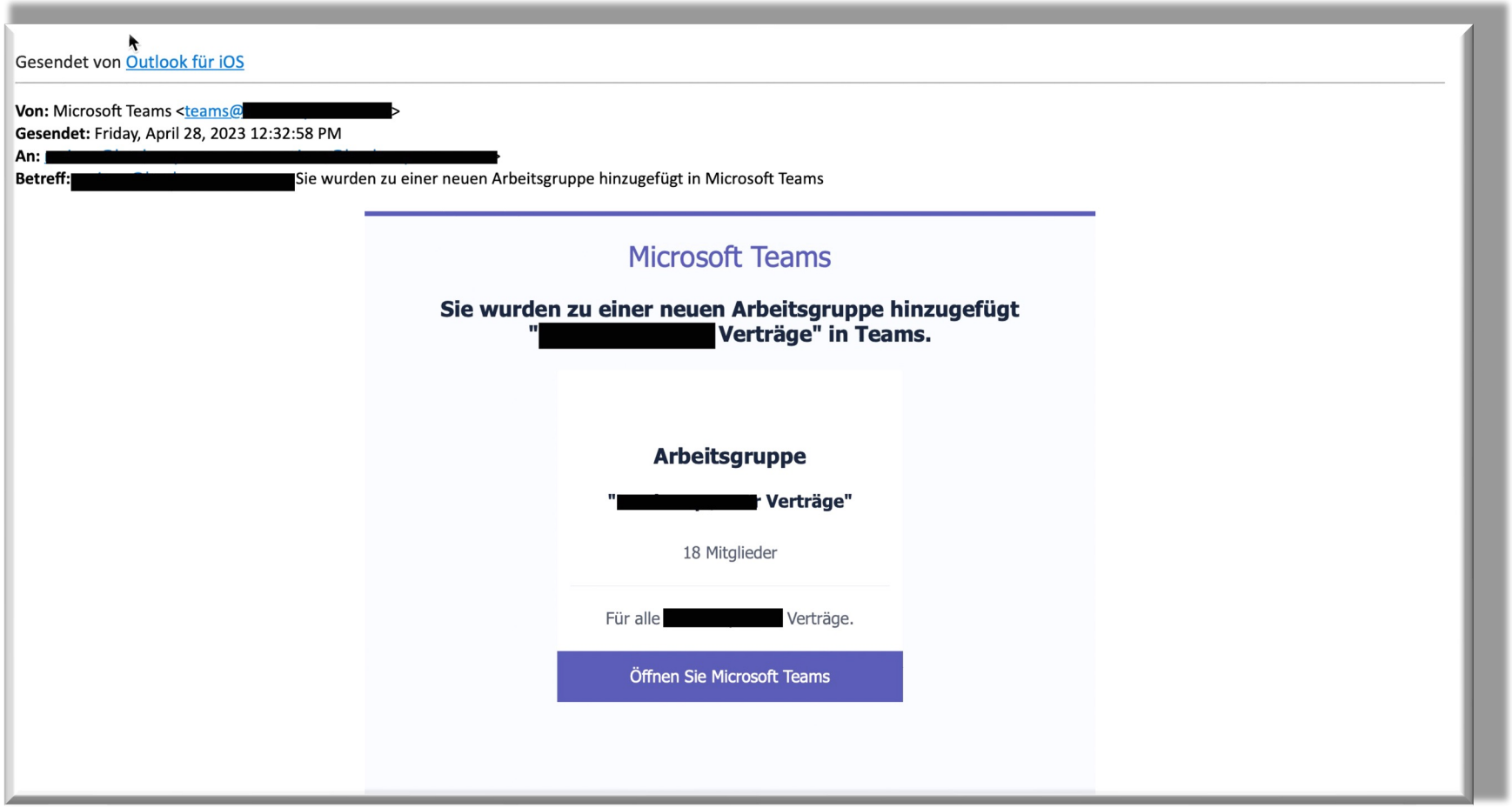


Programme und Software im täglichen Alltag. Meist wird ein Schadprogramm in einem bekannten, jedoch Fake-Programm versteckt.

D.h. es wird ein Programm vorgegaukelt, welches nur den Abzug von Daten und/oder die Infiltration beabsichtigt.

Der User merkt erst mal nichts. Meist wird ein Fehler ausgegeben, bei welchem der User dann auf die originale Website geleitet wird.

Microsoft als SPAM und Gefahrenquelle



Gesendet von Outlook für iOS

Von: Microsoft Teams <teams@[redacted]>
Gesendet: Friday, April 28, 2023 12:32:58 PM
An: [redacted]
Betreff: [redacted]Sie wurden zu einer neuen Arbeitsgruppe hinzugefügt in Microsoft Teams

Microsoft Teams

Sie wurden zu einer neuen Arbeitsgruppe hinzugefügt "[redacted]Verträge" in Teams.

Arbeitsgruppe

"[redacted]- Verträge"

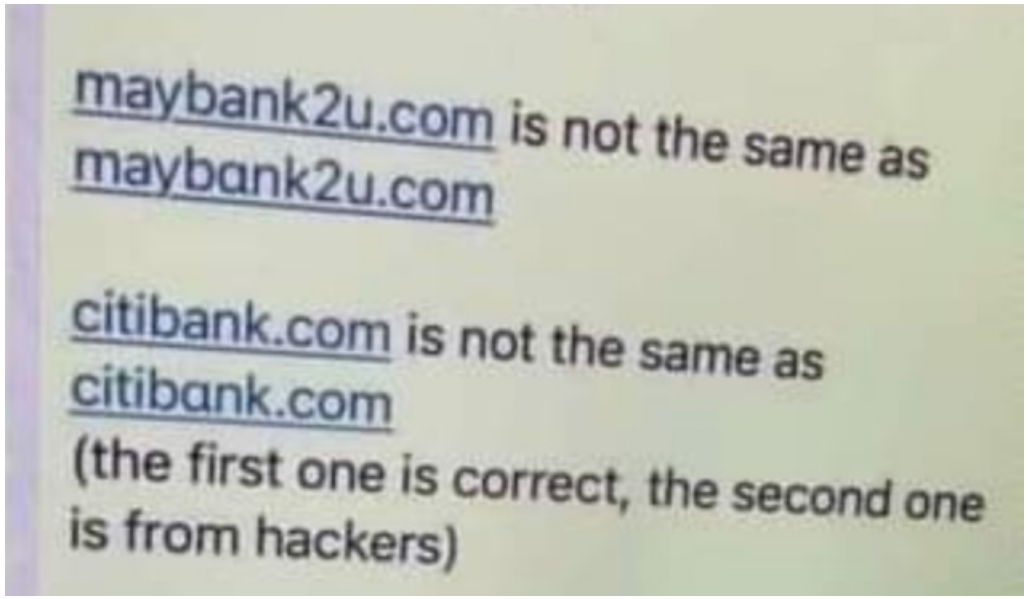
18 Mitglieder

Für alle [redacted] Verträge.

Öffnen Sie Microsoft Teams

Diese Mail wurde von fast allen Empfängern geöffnet

Irreführung durch Buchstabendreher



Ein Link mit Buchstabendreher

D.h. es wird ein Link vorgegaukelt, welcher nur den Abzug von Daten und/oder die Infiltration beabsichtigt.

Der User merkt erst mal nichts. Meist wird auf die Fakewebsite weitergeleitet bei welchem der User dann seine Daten eingibt. Wird dann bestätigt, wird meiste ein Fehler ausgegeben und auf die originale Website weitergeleitet.

Und PDF?

https://www.it-daily.net/it-sicherheit/cybercrime/malware-greift-unternehmen-mit-schaedlicher-pdf-datei-an

Der Banking-Trojaner **Qbot** wird über die echte Geschäftskorrespondenz eines potentiellen Opfers verbreitet, die zuvor von den Cyberkriminellen gestohlen wurde. Hierfür wird eine E-Mail an alle Teilnehmer weitergeleitet, in der sie in der Regel unter Angabe eines plausiblen Grundes aufgefordert werden, den schädlichen PDF-Anhang zu öffnen. Die Angreifer bitten beispielsweise darum, alle im Anhang enthaltenen Unterlagen weiterzuleiten oder die vereinbarte Auftragssumme auf Grundlage der im Anhang veranschlagten Kosten zu berechnen.

Wird das PDF geöffnet, wird ein schädliches Archiv von einem Remote-Server auf den Computer des Opfers heruntergeladen.

Wie sieht die Zukunft von Hacker aus ?

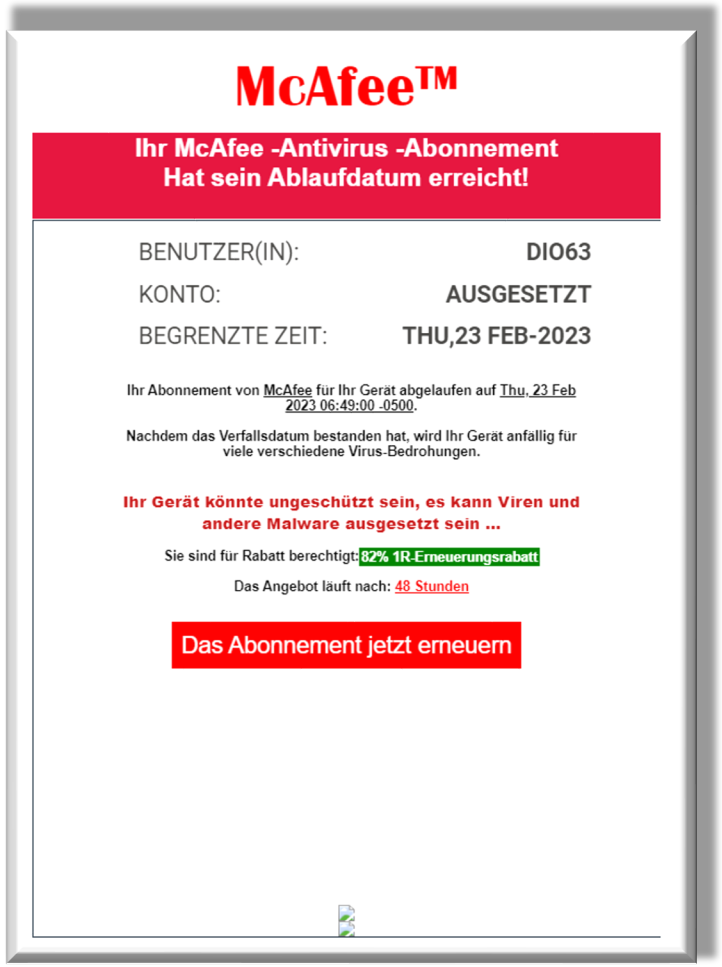
Vom Turnschuh zum Sneaker

Geschäftsmodell: IT-Sicherheitslösung als Datenspion

Die Gründung von IT-Sicherheitslösungs-Unternehmen, welche durch Hacker betrieben werden. Ziel ist es an Informationen und Daten heranzukommen. Auch ein langfristiger Ransomware-Angriff, mit entsprechendem hohen Lösegeld, ist ein Szenario, welches eine hohe Gefahr für Unternehmen bietet.

Ist die gefälschte Sicherheitssoftware (**Fakeware**) erst mal installiert, haben Hacker einfache Möglichkeiten das System auszuspielen und einen sehr gezielten Angriff vorzunehmen.

Was ist eine typische Fakeware?



Fakeware ist eine Softwareanwendung, die von Betrügern erstellt wurde, um Benutzer zu täuschen und ihnen Schaden zuzufügen. Diese Programme können vorgeben, legitime Anwendungen zu sein, aber in Wirklichkeit Malware, Viren oder andere schädliche Software enthalten. Benutzer können gefälschte Programme auf betrügerischen Websites oder durch Phishing-E-Mails herunterladen und installieren.

Hackerunterstützung durch KI?

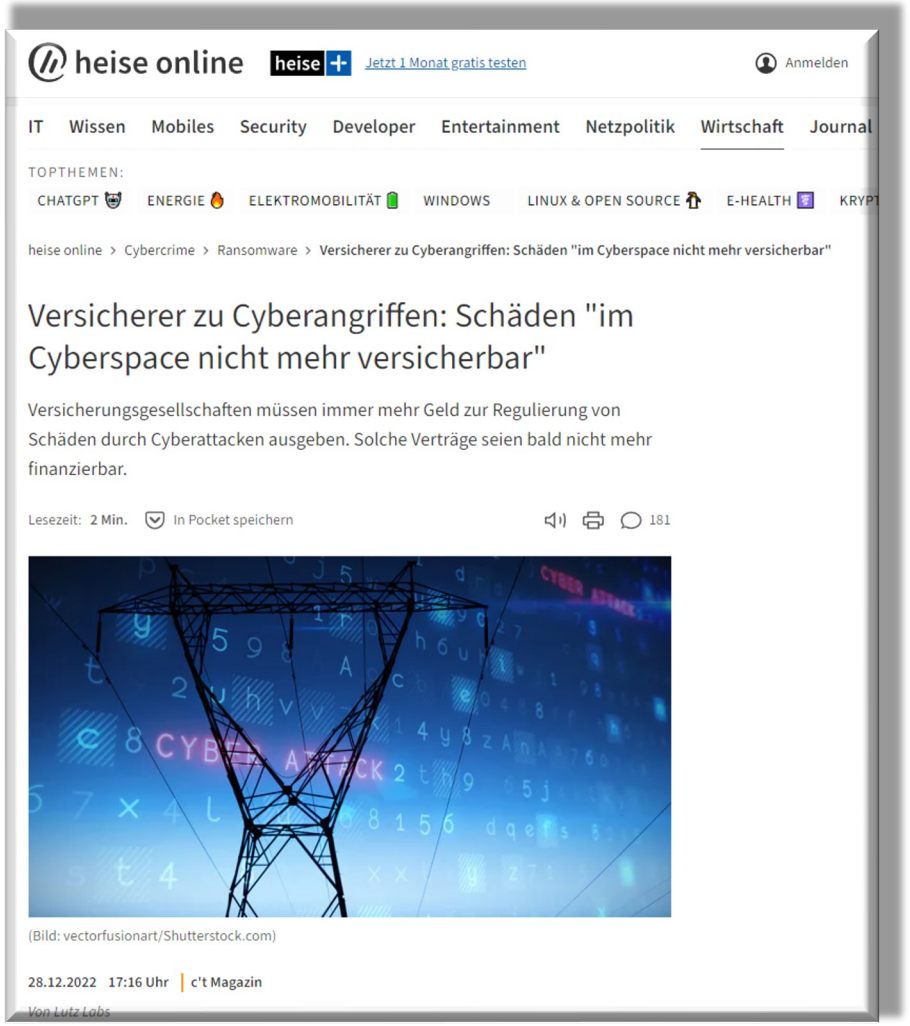
Als KI-Modell bin ich in der Lage, Informationen über die Bedrohungen und Risiken im Zusammenhang mit Künstlicher Intelligenz (KI) oder Artificial Intelligence (AI) zu geben. Die Entwicklung von KI und AI bringt zweifellos zahlreiche Vorteile mit sich, birgt jedoch auch potenzielle Risiken und Gefahren, insbesondere im Bereich der Cybersecurity.

Eine der Hauptgefahren besteht darin, **dass KI-Systeme von Angreifern manipuliert werden können**, um schädliche oder bösartige Handlungen auszuführen. Dies kann beispielsweise dazu führen, dass KI-gesteuerte Systeme in kritische Infrastrukturen eindringen, sensible Daten stehlen oder Cyberangriffe durchführen. Angreifer könnten auch versuchen, KI-Modelle zu täuschen, indem sie manipulierte Daten verwenden, um fehlerhafte oder unzuverlässige Ergebnisse zu erzeugen.

Ein weiteres Risiko besteht in der automatisierten und skalierbaren Natur von KI. Cyberkriminelle könnten KI-Algorithmen einsetzen, um Angriffe zu automatisieren und effektiver zu gestalten. Dies könnte beispielsweise zu einer **Zunahme von Phishing-Angriffen, Social-Engineering-Taktiken oder sogar gezielten Ransomware-Angriffen** führen.

Ein weiteres Problem ist das sogenannte "**Deepfake**", bei dem KI-Techniken verwendet werden, um gefälschte Inhalte zu erstellen, die kaum von echten Inhalten zu unterscheiden sind. Dies kann dazu führen, dass Fehlinformationen verbreitet werden, die das Vertrauen in die Authentizität von Informationen untergraben und zu ernsthaften Konsequenzen führen können.

Hilft eine Cyberversicherung?



Eine Cyberversicherung bietet spezielle Versicherungen an, die genau auf diese Szenarien abgestimmt sind. Jedoch muss immer **genau geprüft** werden, welche Anforderungen seitens der Versicherung, aber auch durch den Auftraggeber erfüllt werden müssen. Je nach Bedarf weicht auch der entsprechende Preis ab.

Einige Versicherer verlangen vorher ein **entsprechendes Konzept oder eine Dokumentation**. Denn es muss bereits im Vorfeld intensiv geprüft werden, was überhaupt versichert werden soll und wie hoch der Schaden ist, wenn es zu einem Angriff/Ausfall kommt. Ist es ein **altes und konzeptionell dünnes System**, wird die Beitragssumme entsprechend höher sein.

Mittlerweile lehnen Versicherungen Unternehmen mit schlechtem oder fehlendem Konzept ab.
Ein **durchdachtes IT-Security Konzept** kann die Kosten für eine Cyberversicherung folglich erheblich beeinflussen.

https://www.heise.de/news/Versicherungswirtschaft-ruft-bei-Cyberangriffen-nach-dem-Staat-7443841.html

Sind Sie vorbereitet?

https://www.it-daily.net/shortnews/nur-jedes-zweite-unternehmen-hat-einen-notfallplan-fuer-cyberattacken

„Bei der Abwehr eines Cyberangriffs ist **Zeit** eine ganz entscheidende Komponente. Alle Unternehmen sollten entsprechende Vorbereitungen treffen und einen klar geregelten Notfallplan aufstellen, um im Fall der Fälle nicht wertvolle Zeit zu verschwenden“, sagt Simran Mann, Referentin Sicherheitspolitik beim Bitkom.

Mann: *„Jedes Unternehmen kann Opfer von Cyberattacken werden, unabhängig von Branche und Größe. Ist die Firmen-IT erst einmal infiziert oder lahmgelegt, entstehen den Unternehmen hohe Kosten, die bis hin zu wochenlangen Produktionsausfällen gehen können.“*

Effektiv, weil simpel!

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

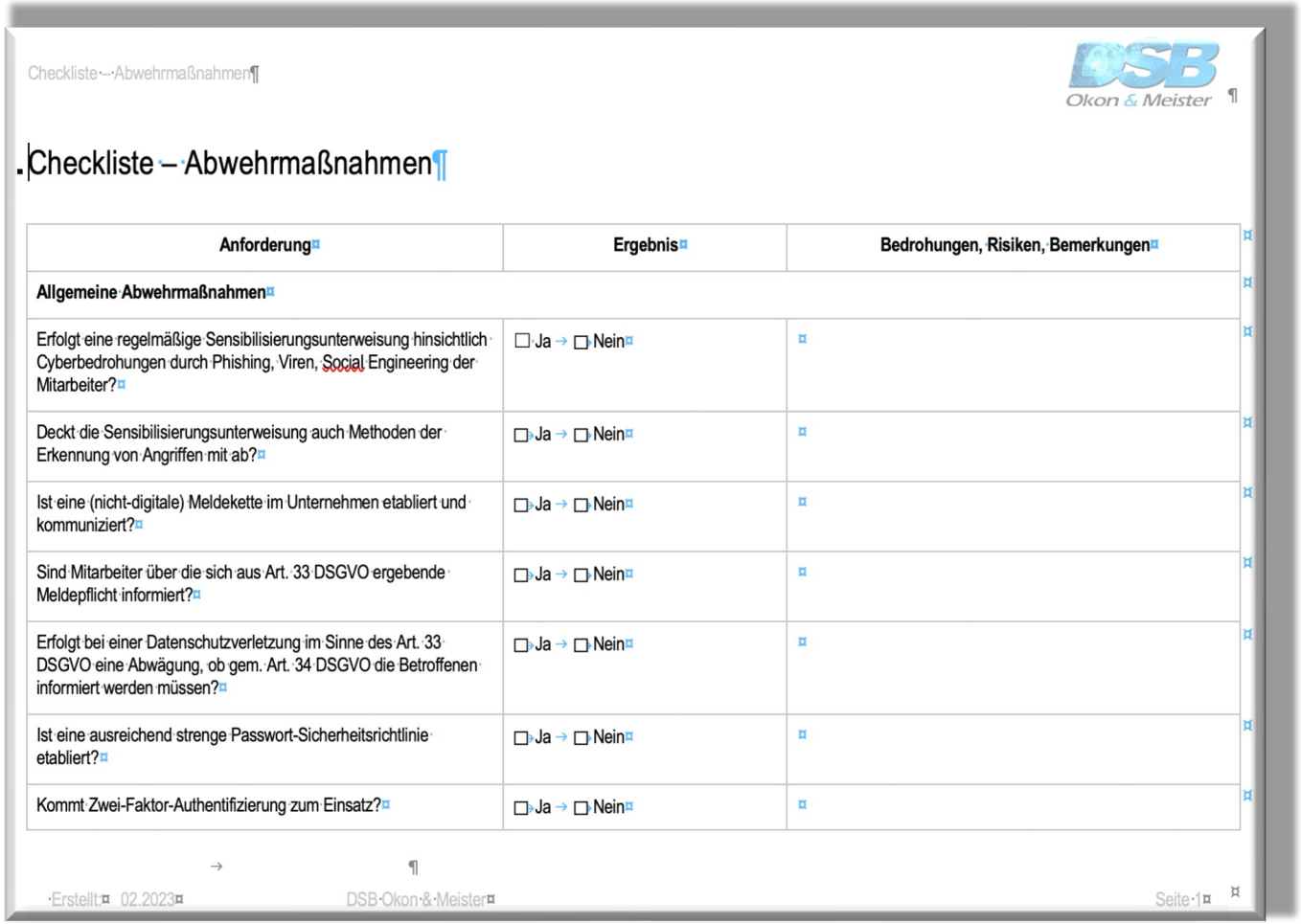
Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Wie beim Feuer-Notfallplan sollte es auch einen Notfallplan für IT geben. Dieser sollte ebenfalls an einem zentralen Ort in jedem Büro angebracht sein. Dieser IT -Notfallplan beinhaltet alle relevanten Informationen, um schnell kritischen Vorfällen zu begegnen.

Dieser Notfallplan kann auf der Website des Bundesamts für Sicherheit in der Informationstechnik (BSI) heruntergeladen und angepasst werden.

Lösungen?



Checkliste – Abwehrmaßnahmen

Checkliste – Abwehrmaßnahmen

Anforderung	Ergebnis	Bedrohungen, Risiken, Bemerkungen
Allgemeine Abwehrmaßnahmen		
Erfolgt eine regelmäßige Sensibilisierungsunterweisung hinsichtlich Cyberbedrohungen durch Phishing, Viren, Social Engineering der Mitarbeiter?	☐ Ja → ☐ Nein	
Deckt die Sensibilisierungsunterweisung auch Methoden der Erkennung von Angriffen mit ab?	☐ Ja → ☐ Nein	
Ist eine (nicht-digitale) Meldekette im Unternehmen etabliert und kommuniziert?	☐ Ja → ☐ Nein	
Sind Mitarbeiter über die sich aus Art. 33 DSGVO ergebende Meldepflicht informiert?	☐ Ja → ☐ Nein	
Erfolgt bei einer Datenschutzverletzung im Sinne des Art. 33 DSGVO eine Abwägung, ob gem. Art. 34 DSGVO die Betroffenen informiert werden müssen?	☐ Ja → ☐ Nein	
Ist eine ausreichend strenge Passwort-Sicherheitsrichtlinie etabliert?	☐ Ja → ☐ Nein	
Kommt Zwei-Faktor-Authentifizierung zum Einsatz?	☐ Ja → ☐ Nein	

Erstellt: 02.2023 DSB Okon & Meister Seite 1

Erfassen Sie Ihre Maßnahmen zur Abwehrfähigkeit von etwaigen Bedrohungen.

Erfassen Sie Ihre gesamte IT. Auch mobile Geräte, sowie Homeoffice und externe Dienstleister.

Durchleuchten Sie Ihre privaten Geräte und unterziehen Sie diese ebenfalls einer kritischen Prüfung.

Wie gut ist Ihr Backup-System?

Checkliste: Datensicherungs-/Back-up-Konzept		
Prüfaspekt	**Erläuterung**	**In Ordnung?**
Wer ist für Datensicherungsmaß - nahmen verantwortlich?	Klare Verantwortungszuordnungen an Personen sorgen für Verbindlichkeit. Akzeptieren Sie keine allgemeinen Festlegungen, wie beispielsweise die IT-Abteilung.	❑ja ❑nein
Sind Datenverarbeitungssysteme und Daten hinsichtlich ihrer Sicherungswürdigkeit bewertet?	Nicht alle Daten in Ihrem Unternehmen sind gleich sicherungswürdig. Manche Daten müssen hochverfügbar sein, sodass Sicherungen und Back-ups häufiger erfolgen müssen. Nur so ist gewährleistet, dass Datenverluste minimal sind.	❑ja ❑nein
Sind die getroffenen Sicherungsmaßnahmen nachvollziehbar, schlüssig und angemessen?	Hinterfragen Sie den kompletten Datensicherungsprozess. Lassen Sie sich an Systemen konkret erläutern, wie die Datensicherung abläuft. Prüfen Sie aus Ihrer Sicht, ob die Maßnahmen nicht nur schlüssig sind, sondern ob mit ihnen auch das Sicherungsziel erreicht werden kann.	❑ja ❑nein
Ist konkret festgelegt, wer wann auf welche Weise Datensicherungen vornimmt?	Möglicherweise gibt es in Ihrem Unternehmen auch nicht automatisierte Datensicherungen. Hier müssen Prozesse existieren, wie die zuständigen Mitarbeiter vorzugehen haben.	❑ja ❑nein
Ist die Durchführung von Datensicherungen dokumentiert?	Schon allein, um nachvollziehen zu können, ob eine Sicherungsmaßnahme erfolgreich war, bedarf es eines manuellen oder automatischen Berichts oder Protokolls.	❑ja ❑nein
Können mögliche Fehler bei der Datensicherung oder bei der Speicherung der zu sichernden Daten erkannt werden?	Lassen Sie sich erläutern, wie man sicherstellt, dass die Datensicherungsmaßnahmen erfolgreich durchgeführt worden sind. Wie erkennt man Fehler, Abbrüche oder unvollständige Sicherungsläufe?	❑ja ❑nein
Wurde die Rücksicherung von Daten in der Praxis erprobt?	Vielleicht klappt die Datensicherung reibungslos. Doch hat man auch schon mal in der Praxis ausprobiert, Daten wiederherzustellen? Wie ging man dabei vor?	❑ja ❑nein
Werden Datensicherungen sicher verwahrt, sprich, können Unbefugte keinen Zugriff nehmen?	Lassen Sie sich die Sicherheitsmaßnahmen erläutern. Doch nicht nur der unbefugte Zugriff ist ein Thema. Wie geht man mit anderen Risiken wie Feuer oder Wasser am Aufbewahrungsort um?	❑ja ❑nein
Werden Datensicherungsmedien vor der Rückgabe oder Entsorgung sicher gelöscht?	Festplatten und Sicherungsbänder halten nicht ewig. Wenn diese defekt sind oder entsorgt werden, muss sichergestellt sein, dass ein unbefugter Zugriff auf die Datensicherung ausgeschlossen ist.	❑ja ❑nein
Kann eine Rücksicherung	Bei einigen Unternehmen werden die Datensicherungen, aber auch die	

- Lassen Sie Ihr System regelmäßig testen.
- Spielen Sie einen Notfall durch
- Sicherung der Hardware?

Mobile Geräte

Es braucht Regeln, um die Sicherheit zu gewährleisten!

Mobile Geräte sind ganz besonders gefährdet. Sie werden am häufigsten verloren, gestohlen oder durch andere Personen (Familienmitglieder) unberechtigterweise genutzt.

- Welche Sicherheitsvorkehrungen wurden auf dem Handy getroffen?
- Wie/was ist geregelt, wenn es nicht mehr auffindbar ist?
- Gibt es eine Datensicherung?
- Wer ist zu benachrichtigen?
- Was könnte passieren, wenn ein unberechtigter Zugang bekommt?

Lösung: Eine zentrale Übersicht = Mobile Device Management (MDM)

Brauche ich einen Virenschutz auf dem Android?

Jeder Schutz ist besser als gar kein Schutz!

- Der beste Virenschutz ist immer der User
- Jedes Mobiltelefon ist angreifbar!
- Es gibt weniger schädliche Software für iPhone als für Android
- Android steht mit seinem Betriebssystem an der Spitze aller angreifbaren Betriebssysteme für Mobilgeräte
- Im Gegensatz zu Apple wird die Installation von Hard- und Software nicht überwacht
- Nutzen Sie primär den Google Play Store für Apps
- Adware (meistens Werbung) überliefert oft unbemerkt Nutzerdaten und dienen als Einfallstor für Angriffe
- Einstellungen in Google sind hier oft die Ursache für übermäßig viel Werbung.
- Drittsoftware auf einem Android-Betriebssystem ist mitunter sinnvoll

Virenschutz auf dem iPhone?

Jeder Schutz ist besser als gar kein Schutz!

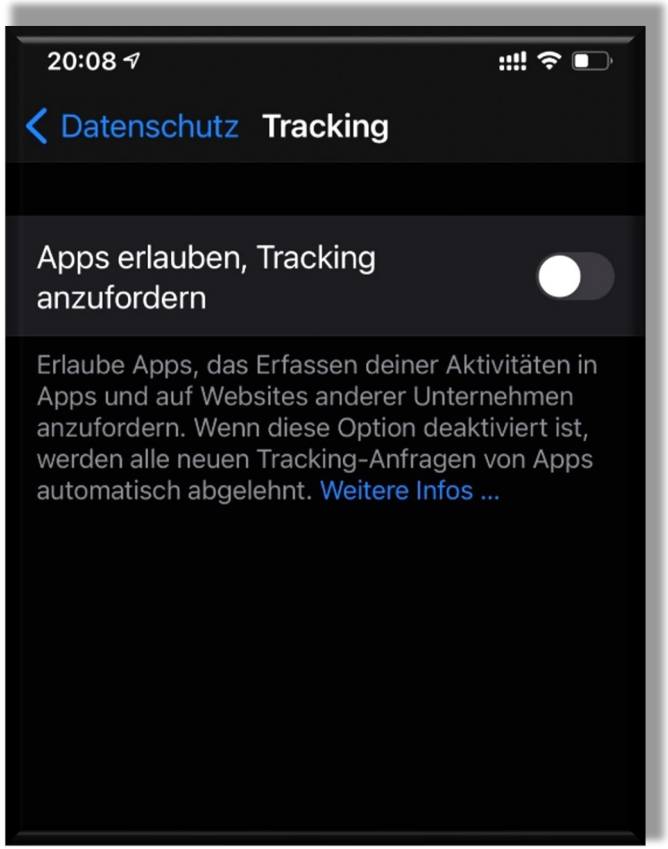
- Der beste Virenschutz ist immer der User!
- Jedes Mobiltelefon ist angreifbar!
- Es gibt weniger schädliche Software für iPhone als für Android
- Das Sandbox-System bietet hohe Sicherheit
- iPhone ist nicht unverwundbar (Virus „TinyV“ durch Jailbreak)
- NSA Zugang zu iPhones über Tool „Pegasus“ (Jailbreak)
- Spiel „Cydia“ durch Jailbreak Trojaner im Gepäck
- Apple überwacht, welche Hard- und Software verwendet werden kann
- Die Bedrohung für Mac-Systeme stieg im Jahr 2019 um mehr als 400 %
- Adware (meistens Werbung) überliefert oft unbemerkt Nutzerdaten und dienen als Einfallstor für Angriffe
- Drittsoftware ist nicht zwingend notwendig aber manchmal auch sinnvoll
- Achtung manche Apps zur Sicherheit transportieren oft mehr Daten, als sie schützen sollen.

Mobile Geräte mit Bordmitteln schützen

iPhone mit Bordmitteln schützen

Zwar bietet Apple seit jeher eine relativ hohe Verschlüsselung, jedoch wurde auch diese Verschlüsselung mittlerweile geknackt. Der „FBI-Fall“ aus 2016 zeigte jedoch, wie stark und sicher die „hauseigene“ Verschlüsselung der Geräte mit iOS-Betriebssystem ist. Nicht jede Verschlüsselungs-Software für iPhone ist sinnvoll. Hier sollten Benutzer vergleichen.

Aber andere Sicherheitseinstellungen sollten zwingend aktiviert werden!!

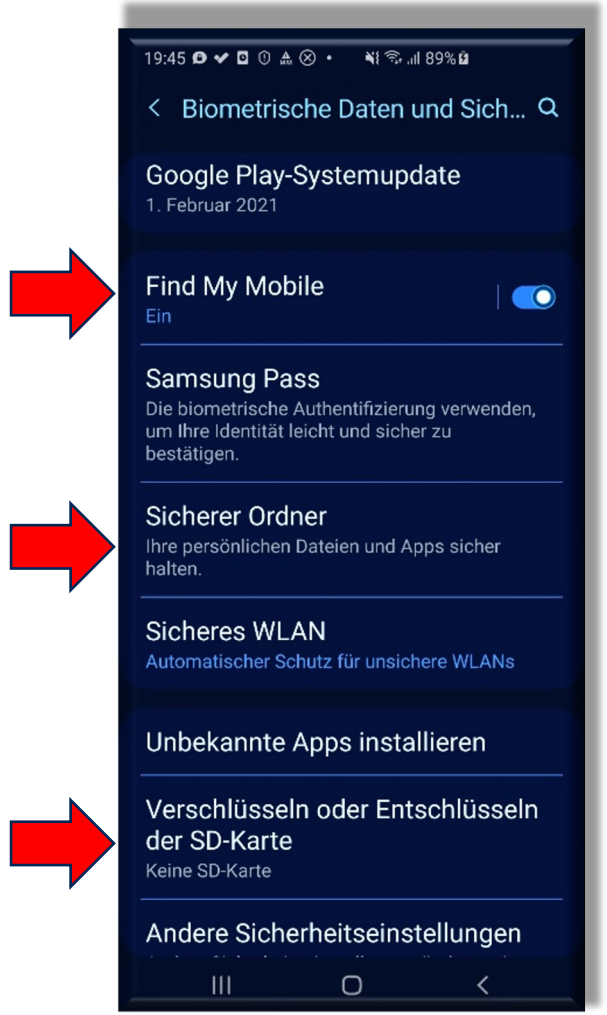


Mobile Geräte mit Bordmitteln schützen

Android mit Bordmitteln schützen

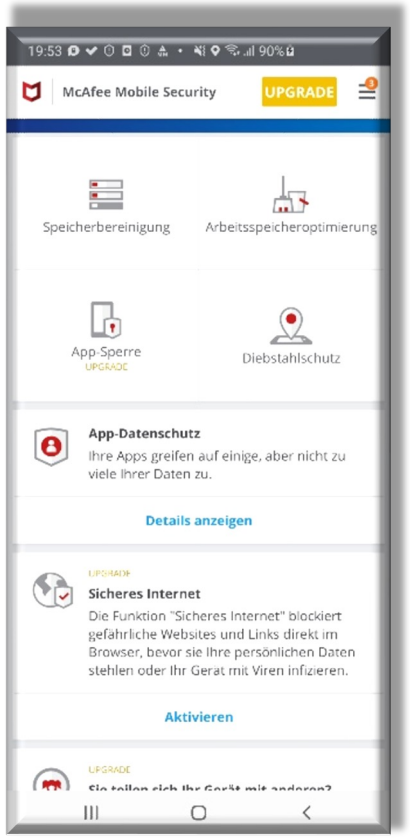
Das Betriebssystem „Android“ steht an der Spitze der „gehackten“ Betriebssysteme für Mobilgeräte. Daher sind zwingend Einstellungen im Betriebssystem vorzunehmen.

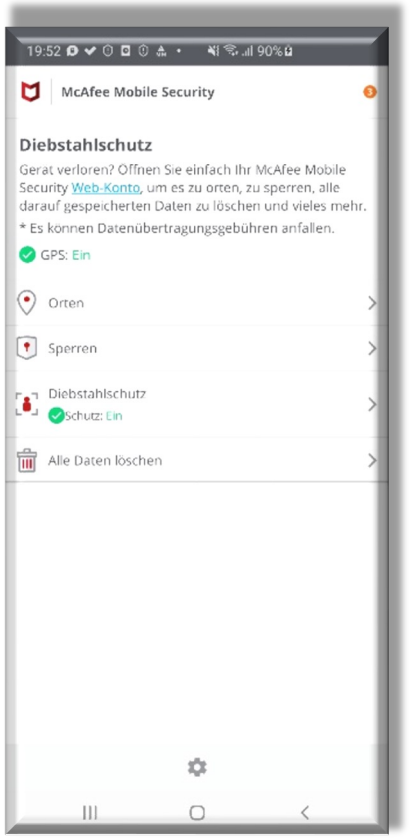
- **„Find My Mobile“** ein verlorenes Gerät kann aus der Ferne lokalisiert, gesperrt und gelöscht werden,
- **„Sicherer Ordner“** Daten können verschlüsselt gespeichert werden,
- **„Verschlüsseln“** beispielsweise die externe „SD-Karte“ kann mit Bordmitteln verschlüsselt werden!

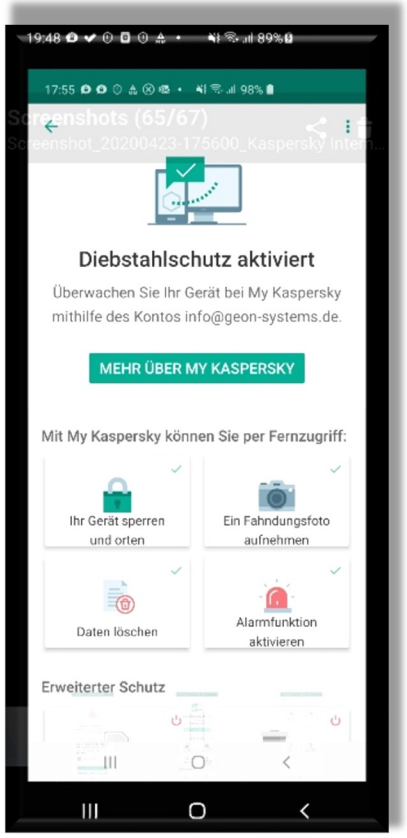


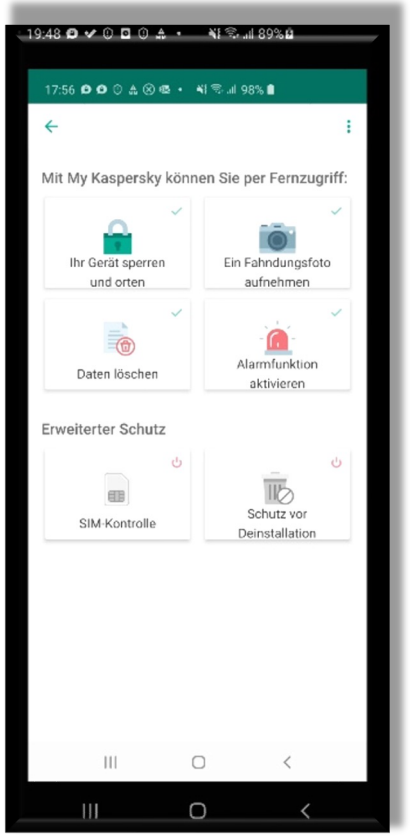
Mobile Geräte mit spezieller Software schützen

Android über Drittthersteller schützen









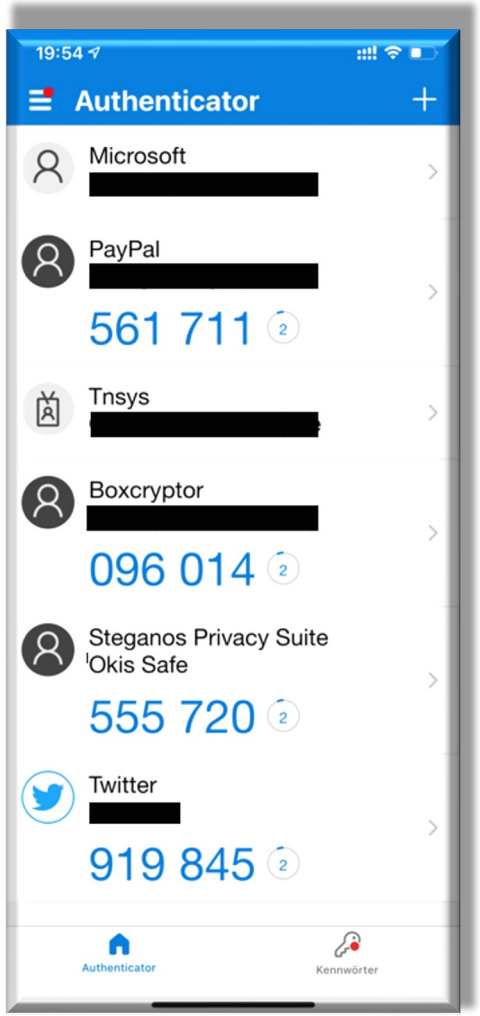
Zusätzliche Sicherheit mit speziellen Tools

Zweifache Authentifizierung

Wenn möglich sollte immer die **„2-Faktor-Authentifizierung“** aktiviert werden. Nur so lässt sich beispielsweise überprüfen, ob ein Fremdzugriff stattfindet.

Nachteil: der Anmeldevorgang dauert länger. Das ist häufig die Ursache für eine Deaktivierung dieses Sicherheitsfeatures. Es ist zwingend anzuraten dieses Anmeldeverfahren beizubehalten.

Beispiel: Authenticator-App



Modus „Verloren“

Wofür ist dieser sinnvoll?

- Individuelle Meldung können auf dem Home-Bildschirm angezeigt werden.
- Während das Gerät zwar immer noch in Betrieb ist, werden Nachrichten, Mitteilungen Kalendereinträge nicht auf dem Home Bildschirm angezeigt. Auch Töne werden nicht gespielt.
- Anrufe (auch FaceTime) sind möglich
- Sämtliche Einstellungen zu Kreditkarten, die für Apple Pay auf dem iPhone hinterlegt wurden werden deaktiviert. Apple Pay selbst ist auch gänzlich deaktiviert.
- Die gesperrten Karten lassen sich wiederverwenden, sobald das Gerät ordnungsgemäß entsperrt wurde.
- Der Modus „Verloren“ ist auch für Geräte von etwaigen Familienmitgliedern aktivierbar

Modus „Löschen“

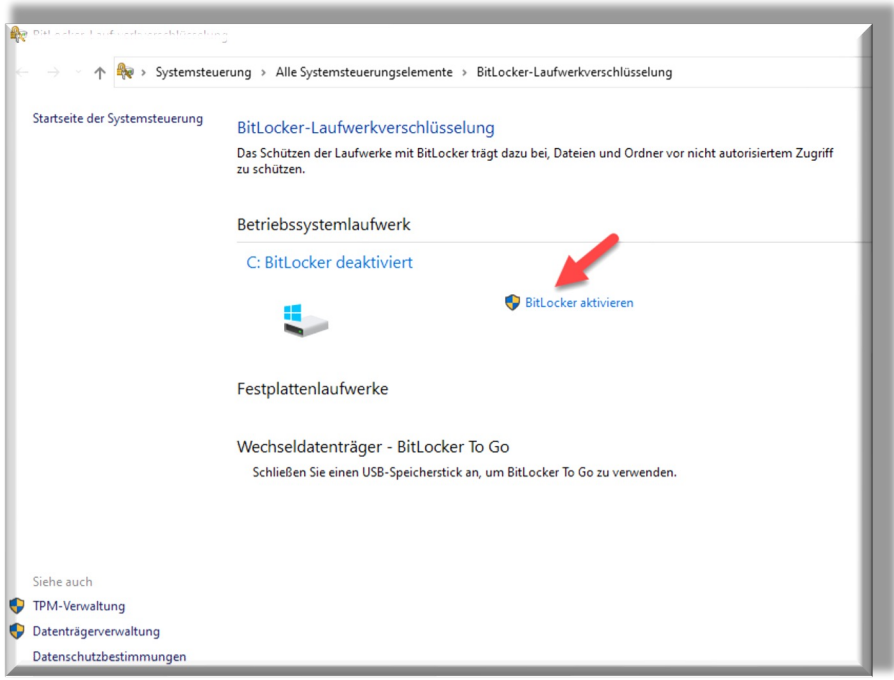
Wofür ist dieser sinnvoll?

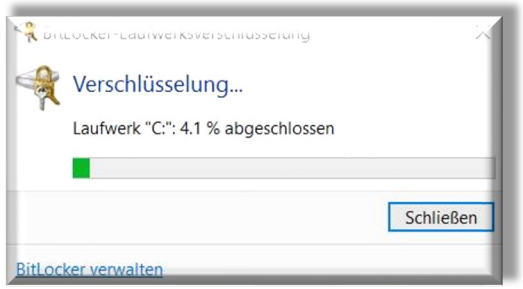
- Alle Daten werden vom Gerät entfernt. Dies allerdings nur solange es eingeschaltet und erreichbar ist.
- Das iCloud-Backup sollte aktiviert sein. Somit ist eine Wiederherstellung unproblematisch.
- Die SIM-Karte sollte beim Provider gesperrt werden. Hierzu ist es sinnvoll sich die Sim-Karte-Nummer zu notieren.
- Ein verlorenes iPhone ist relativ schwer durch einen unberechtigten Nutzer zu betreiben. Daher sollte das Passwort (PIN) mindestens sechsstellig sein.
- Sie sollten unbedingt vorher die SN-Nr. sowie die IMEI und ICCID notiert haben.

Mobile Geräte mit Bordmitteln schützen

Laptops mit Bordmitteln schützen

Gerade Laptops sind besonders gefährdet. Häufig sind Diebstahl und Verlust die häufigsten Ursachen für Datenpannen. Seit der Einführung von Windows 10 wird auch ein eigenes Verschlüsselungssystem (**Bitlocker**) seitens Microsoft mitgeliefert. Dieses sehr effektive Tool sollte genutzt und aktiviert werden. Gerade kleinere Unternehmen mit weniger Budget sollten diese Methode zwingend einführen und umsetzen.





Ihre Aufgaben

Darauf müssen Sie stets achten

- Firmen-Laptop oder privater Computer (BYOD-Regelung)
- Nutzung von Papierakten und Dokumenten zu Hause?
- Regelung zur Abwesenheit?
- Bildschirmsperre und Passwortregelung?
- Mobile Medien (Chipkarten, USB-Sticks, etc.)
- Regelung zur Mitnahme von mobilen Geräten ins Ausland/Urlaub
- Regelung zum Eingriff durch das Unternehmen (Fernwartung)
- Sichere Verbindung zum Unternehmen (VPN)
- Regelung zu Virenschutz und Sicherheitsvorkehrungen an privaten Gerä
- Schriftliche Verpflichtung zur Einhaltung der Verhaltensregeln und Sicherheitsmaßnahmen

Ihre Aufgaben

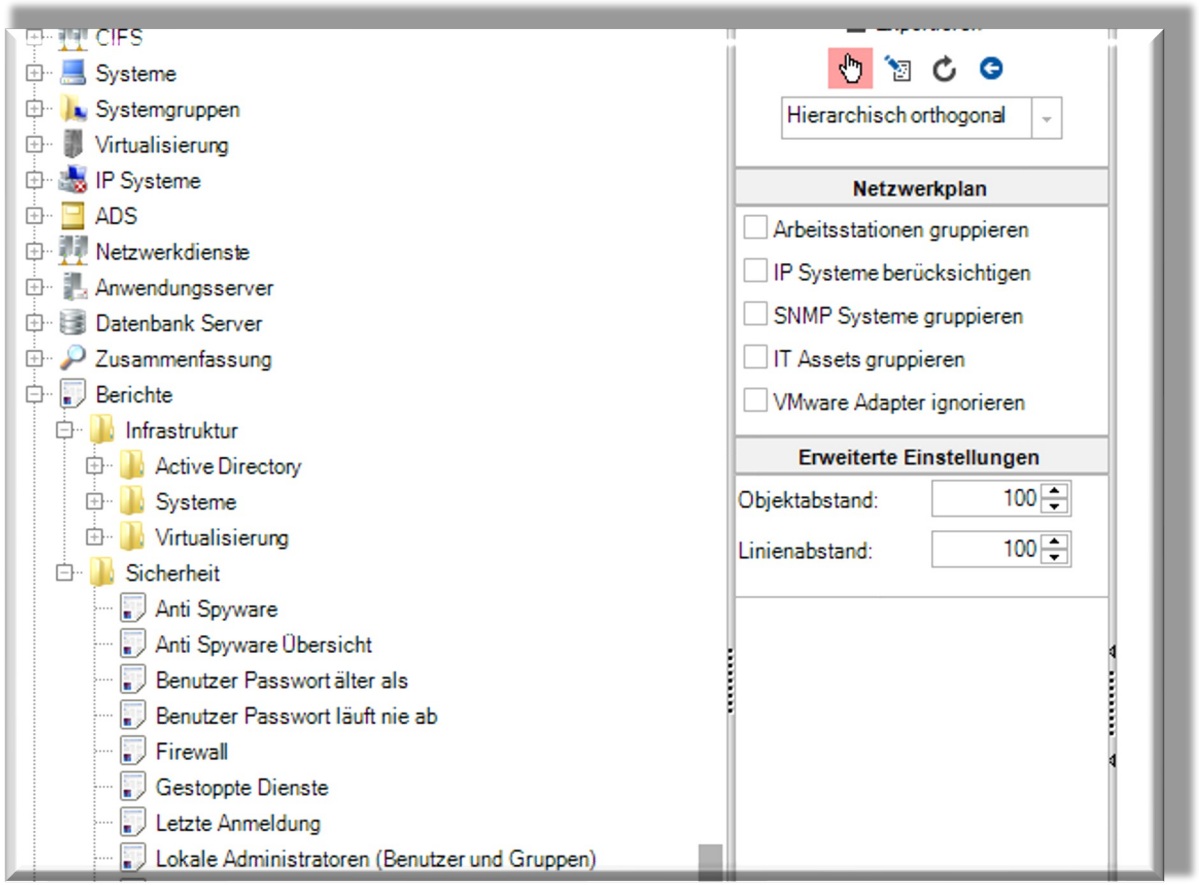
Darauf müssen Sie stets achten

- Starke Passwörter
- Zwei-Faktor-Authentifizierung (2FA)
- Software-Updates
- E-Mail- und Nachrichtensicherheit
- Firewall und Antivirenprogramm
- WLAN-Sicherheit
- Vorsicht im öffentlichen WLAN
- Schutz persönlicher Daten
- Regelmäßige Backups
- Bildung und Aufklärung
- Sichere Online-Transaktionen
- Einschränkung der Nutzung von sozialen Medien
- Datenverschlüsselung
- Physischer Schutz von Geräten
- Verwendung eines Werbeblockers
- Virtual Private Network (VPN) im Ausland auch nur zum Surfen
- Deaktivierung ungenutzter Services und Ports
- Begrenzung der Anzahl der Anmeldeversuche
- Hardware-Firewall
- Kontenüberwachung auf ungewöhnliche Aktivitäten
- Datensicherheitswerkzeuge
- Professionelle Hilfe in Anspruch nehmen

Ihre Aufgabe: Durchblick ist Pflicht

Durchleuchten Sie Ihre gesamte EDV-Struktur

- Notieren Sie Lizenzen für Programme und Betriebssysteme
- Notieren Sie alle Programme, die Sie auf dem PC installiert haben
- Überprüfen Sie ob Programme eine Datensicherung anbieten (DATEV)
- Haben Sie einen Überblick über Ihre Passwörter (Passwort-Manager)
- Wie viele Datensicherungen gibt es? (Generationsprinzip)



Geben Sie ihm keine Chance

Reagieren Sie frühzeitig!