WOHIN ESKALIERT RANSOMWARE? – EIN AKTUELLES LAGEBILD ZU RANSOMWARE

Ransomware basiert auf der sogenannten Locker-Schadsoftware. Es handelt sich dabei um eine unerwünschte Schadsoftware, die die Dateien auf dem betroffenen Computer verschlüsselt und den Schlüssel erst durch eine Lösegeldzahlung an Kriminelle wieder freigibt. Manche Experten bezeichnen Ransomware mittlerweile als die größte Bedrohung im Internet und die USA haben unlängst Ransomware-Angriffe auf Betreiber von kritischer Infrastruktur mit einem terroristischen Anschlag gleichgestellt.

Seit März 2020 haben sich Cyberangriffe mit Ransomware – die *Pandemie in der Pandemie* - so rasant weiterentwickelt, dass es für fachlich Außenstehende fast unmöglich geworden ist, hier noch thematisch mitzuhalten. Wir wollen unseren Leserinnen und Lesern daher ein aktuelles Lagebild liefern, Klarheit schaffen und zeigen, wie sich das Internet in den letzten Jahren über ständige Eskalationen durch Ransomware-Gruppierungen zur größten Schutzgeldzone der Welt entwickelte und so die fortschreitende Digitalisierung in den G20-Industrienationen bedroht.

Die fünf wichtigsten Erkenntnisse mit Stand August 2021 fassen wir für Sie kompakt zusammen.

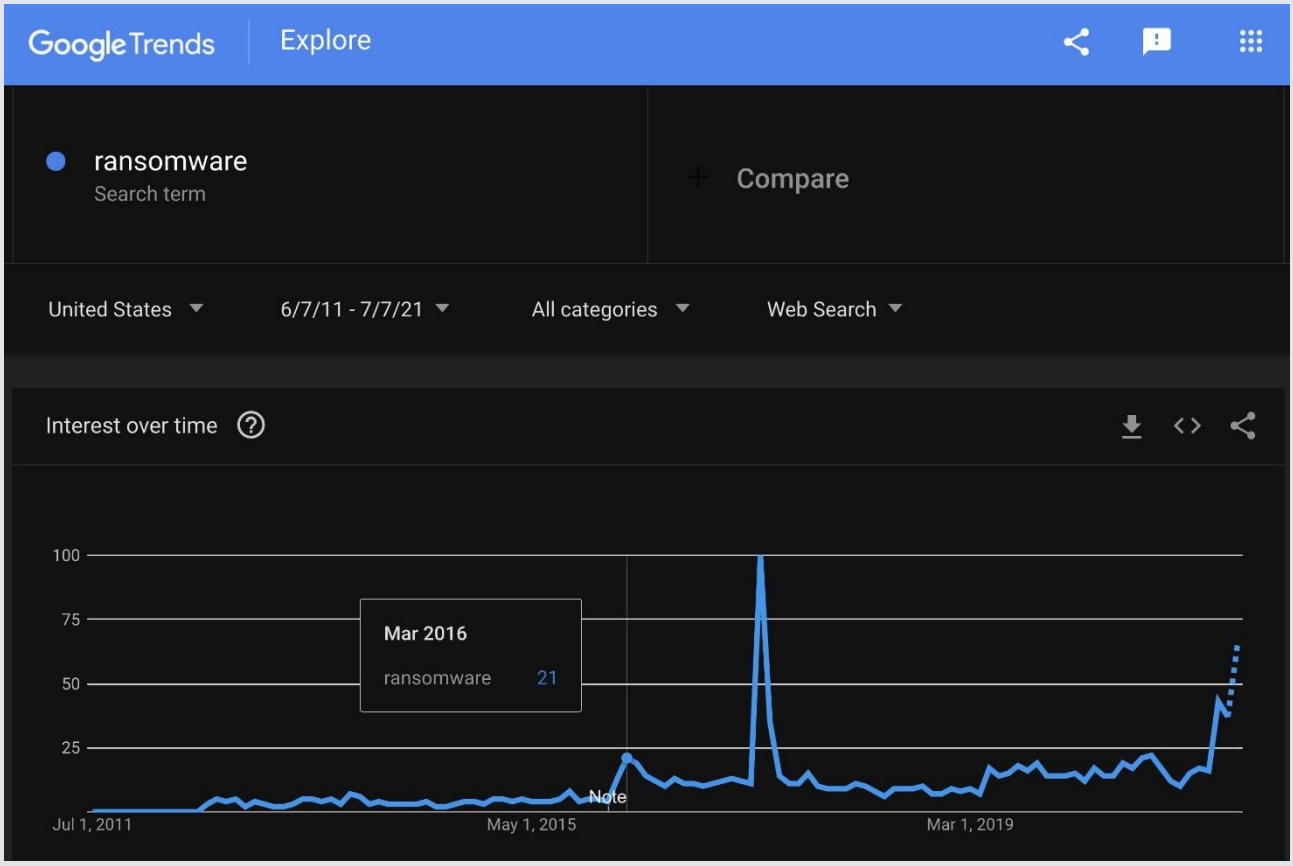
Die Quintessenz: Es geht nur um das Lösegeld!

Zahlen oder nicht zahlen bei Ransomware? Viele Unternehmen stellen sich mittlerweile diese Frage. Die Erpressungsschreiben von Ransomware an Betroffene mögen vielleicht eine unfreiwillige, aber eine „notwendige Dienstleistung“ suggerieren. Jedoch sind die darin gegebenen Versprechen, wie etwa gestohlene Dateien zu löschen oder deren Kopien im Internet zu entfernen, bis dato höchst unzuverlässig gewesen. Viele Betroffene sprechen Wochen später von weiteren Angriffen mit anderer Ransomware, quasi einer „Nacherpressung“ mit Datenlecks, oder von defekten Dateien nach der Entschlüsselung.

Das Versprechen von kriminellen und namenlosen Erpressern, hier ein Service anzubieten, selektiv Organisationen von Angriffen auszuklammern oder Daten garantiert nach Erhalt von Lösegeld zu löschen, wurde bereits mehrfach gebrochen. Konkret wurden 80% der Opfer, die bereits einmal Lösegeld für Ransomware bezahlten, gemäß einer Befragung[1] von über 1.200 Cybersicherheitsexperten auch ein zweites Mal erpresst.

Blicken wir ein paar Jahre zurück: Im Mai 2017 wurde Ransomware durch WannaCry öffentlich medial bekannt, auch wenn Fachleuten diese Art von Computer-Schädling bereits seit 1989 bekannt war und damals noch irgendwo zwischen „Computer Viruses, Worms, Data Diddlers, Killer Programs“[2] angesiedelt war. Bei WannaCry wurden stolze USD 800 Lösegeld in Bitcoin verlangt, heute im Jahr 2021 gehen die geforderten Lösegelder bereits in Millionenhöhe und auf zweistellige Millionenbeträge zu. Eine historische Trendanalyse vom Google-Suchbegriff „Ransomware“ zeigt einen ersten deutlichen Anstieg im März 2016, als die Ransomware Petya aktiv wurde:

[1] vgl. https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report
[2] McAfee, John & Haynes, Colin: Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System. What They Are, how They Work, and how to Defend Your PC, Mac, Or Mainframe. St. Martin's Press, 1989.



Die Ransomware Petya – nicht zu verwechseln mit NotPetya – wurde erstmals im März 2016 aktiv.
Idee zur Analyse und Screenshot stammen von Johns Hopkins Professor Thomas Rid[3].

Mit Stand Juni 2021 kennen Sicherheitsforscher bereits über 38 Varianten von Ransomware, die neben der Verschlüsselung sensible personenbezogene Daten im Internet zwecks Erpressung von Unternehmen veröffentlichen:

- #ElonMusKnow
- AKO
- Astro Team
- Avaddon
- Black Shadow
- Clop/TA505/MINEBRIDGE
- Conti
- Cuba Ransomware (Hancitor)
- Dark Leak Market
- DarkSide
- Dopplepaymer/Doppelpaymer
- Egregor
- Everest
- Evil Corp: WastedLocker/Hades/Phoenix/Babuk/PayloadBin
- File Leaks
- Galaxy
- Gandcrab
- Grief
- Hive
- LockBit
- Lorenz
- LV Blog
- Marketo
- Maze Ransomware
- Mount Locker
- N3tw0rm
- Nefilim/Nephilim/NEMTY
- NetWalker/Mailto
- Noname
- Pay2Key
- ProLock
- Prometheus
- Pysa/Mespinoza
- Ragnarok/Ragnar Locker
- RansomEXX
- Ranzy Locker/ThunderX/MedusaReborn
- REvil/Sodinokibi / GOLD SOUTHFIELD
- SEKHMET
- SunCrypt
- Team Snatch
- Vice Society
- XING LOCKER

Von BDO Consulting über die Jahre beobachtete Ransomware. Einige Gruppierungen sind bereits wieder offline (inaktiv).

[3] vgl. https://twitter.com/RidT

Daneben gibt es noch unzählige Varianten, die ausschließlich verschlüsseln (z.B. Ryuk, JSWorm), und Untergrund-Marktplätze, die mit Datenlecks anderer Ransomware erpressen oder diese versteigern.

Cyberkriminelle nutzen dabei alle erdenklichen Tricks, um ihre Opfer zu einer Bezahlung zu motivieren: Backup vorhanden? *Datenleck oder Verhinderung von Diensten.* Desinteresse eines Börsennotierten Konzerns an einer Erpressung? *„Short-Seller" und Spekulanten mit Insider-Informationen versorgen, damit diese den Aktienkurs manipulieren.* Keine Kontaktmöglichkeiten? *Kundinnen und Kunden des betroffenen Unternehmens über Call-Center in Indien anrufen lassen.* Probleme in Bitcoin im Dark Web zu zahlen? *Helpdesk mit TeamViewer-Support anbieten.*

Mit solchen Eskalationsschritten gelingt es Cyberkriminellen seit 2017, ihren Profit um das 1.000-fache und darüber hinaus zu steigern. Natürlich spielt der Faktor einer bequemen Erpressung mit Kryptowährungen eine große Rolle, was seit wenigen Jahren an die Popularität und den rasanten Kursanstieg von Bitcoin gekoppelt ist. Dies lässt sich nicht vom Tisch wischen, auch wenn Bitcoin an Ransomware genauso „mitschuldig" ist wie Bargeld am Drogenkonsum. Anstatt der polemischen Forderung alle Kryptobörsen mit amerikanischen Kundinnen und Kunden[4] zwangsweise zu regulieren, schlagen Experten wie Bruce Schneier eine sogenannte „Disruption"[5] vor, also die gezielte Unterbrechung von Offshore-Kryptobörsen, über die Kriminelle ihre illegalen Profite aus Ransomware und Erpressung bequem und leicht reinwaschen können.

Aktivismus, kriminell oder staatlich motiviert?

Wer für Entwicklung und Verbreitung von welcher Ransomware zuständig ist, lässt sich aktuell nicht leicht beantworten. Diese kriminellen Gruppierungen arbeiten im Untergrund und rekrutieren „Freelancer" über Grenzen und Zeitzonen hinweg. Pseudonamen, namensähnliche Varianten und Überlappungen im Quellcode machen eine Identifizierung und Zuordnung extrem schwierig oder unmöglich. Gerüchten zufolge soll Nordkorea bereits vor Jahren den Quellcode für die Hermes-Ransomware in russischsprachigen Untergrundmärkten verkauft haben und Hacker aus dem Iran offerierten zeitweise Zugangsdaten zu kompromittierten Unternehmensnetzwerken aus dem Westen. Mittlerweile stehlen konkurrierende Kriminelle die Ransomware von anderen Gruppierungen und adaptieren sie für eigene Zwecke.

Es gibt ebenso Beispiele für Ransomware zwecks politischen Aktivismus, wie von der mit China assoziierten Gruppe WINNTI gegen taiwanesische Unternehmen, die Gruppe Cuba aus Lateinamerika oder Pay2Key aus dem Nahen Osten – letztere erpresst bewusst nur israelische Unternehmen. Bei Emotet und Clop spekulierten Experten zu deren Ursprüngen im Gebiet der russischen Föderation (CIS-Staaten), erste Festnahmen erfolgten jedoch in Bulgarien (Emotet) und der Ukraine (Clop). Die Festgenommenen von Clop sollen anderen Kriminellen als illegale Geldboten (Crypto-Money-Mules) geholfen haben, über USD 500 Millionen Profit aus Ransomware wieder in legale Kanäle einzuschleusen. Dies würde bereits den kriminellen „Umsatz" von über USD 380 Millionen für Ransomware im Jahre 2020 bei weitem übertreffen. Clop hat kurz nach der Festnahme weitere Opfer im Dark Web veröffentlicht und ist weiterhin aktiv.

Scherzhaft fragen manche Zeitgenossen, darunter überraschenderweise auch Experten, warum es eigentlich keine Ransomware „Made in America" gibt, die beispielsweise russische Leitbetriebe lahmlegt. Die Antwort wird bei einer geopolitischen Betrachtung von Cyberkriminalität, -sabotage und -spionage schnell klar: Illegale Geldbeschaffung über digitale Wege – also Angriffe im Internet auf Kryptobörsen, Cyberattacken auf Banken, Business E-mail Compromise, Ransomware, Cryptojacking, usw. – erfolgt hauptsächlich aus Ländern, die geopolitisch von der internationalen Staatengemeinschaft sanktioniert oder wirtschaftlich stark benachteiligt werden. Trotzdem darf und kann Aktivismus in Form einer

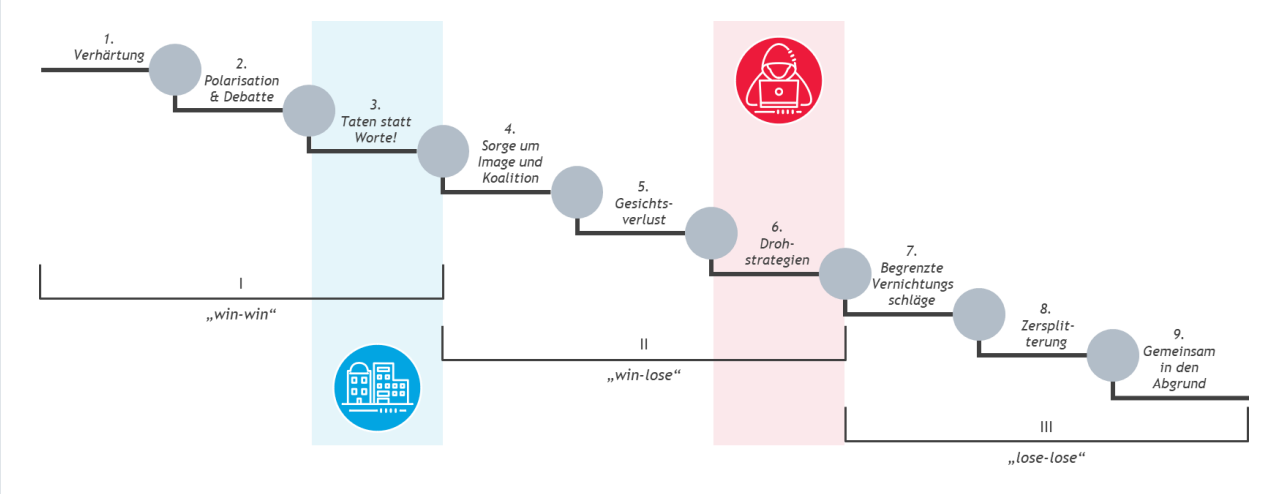
[4] *„Cryptocurrency firms serving U.S. customers are supposed to be subject to the same anti-money-laundering requirements as traditional financial institutions, but more can be done."* Vgl. https://www.wsj.com/articles/ban-cryptocurrency-to-fight-ransomware-11621962831
[5] vgl. https://www.schneier.com/blog/archives/2021/07/disrupting-ransomware-by-disrupting-bitcoin.html

vermeintlichen Vermögensumverteilung nicht als Entschuldigungsversuch gesehen werden, denn Cyberkriminelle geben genauso gerne mit Sportautos, Luxusartikeln und dicken Bitcoin Wallets an.

Das nordkoreanische Regime finanziert mutmaßlich Teile seines nuklearen Waffenprogramms über Einnahmen aus Cyberkriminalität, wozu ebenfalls WannaCry gehören soll. Und wer Ransomware als späte Rache für amerikanische Cyberspionage betrachtet, der irrt ebenfalls, obwohl bereits geheime Software des Nachrichtendienstes der Vereinigten Staaten für die Verbreitung von Ransomware als technische Grundlage diente.

Die Eskalationsstufen bei Ransomware

Der österreichische Ökonom, Organisationsberater und Konfliktforscher Prof. DDr. Friedrich Glasl hat ein Eskalationsstufenmodell entwickelt, bei dem sich zwei Akteure in Schritten bewegen und das sich hervorragend auf Konflikte im Cyberspace (Internet) umlegen lässt, wenn man die kriminellen Cyberangreifer und deren Opfer als jeweils fiktive Entität (ein Angreifer in Rot, ein Opfer in Blau) in einem Konflikt betrachtet:



Adaptierung von Phasenmodell der Eskalation nach Friedrich Glasl (1980)[6]

Kriminelle sind rot, betroffene Unternehmen sind blau dargestellt.

Im Modell von Friedrich Glasl gibt es drei Phasen der Gewinner und Verlierer, wobei sich bei Konfliktstufen 4 bis 6 in der mittleren Phase „win-lose“ sowohl ein Gewinner als auch ein Verlierer befinden. Würde bei Ransomware die Stufe 7 „Limited Destruction“ erreicht werden, nämlich der begrenzte Vernichtungsschlag als Auslöser von Cyberkrieg (Warfare) zwischen zwei Staaten, dann gäbe es auf beiden Seiten des Konfliktes nur Verlierer:

[6] vgl. https://de.wikipedia.org/wiki/Konflikteskalation_nach_Friedrich_Glasl

Eskalationsschritte von Cyberkriminellen	Konflikteskalation: Stufen nach Friedrich Glasl	Original/Englisch	Erklärung/Übersetzung	Hinweise
1	**1 - Verhärtung, 2 - Debatte, Polemik**	**Encrypt internal files**	Die Dateien eines Anwenders werden über Schadsoftware von Unbekannt verschlüsselt (Systemdienste und Anwendungen sind ausgenommen)	1989: „AIDS Trojan“ durch Joseph Popp (PC Cyborg Corporation)
2	**3 - Taten statt Worte**	**Demand a ransom in Crypto**	Lösegeld wird in Kryptowährungen (statt Pre-Paid-Karten oder Western Union) verlangt	Dezember 2013: CryptoLocker 2.0
3		**Steal the files**	Vertrauliche Daten werden vor der Verschlüsselung auf einen externen Server kopiert und von Kriminellen zwecks Erkundung analysiert	Seit ca. 2019
4		**Leak the files (a/k/a „Double extortion“)**	Vertrauliche Daten der Opfer (Unternehmen) werden im Dark Web veröffentlicht	Seit Mai 2019 („Team Snatch")
5	**4 - Koalitionen, Images**	**Affiliates**	Ransomware-Gruppierungen starten eine Aufgabenverteilung an freiwillige IT-Experten, die wie externe Mitarbeitende bezahlt werden	
6	**5 - Gesichtsverlust**	**Press release**	Die Veröffentlichung von vertraulichen Daten wird medienwirksam angekündigt; die IT-Abteilung bzw. das Management der Ransomware-Opfer wird öffentlich kritisiert/gedemütigt (Kunde statt Opfer; Audit statt Erpressung usw.)	
7	**6 - Drohstrategien**	**DDoS**	Nicht zahlungswillige Opfer (Unternehmen) werden zusätzlich mit einer Verhinderung von Diensten erpresst	
8		**Call center**	Ein Call-Center telefoniert mit dem Opfer (Unternehmen) oder Kundinnen und Kunden eines betroffenen Unternehmens	
9		**Auction**	Vertrauliche Daten werden zuerst an Interessenten versteigert	Seit ca. 2021
10		**Short-sellers; rogue traders**	Aktienhändler werden eingeladen, auf fallende Kurse eines betroffenen Unternehmens zu spekulieren	
11		**Disclose private facts (a/k/a „Revenge porn“)**	Persönliche, vertrauliche und sensible Daten von Führungskräften (z.B. CEO) werden medienwirksam verbreitet	Stand Juni 2021
12		**Send stolen files to competitors**	Daten werden gezielt an den Mitbewerb eines Opfers (Unternehmens) versendet	
13		**Attack on cyber-insurance**	Gezielte Angriffe auf Kunden mit einer Cyber-Ransom-Versicherung oder auf Versicherungskonzerne	
14		**Supply-chain-compromise**	**Ransomware wird in Software von bekannten Herstellern versteckt und so an die Endkunden „ausgeliefert" bzw. automatisch weiter verteilt [bis dato nicht eingetreten]**	**Stand Juli 2021**
15		**Artificial Intelligence**	**Ransomware versteckt sich mithilfe künstlicher Intelligenz [Experten-Vorhersage]**	
…	**7 - Begrenzte Vernichtung(sschläge)**		**Erpressung der gesamten Volkswirtschaft über gezielte Ransomware-Angriffe auf kritische Infrastruktur und militärische Einrichtungen eines Staates [von US-Präsidenten Joseph Biden angesprochen]**	

Ist Stufe 7 nach Glasl schon erreicht? Wir sagen ‚Nein‘ und eine Begründung folgt.

Seit Mai 2019 sind zehn Eskalationsschritte durch Cyberkriminelle dazugekommen, während es in den fast 30 Jahren davor gerade einmal drei waren. Natürlich haben erst die rasanten Leistungen unserer Computer, das globale Internet und Kryptowährungen eine so rapide Beschleunigung ermöglicht. Und wo stehen wir? Gefühlsmäßig auf der zweiten Stufe „Debatte, Polemik“ mit Tendenz zur dritten Stufe „Taten statt Worte“.

Bei einer genauen Betrachtung erkennen wir ebenfalls Stufen einer Deeskalation, wo Cyberkriminelle weitere Grenzüberschreitungen mit eigenen Korrektur-/Gegenmaßnahmen verhindern wollen – das Geschäft mit Ransomware ist zu lukrativ geworden, um es sich mit militärischen Maßnahmen gegen das eigene Land zerstören zu lassen:

Deeskalationsschritte von Cyberkriminellen	Stufen einer Deeskalation	Original/Englisch	Erklärung/Übersetzung	Hinweise
1	Stufen 1-2	Target selection	Technische Maßnahmen, um keine Opfer im eigenen Land zu erpressen	Seit ca. 2019
2	Stufen 1-2	Protecting the reputation	Das Versprechen, veröffentlichte Daten wieder zu löschen bzw. eine funktionierende Entschlüsselung zur Verfügung zu stellen	Seit ca. 2020
3	Stufen 1-2	No attacks on hospitals	Das Versprechen, keine Gesundheitseinrichtungen anzugreifen	Seit ca. April/Mai 2020
4	Stufen 1-2	No attacks on critical infrastructure	Das Versprechen, keine Betreiber von kritischer Infrastruktur anzugreifen	Stand Mai 2021
5	Stufe 3	Banning ransomware markets	Untergrundforen wie XSS verbieten Werbung und Beiträge zum Thema Ransomware	
6	Stufe 3	Only dataleaks	Ransomware-Gruppierungen „überlegen", sich nur auf Datenlecks zu fokussieren, um potenziell keine Schadsoftware in kritischer Infrastruktur zu verbreiten	Stand August 2021

Ein paar wenigen Stufen der Deeskalation.

In den Stufen 1-2 einer Deeskalation sprechen Experten von Selbsthilfe und in den Stufen 3-4 einer Deeskalation von Mediation/Vermittlung durch Familie oder Freunde. Die Stufen der Deeskalation sind weitaus schwieriger darzustellen, da einzelne Ransomware-Gruppierungen bei deeskalierenden Maßnahmen weit inhomogener agieren als zusammengefasst als einziger Akteur. Beispielsweise halten sich manche Gruppierungen an eigene Versprechen, ändern diese später wieder oder ignorieren die Empfehlungen der Konkurrenz.

Die wichtigste Erkenntnis von Stufen der Eskalation, ist zu erkennen, wo sich die Akteure befinden. Nach einem Ransomware-Angriff auf den größten Fleischverarbeitungsbetrieb in den USA, den die Angreifer irrtümlich in Brasilien vermutet hatten, kippte der amerikanische Volkszorn aus Angst vor einer Steak-Knappheit in Polemik (Stufe 2): Der mediale Hilferuf nach rettenden Navy SEALs, die in Kasachstan medienwirksam eine Fabrik mit Dark Web Servern übernehmen oder ein vermeintliches CIA-Video eines Hellfire-Raketenangriffs auf den Luxussportwagen eines Cyberkriminellen blieben bis dato aus, was für die geopolitische Weltlage weiterhin sehr besonnen erscheint. Weder ein konstantes (Vor)Verurteilen von Russland durch die USA noch eine Dauerduldung von Ransomware-Gruppierungen durch Russland für geopolitisches Sticheln wird in Zukunft eine erhoffte Lösung bringen. So antwortete im Juni 2021 US-Präsident Joe Biden auf die Frage eines Journalisten zu den weiterhin gängigen diplomatischen Protokollen mit Russland: „*If you don't understand that, you're in the wrong business.*"[7]

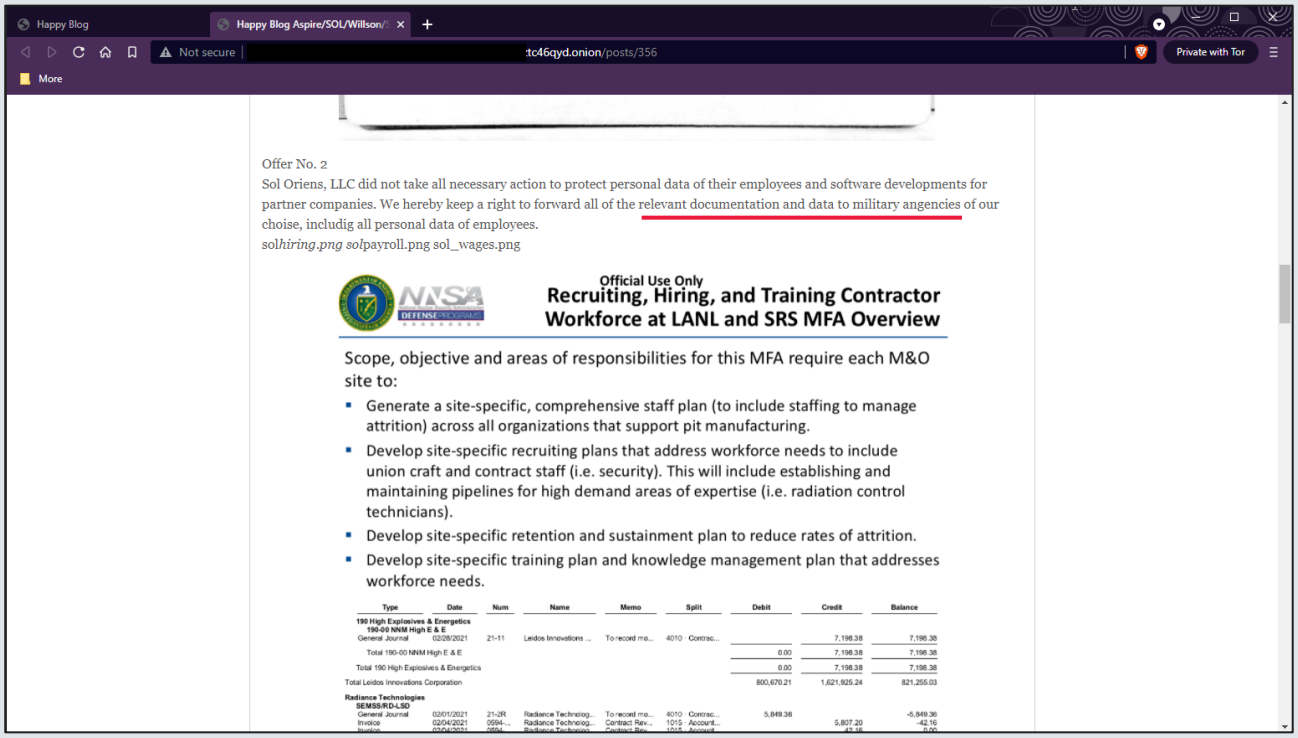
Diese Sichtweise korrespondiert ebenfalls mit der Meinung der „besonnenen" Fachexperten, wie jener von Dmitri Alperovich. Als Kind russischer Einwanderer und Gründer der US-Sicherheitsfirma CrowdStrike will Alperovich weiterhin nicht von einem Cyberkrieg sprechen: „*We also need to apply significant pressure on countries harboring these criminals and offering them safe haven (primarily Russia). We need to demand immediate arrests and prosecutions…*"[8]

Wo verläuft die rote Linie bei Ransomware?

Seit Jahren prophezeien Experten mögliche Cyberangriffe auf Betreiber von kritischer Infrastruktur wie Gesundheitseinrichtungen, Wasser-, Energieversorger und ITK-Unternehmen. Cyberangriffe auf diese Betreiber wären die rote Linie, die es nicht zu überschreiten gelte. Nach Ransomware-Angriffen auf Energieversorger, Spitäler – sogar einem mit Todesfolge in Deutschland – und einem Pipeline-Betreiber in den USA wurde diese rote Linie mehrfach und scheinbar ohne gröbere Konsequenzen überschritten. Laut einem Interview mit einem anonymen Mitglied einer kriminellen Gruppe sollen sogar Atomkraftwerke

[7] vgl. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4
[8] vgl. https://twitter.com/DAlperovitch/status/1399780133704175624

leichte Angriffsziele sein. Ein fabriziertes Gerücht? In den USA wurde im Mai 2021 der bis dato unbekannte Dienstleister SOL ORIENS LLC angegriffen, der mutmaßlich nukleare Uboot-Torpedos für amerikanische Streitkräfte serviciert. Vertrauliche Dokumente von SOL ORIENS wurden zeitweise im digitalen Untergrund angeboten:



Ankündigung zu SOL ORIENS LLC – mit dem Hinweis einer „Weiterleitung" der Dokumente – eine rote Linie für US-Streitkräfte?

Viele staatliche Vergeltungsmaßnahmen verlaufen oft für die breite Öffentlichkeit unbemerkt: Staatliche Einrichtungen und Softwarefirmen wie Microsoft konfiszieren gemeinsam Bitcoins und Domains von Kriminellen, blockieren Steuer-Server für Command and Control im Internet oder zerstören Schadsoftware über die Manipulation von Quellcode. Für Experten viel zu langsam und viel zu wenig, was teilweise mit den dafür notwendigen richterlichen Anordnungen zu tun hat.

Dafür haben amerikanische Bürokraten ihre Version einer roten Linie definiert: Wer beispielsweise an die Gruppierung Evil Corp. das Lösegeld in Bitcoin bezahlt, der verstößt gegen „internationale" Sanktionen der USA und kann dafür weltweit von der amerikanischen Justiz belangt werden.[9] In der Privatwirtschaft hat sich inzwischen ein Nischenmarkt für moderne Lösegeldverhandler[10] entwickelt, die den betroffenen Firmen mehr Zeit und weniger hohe Forderungen für die garantierte Rückgabe der gestohlenen Daten ermöglichen sollen. Was in den 1980er-Jahren in Südamerika und Südosteuropa für den Freikauf von Geiseln notwendig war, wiederholt sich im Cyberspace.

Der bisherige Höhepunkt der Ransomware-Eskalation kam schließlich im Juli 2021, wie Experten und Kommentatoren vermuteten: Das amerikanische Software-Unternehmen Kaseya wurde Opfer eines „hochkomplexen" Angriffs auf seine Lieferkette durch die Ransomware-Gruppierung REvil. Was im ersten

[9] vgl. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[10] vgl. https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers

Moment nach einem Angriff auf die Lieferkette von Kaseya aussah, entpuppte sich wenige Tage später als alter Hut: Über einen SQL Injection Angriff konnten die Angreifer die Kaseya Virtual System Administrator-Software manipulieren. Von Kaseya empfohlene Ausnahmeregeln verhinderten die Entdeckung von Computerviren und so konnte über kompromittierte Updates die REvil-Ransomware an weit über tausend Endkundinnen und -kunden verbreitet werden. Kaseya ermöglicht seiner Kundschaft, die Netzwerke von deren Kundinnen und Kunden mit Software-Updates zu administrieren und somit entwickelte sich das tatsächliche Schadensausmaß exponentiell.

Sicherheitsforschern waren diese Angriffsmöglichkeit bereits seit mindestens 2015 bekannt, wie Kommentare[11] auf einer bekannten Plattform für Zero-Day-Sicherheitslücken bzw. ein Artikel aus einem russischsprachigen IT-Medium zeigten. Ein IT-Unternehmer kommentierte dies treffend in seinem Twitter-Benutzerbeitrag mit den Worten: *„It is unacceptable that certain vendors (looking at you Kaseya) don't fix their crap software when notified.“*[12]

Ransomware: Was (vorher) tun?

Damit ergibt sich die berechtigte Frage: Sind wir der Ransomware komplett ausgeliefert und können wir nur hilflos zuwarten? In einem animierten Werbespot für einen Energydrink unterhalten sich zwei Antilopen über die Wirksamkeit des beworbenen Getränks als Schutz vor einem herannahenden Löwen. Die eine formuliert dabei pointiert: *„Ich muss ja gar nicht schneller sein als der Löwe. Nur schneller als du.“* Diese humorvolle Betrachtung trifft aktuell auf viele Unternehmen in Bezug auf Ransomware zu.

Bei Medienbeobachtungen von Vorfällen ergibt sich qualitativ betrachtet im Nachhinein fast immer das gleiche Bild: Gängige Standards und wiederholte Warnungen wurden bereits im Vorfeld ignoriert, technisch-organisatorische Maßnahmen waren nicht oder nur unzureichend vorhanden und längst notwendige Updates wurden aus Zeit- oder Kostengründen nicht eingespielt. Ein konkretes Beispiel dafür stammt aus dem Jahr 2019 - schon Jahre vor einem Ransomware-Angriff war dem Berliner Kammergericht eine veraltete IT-Landschaft von einem externen Prüfer attestiert worden. So schrieb das IT-Fachmedium Heise Online zu diesem Vorfall: *„Es habe im Haus [im Kammergericht] immer wieder Kritik an ausbleibenden Backups, Schulungen und Sicherheitsupdates gegeben, ‚die mutmaßlich aus Kostengründen eingespart wurden‘.“*[13]

Die bekannte Journalistin Kim Zetter wiederum beschreibt einen Vorfall in den USA, bei dem während einer Krisenbesprechung ein Mitarbeiter einen Taschenrechner zur Hand nahm und durchrechnete: Bei der vorhandenen Bandbreite und Entfernung zum Backup-Server, der Backup-Lösung und dem Stand der Backups würde eine Wiederherstellung des Betriebs mehrere Jahre benötigen…

Seit Jahren bewährt sich das Modell der drei Verteidigungsstufen im Geschäftsalltag, im Englischen als „Three Lines of Defense“ bekannt, und ist genauso für Reputations- und Cyberrisiken adaptierbar:

[11] vgl. „Kaseya Virtual System Administrator Remote Privilege Escalation Vulnerability“, https://www.zerodayinitiative.com/advisories/ZDI-15-448
[12] vgl. https://twitter.com/_IntelligenceX/status/1415647601106604032
[13] vgl. https://www.heise.de/newsticker/meldung/Mutmasslicher-Emotet-Befall-Trojaner-wuetet-in-Berliner-Kammergericht-4544747.html

THREE-LINES-OF-DEFENSE-MODELL			
Verteidungsstufe	FIRST LINE OF DEFENSE (1. Verteidigungsstufe)	SECOND LINE OF DEFENSE (2. Verteidigungsstufe)	THIRD LINE OF DEFENSE (3. Verteidigungsstufe)
	steuert	Vorstand/Geschäftsführung konsultiert	erteilt Auskunft an
Verantwortlich	Operatives Management	Riskomanagement/Revision	Auditoren/Aufsichtsrat
Verantwortung	Besitzer von Kontrollen und Risiken	Technische oder organisatorische Mängel identifzieren und neue Risiken durch Trends identifzieren	Auditierung der Rahmenwerke gemäß Regulatorien, internationaler Standards und Empfehlungen (Best Practices)
Umsetzung	Kontrollen überwachen und Risiken behandeln (abwenden, behandeln, versichern)	Rahmenwerke für Kontrollen und Risiken (Technisch-organisatorische Maßnahmen) vorgeben	Entlastung erteilen oder Defizite aufzeigen und Verbesserungen einfordern
Outsourcing/Co-Sourcing durch BDO Consulting	Business-Partner-/Vendor-Management Vulnerability Scan (Pen Testing) Datenschutz (DSGVO) Information Security (ISO 27001) IT Control & IT Governance Phishing Simulation	Cyber Intelligence (Cyber Risk Monitoring) Risikomanagement Threat Intelligence (Information Sharing)	Datenanalyse IT-Forensik Internal Audit/IT-Audit Incident Management

Adaptierte Version der „Three Lines of Defense“ durch den Autor (BDO Consulting)

Ransomware-Angriffe sind in erster Linie Cyberangriffe auf den operativen Teil des Unternehmens und werden durch eine nicht adäquate Umsetzung der vorhandenen Kontrollen und/oder dem Negieren von Risiken möglich: Beispielsweise werden Passwörter für private freizeitorientierte soziale Netzwerke für Zugänge von Microsoft Outlook Web Access (OWA) gewählt, wodurch Kriminelle den Zugriff auf Outlook leicht „erraten“ können. Im Rahmen von „Penetration Tests“ können Schwachstellen bei der Konfiguration und der Version von Software erkannt werden, die serverseitig im Internet sichtbar sind. Genau dieses Penetration Tests lassen Ransomware-Gruppierungen selbst von Dritten umsetzen, um nachher gezielt Software, Server und Services mit kritischen Sicherheitslücken zu attackieren.

Outsourcing an Dienstleister/Vendoren kann ebenfalls zu einem Cyberrisiko werden, wie beispielswiese Cloud-Dienste (Managed Service Provider) für Datenaustausch, die nicht korrekt abgesichert sind und so sensible Daten von unbefugten Dritten eingesehen und übernommen werden können. Eine kritische Sicherheitslücke bei der Accellion „File Transfer Appliance“ wurde dieses Jahr entdeckt, sofort von der Ransomware-Gruppierung Clop ausgenutzt und mehrere Finanzdienstleister – darunter eine Zentralbank – angegriffen sowie versuchsweise erpresst. Ungesicherte Datenbanken in der Cloud (z.B. bei Amazon Web Services) sind mittlerweile eine der häufigsten Ursachen von Datenlecks im Internet und geben viel über die Kundinnen und Kunden als auch das Unternehmen preis. Der Aberglaube, dass der erhöhte Netzwerkverkehr einen bevorstehenden Cyberangriff vorab anzeigen würde, wird durch eine verdeckte Übertragung auf Cloud-Dienste zu Amazon Web Services, Google oder Microsoft OneDrive kompensiert und geschickt in der Ruhezeit des betroffenen Unternehmens umgesetzt.

Ergänzende externe Dienstleistungen sind per se effizient, ressourcensparend und ermöglichen eine Digitalisierung von Dienstleistungen bei KMU, die davor nur großen Konzernen vorbehalten waren. Jedoch müssen auch externe Dienstleister eingebunden und verwaltet werden. So ist es nicht unüblich, dass Partner typische Anwendungen wie Remote Desktop, Server-Shares oder TeamViewer verlangen, um schnell und unkompliziert auf interne Ressourcen des Auftraggebers zugreifen zu können. Dies mag

durchaus Legitimation haben, muss aber durch Berechtigungsmanagement und technisch-organisatorische Maßnahmen – Stichwort „Zero-Trust“ – streng reguliert und abgesichert sein. Die Auswahl der Dienstleister/Vendoren sollte nach Kriterien erfolgen, die sich nicht nur am Angebotspreis orientieren, sondern auf risikoreduzierende Kriterien wie Nachhaltigkeit (z.B. Standort und Energieeffizienz von Managed Service Providern), Reputation (z.B. geographische Lage, Beteiligungen, Kundenstock, Historie der Datensicherheit) und den technischen Stand (z.B. Hardware, Softwareversionen) eingehen.

Ebenso nutzen Ransomware-Gruppierungen den über Jahre angesammelten Datenmüll der betroffenen Unternehmen aus, worin sich vergessene Ausweiskopien oder anderwärtige sensible personenbezogene Daten befinden. Hier unterstützt BDO beispielsweise seine Kundinnen und Kunden bei der Reduktion von Daten, indem veraltete Datenbestände de-duplizieret, archiviert und über eDiscovery nicht mehr notwendige Kundendaten DSGVO-konform gelöscht werden.

Viele Ransomware-Angriffe haben ebenso die Problematik von Backup-Lösungen aufgezeigt: So mag zwar die kostensparende Archivierung in ein magnetbandbasiertes Cold Storage für bestimmte Anwendungsfälle (z.B. Dokumentenarchiv) optimal sein, aber Faktoren wie Bandbreite, Anzahl der Arbeitsplätze, gewählte Backup-Lösung und Standort des Backup-Rechenzentrums haben schon manche IT-Verantwortliche bitter überrascht, wie lange ein Wiederherstellen im Ernstfall tatsächlich benötigen würde. Was inkrementell nachts über Monate hinweg zum (virtuellen) Backup-Server transferiert wird, kann bei dem Versuch einer kompletten Wiederherstellung völlig anders aussehen. Amazon Web Services bietet aus diesem Grund in den USA bereits ein bewachtes und mobiles Rechenzentrum als LKW-Anhänger an. Manche Unternehmen entdeckten schon kompromittierte Backups, zu denen entweder der digitale Schlüssel zur Wiederherstellung von den Kriminellen zerstört worden oder bei denen die Integrität der wiederhergestellten Dateien mangelhaft war. So berichtete unlängst ein verärgerter Software-Entwickler in sozialen Medien, dass sogar die PDF-Dateien auf seiner Harddisk für die „Paper Keys“[14] zur Wiederherstellung von administrativen Zugängen von den Kriminellen kopiert worden seien…

Zum Schluss noch die wirklich schlechte Nachricht: Es gibt weit gefährlichere Bedrohungen im Internet als Ransomware. Beispielsweise durch staatliche Angreifer kompromittierte Software-Updates, die weltweit alle Anwenderinne und Anwender ausspionieren, oder wiederkehrende Zensurversuche durch staatliche Stellen gegen „blasphemische“ Medien wie YouTube, die das veraltete Border Gate Routing Protocol und Teile vom Internet lahmlegen. Luxemburg war im Juli kurzfristig offline[15], weil jemand irrtümlich über einen „Mass-Scan“ mit falschen Parametern das Internet absuchen wollte. Dazu kommen unreparierbare Schwachstellen beim „Internet der Dinge“ (IoT) oder veraltete Industriesteuersysteme (OT) mit Windows 7 oder XP im Dauerbetrieb von kritischer Infrastruktur.

Auch wenn Ransomware seit Monaten medial dominiert, so gibt es noch andere Formen von Cyberkriminalität: *Business E-Mail Compromise* (BEC) bleibt als kriminelles Geschäftsmodell weiterhin erfolgreich und „erwirtschaftete“ im Jahr 2020 von betroffenen Unternehmen einen Gesamtschaden von über USD 1,8 Milliarden. *Cryptojacking* erlebt seit der Pandemie wieder einen Boom und frisst Strom und Ressourcen für die unerwünschte Erzeugung von Kryptowährungen auf. Bei Ransomware lag der kriminelle Profit im Jahr 2020 vergleichsweise „nur“ bei USD 370 Millionen. Mit hoher Wahrscheinlichkeit wird Ransomware im Jahr 2021 noch ordentlich dazugewinnen: 2019 wurden gemäß DarkTracer 12 Unternehmen mit erpresserischer Ransomware erpresst, im Jahr 2020 bereits 1.390 Opfer und bis Juni 2021 waren es schon 1.115 Opfer, die erpresst wurden. Der Trend zeigt nach oben! Wer wann und wie viel

[14] Anmerkung: PDF-Dateien mit Paper-Keys sollten ausgedruckt und sicher verwahrt werden. Die PDFs dazu gehören logischerweise im Anschluss, also nach dem Druckvorgang, digital zerstört und sollten nicht abgelegt oder per E-Mail versandt werden.
[15] Siehe https://twitter.com/tcpdirect/status/1412177003877343232

gezahlt hat, wird eine Dunkelziffer bleiben und grobe Schätzungen dazu werden erst gegen Jahresende 2021 möglich sein.

Und jetzt? Es folgen die Klagewellen…

Ein aktuelles Beispiel aus den USA demonstriert, was Unternehmen in den nächsten Monaten und Jahren nach Ransomware-Angriffen erwarten wird. Gemeint sind nicht etwa die „obligatorischen" Klagen einer Börsenaufsicht oder Datenschutzbehörde, sondern Sammelklagen durch verärgerte Kundinnen und Kunden, die von Ransomware-Vorfällen bei Unternehmen zwar nur indirekt, aber wegen dadurch fehlender Ressourcen voll betroffen sind. So zitiert das Medium Golem den amerikanischen Rechtsanwalt John Yanchunis, der zu dem Vorfall bei dem Pipeline-Betreiber Colonial-Pipeline ausführt: „*Eine Sache, die [Colonial-Pipelines] nicht getan ha[t] und in der sie nicht gut sind, ist der Schutz ihres Informationssystems, denn das kostet Geld, und es ist kein Geld, das zur Steigerung des Gewinns verwendet wird…*"[16]

Neben einer Klage der Tankstellenbetreiber gegen Colonial-Pipeline klagen nun die Konsumentinnen und Konsumenten der betroffenen Tankstellen und sogar eine dritte Sammelklage gegen Colonial-Pipeline soll bereits in Vorbereitung sein.

[16] Siehe https://www.golem.de/news/usa-tankstellen-verklagen-colonial-nach-ransomware-angriff-2107-158428.html

Die fünf wichtigsten Erkenntnisse zu Ransomware mit Stand August 2021

1. **Ransomware ist eine aufstrebende und höchst lukrative „Industrie“:** Irrtümliche Angriffe auf Betreiber von kritischer Infrastruktur, das Ausnutzen von Netzwerkeffekten, die Verkettung von Angriffen durch unterschiedliche Akteure und vermutete staatliche Interessen wie Sabotage (Destabilisierung) zeigen, dass wir uns in ferner Zukunft auf einen Cyberkonflikt zubewegen, der entweder zu einem Ausfall oder wahrscheinlicher zu einer Segmentierung des weltweiten Internets führen könnte. Eine politisch motivierte Absicht muss jedoch nicht dahinterstecken. Hingegen wird der Einsatz von künstlicher Intelligenz oder von Hochleistungscomputern für Cyberangriffe bald für Cyberkriminelle leistbar sein, die jetzt schon durch ihre Kriegskassen über unveröffentlichte Sicherheitslücken (Zero-Days) verfügen. Früher war ihr Einsatz nur staatlichen Akteuren vorbehalten.
2. **Eine staatliche Duldung (Safe Heaven) von Ransomware-Gruppierungen ist erkennbar, aber nicht nachweisbar:** Ob Russland bewusst Ransomware-Gruppierungen wie Clop, Evil Corp. und REvil zur Destabilisierung im Westen einsetzt, kann aktuell weder bestätigt noch ausgeschlossen werden. Wir vermuten Ransomware-Gruppierungen im Umfeld von privaten IT-Firmen, die staatliche Aufträge übernehmen, wofür es bereits in der Vergangenheit ähnliche Beispiele (z.B. WINNTI) gab. Möglicherweise wissen die staatlichen Auftraggeber von den „Freizeitaktivitäten“ ihrer Subunternehmen nichts oder halten nur die Hand auf. Eine vermeintliche Funkstille, also das Abtauchen von Ransomware-Gruppierungen, war bis dato kein eindeutiges Indiz dafür, dass die Kriminellen tatsächlich aufhören oder sogar verhaftet wurden.[17] In vielen Fällen tauchen die Kriminellen aber ein paar Wochen später unter einem anderen Ransomware-Pseudonym wieder auf.
3. **Unternehmen können und müssen sich vor Ransomware schützen:** Zu den von Ransomware besonders betroffenen Ländern gehören die USA, Kanada, Frankreich, Großbritannien und Italien, wie eine aktuelle Statistik von DarkTracer zeigt. Gemäß unseren Recherchen ist Ransomware in Südostasien und China ebenfalls ein Problem. Es trifft wirklich alle – es sind Ransomware-Vorfälle aus Russland bekannt, die Opfer genauso hart treffen wie anderswo. Die Kriminellen holen sich die leichtesten Opfer zuerst und von denen gibt es mehr als genug, wie Medienberichte hinlänglich dokumentieren. Was können Unternehmen dagegen tun? Der Kauf einer kyrillischen Tastatur ist jedenfalls keine Lösung. Experten wie Matt Bromiley[18] schlagen stattdessen vor: Ein ständiger Informationsaustausch (Threat Intelligence, CERTs), das Absichern von administrativen Zugängen mit einer Multi-Faktor-Authentifizierung, Notfallpläne erstellen und ein regelmäßiges Üben dieser gehört zu den Grundlagen.
4. **Ransomware-Angriffe über die Lieferkette von Software-Unternehmen sind bis dato nicht vorgekommen:** Fehlerhafte Software und Datenlecks mit Benutzerkonten sind mehr als ausreichend vorhanden. Gab es tatsächlich noch keine Fälle von Ransomware in Lieferketten? Bis dato definitiv nein. NotPetya war keine Ransomware, sondern ein gezielter Cyberangriff zur Destabilisierung der Ukraine, die Cyberangriffe auf RSA und SolarWinds dienten der Spionage und im Falle des Unternehmens Kaseya sind wir im Juli 2021 knapp an diesem Szenario vorbeigeschrammt. Bei Kaseya und SolarWinds sind neben den kritischen Schwachstellen nachweislich Empfehlungen kursiert, wichtige Ordner am Speichermedium von der ständigen Überprüfung durch Anti-Viren- bzw. Sicherheitssoftware auszuklammern, was Mikko Hyppönen von F-Secure stark kritisiert. Die berichteten Pannen bei

[17] vgl. https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil
[18] vgl. https://threatpost.com/ransomware-defense-top-5-tips/167536

Unternehmen wie Accelion, Kaseya und SolarWinds zeigen, dass ein Mix aus Marketingversprechen (*overpromise*) und Profitdenken (*underdelivery*) die Softwareentwicklung vieler Unternehmen steuert und fernab von Security by Design ist. Die Quintessenz: Regelmäßige Software-Updates sind immer noch eines der wichtigsten Mittel im Kampf gegen Ransomware, auch wenn Medien kompromittierte Lieferketten von Softwareunternehmen als alternatives Ende der Menschheit darstellen wollen. Auch bei der Aktualisierung von Software gibt es Sicherheitsmaßnahmen und Empfehlungen von Experten.

5. **Ransomware ist eine indirekte Antwort auf geopolitische Sanktionen:** Gelebte Nachhaltigkeit über Entschleunigung, gelenkte Migration zur fairen Verteilung und fundierte Entwicklungshilfen sind geostrategische Maßnahmen, die in den letzten Jahren gegen den Rat von Experten vernachlässigt wurden. Mit diesen Themen lassen sich für Populisten keine Wahlen gewinnen. Piraterie und Erpressung sind jedoch seit Jahrhunderten bekannte Formen der Kriminalität, die durch die Klimakrise und geopolitische Sanktionen virtualisiert und somit beschleunigt werden.

KONTAKTDATEN

Ewald Kager
Partner

+43 5 70 375 - 4211
+43 664 60 375 - 4211
ewald.kager@bdo.at

Lorenz Szabo
Manager

+43 5 70 375 - 1836
+43 664 60 375 - 1836
lorenz.szabo@bdo.at