FAST LTA
Wir sichern Petabytes.

Faktencheck

Was kostet ein Ransomware-Angriff?

2020 war ein in jeder Hinsicht außergewöhnliches Jahr. Auch und gerade für Ransomware. Über 20.000 neue Berichte über aufgedeckte Sicherheitslücken, eine 50-prozentige Zunahme von Schwachstellen in mobilen Geräten und ein Anstieg der Angriffe um 72% seit Beginn der Corona-Pandemie[1]. **Im dritten Quartal 2020 erreichten die Forderungen ihren Höhepunkt** mit durchschnittlich 230.000 USD, im vierten Quartal fiel der Wert wieder leicht[2].

In vielen prominenten Fällen von Ransomware-Angriffen ist nicht öffentlich bekannt, ob und wie viel Lösegeld die Opfer bezahlt haben. **Klar ist jedoch, dass die Kosten, die insgesamt durch einen Ransomware-Angriff entstehen, um ein Vielfaches höher sind** - auch wenn nicht jeder Fall mit über 50 Millionen USD zu Buche schlägt, wie die Bilanz der Universal Health Services, Inc (UHS) ausweist[3].

Wir haben uns die 5 größten finanziellen Risiken angesehen, die ein Ransomware-Angriff auf Unternehmen, Behörden oder Gesundheitseinrichtungen mit sich bringt.

Stand: April 2021

#1

Ausfall der IT

Da der Großteil aller Kommunikation, Abwicklung, Lagerhaltung und Abrechnung heute digital ist, bedeutet jeder Tag ohne funktionierende IT direkte Verluste. **Je länger ein Unternehmen „offline“ ist, desto mehr machen sich Umsatzeinbußen und Stornierungen bemerkbar.**

Aber es drohen auch langfristige negative Folgen, wenn etwa Wartungsverträge nicht erfüllt werden können. In diversen Studien hat sich herausgestellt, dass die Kosten, die durch „Downtime“ entstehen, **bis zu 50 mal höher sind als die eigentliche Lösegeldforderung**[4].

Im Durchschnitt vergehen drei Wochen, bis ein betroffenes Unternehmen wieder operabel ist[5]. Es gibt aber auch Beispiele, bei denen der Prozess der Säuberung und Wiederherstellung der IT-Infrastruktur wesentlich länger dauerte. Fälle wie der des Aluminiumriesen Norsk Hydro, der 2019 **über 3 Monate offline** war[6], sind allerdings außergewöhnlich. Bei dem norwegischen Konzern wurden in kürzester Zeit 22.000 Computer an 170 Standorten in 40 Ländern befallen. **Die gesamte Belegschaft von 32.000 Mitarbeitern musste monatelang zurück zu Stift und Papier**, was das Unternehmen am Ende über 70 Millionen USD gekostet hat[7].

Was tun?

Es ist essenziell, die Zeit bis zur erneuten Verfügbarkeit aller Dienste und Systeme zu verkürzen. Dies fällt naturgemäß umso schwerer, je mehr Systeme befallen sind. Aber es gibt eine entscheidende Komponente, die überlebenswichtig ist: **sichere, richtig konfigurierte Backups**.

Obwohl Backups ganz sicher zu den Datenschutzmaßnahmen gehören, die jedes Unternehmen und jede Behörde einsetzt, macht die Art der Sicherung hier den Unterschied. Moderne Schadsoftware attackiert heutzutage auch gezielt Backups, so dass sich bei reinen Netzwerk- und Online-Backups die vermeintliche Sicherheit schnell in Luft auflösen kann.

Grundvoraussetzung sind also Backups, die unter keinen Umständen durch Ransomware kompromittiert werden können. Diese Backups müssen lokal verfügbar sein (im Notfall werden ja als erstes alle Verbindungen zum Internet gekappt), dürfen nicht mit dem laufenden Netzwerk verbunden sein (sonst sind sie eben auch Ziel der Ransomware-Attacke), und müssen hinsichtlich der Anforderungen und finanziellen Möglichkeiten entsprechend konfiguriert worden sein. Die beiden Kern-Parameter, die jeder IT-Admin kennt, sind RTO und RPO[8]:

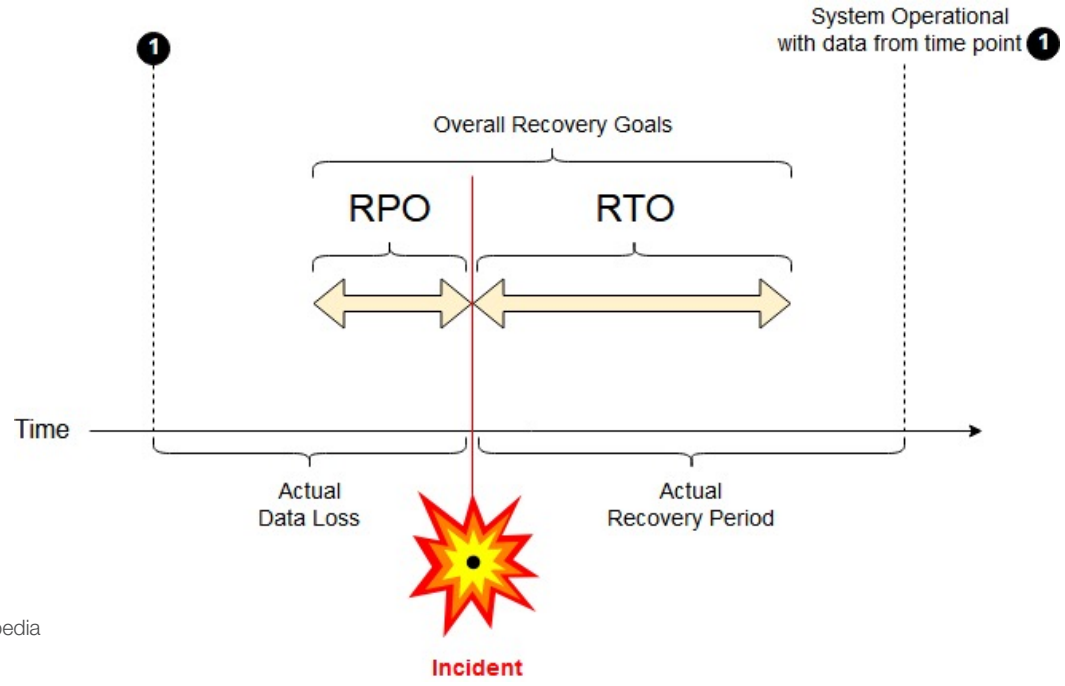


Abb.: Wikipedia

- **RTO - Recovery Time Objective** - bezeichnet die Zeit, die ein Ausfall maximal dauern darf, bis alle Daten aus dem Backup wiederhergestellt werden konnten.

- **RPO - Recovery Point Objective** - legt fest, welcher Datenverlust noch hinnehmbar ist, wenn Daten aus früheren Backups wiederhergestellt werden müssen.

Am besten wäre es natürlich, beide Parameter auf 0 setzen zu können, was aber technisch nicht möglich ist. Je nach Budget gilt es also, **einen sinnvollen Kompromiss** zwischen häufigen Backups, die schnell wieder eingespielt werden können, und den Kosten für die Backup-Infrastruktur zu finden.

Zur Wiederherstellung der Daten kommt im Fall eines Ransomware-Befalls immer auch die Zeit zum Aufspüren der Schädlinge, zur Säuberung aller Komponenten und Neuinstallation bzw. zum Ersatz einzelner Server und PCs. Erst dann können die entsprechenden Backups wieder eingespielt werden. **Dabei ist jedoch besondere Vorsicht geboten**: Da Ransomware sich oft wochen- und monatelang unauffällig im System verbreitet, bevor die eigentliche Verschlüsselung beginnt, dürfen die wiederhergestellten Daten natürlich keine Komponenten der Schadsoftware enthalten bzw. diese Daten nicht aus den Backups wiederhergestellt werden.

Eine individuell auf das Unternehmen, die Behörde oder Gesundheitseinrichtung abgestimmtes Backup-Konzept **mit mehreren Instanzen (Stichwort: 3-2-1-Regel), Offline-Kopien (auch als Air Gap bezeichnet) und lokalen Backup-Archiven** ist deshalb unausweichlich.

Unser Tipp

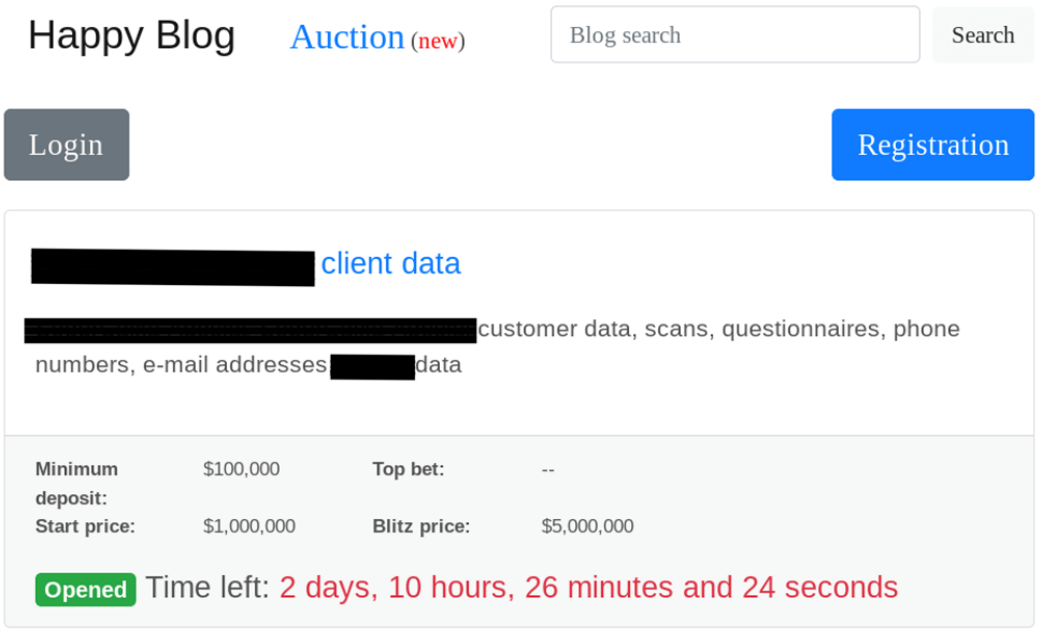
Wie immer gilt: Jedes Backup ist nur so gut wie der Restore. In einer aktuellen Studie fand der Backup-Spezialist Veeam heraus, dass **über die Hälfte der Versuche zur Wiederherstellung fehlschlagen**[9]. Wie man ganz grundsätzlich eine umfangreiche und komplette Backup-Strategie **mit Veeam und dem flexiblen Sekundärspeicher Silent Bricks** umsetzt, haben wir in unseren Veeam Mini Guides beschrieben[10].

#2

Doppelte Erpressung

Eine weitere Erfahrung aus den letzten Jahren zeigt, dass Angriffe gezielter werden. Große Unternehmen, Behörden und Einrichtungen des Gesundheitswesens geraten verstärkt in den Fokus der Angreifer. Und um die **aus Sicht der Hacker schlechte Zahlungsmoral** zu verbessern, kommt nun ein weiterer Aspekt hinzu: Vor der Verschlüsselung greifen aktuelle Malware-Versionen wie DoppelPaymer, Ryuk oder Egregor massiv Daten aus den befallenen Systemen ab und **drohen dann damit, unternehmenskritische oder personenbezogene Datensätze zu veröffentlichen**. Die Drohung geht meist mit sehr hohen Lösegeldforderungen, teils im Millionenbereich, einher und baut zusätzlich Zeitdruck auf. **Wird nicht sofort gezahlt, werden nach und nach Daten veröffentlicht, und die Lösegeldforderung verdoppelt sich**.

Es gibt zahlreiche Beispiele aus den letzten Monaten, dennoch dürfte nur ein Bruchteil der erfolgreichen Angriffe überhaupt publik werden. Prominente Opfer waren unter anderem der Spiele-Hersteller CAPCOM (Japan)[11], der portugiesische Energie-Lieferant EDP[12], und der deutsche Software-Riese software AG[13]. Die software AG musste schließlich einräumen, dass „**Daten von Servern und Notebooks**“ von Mitarbeitern heruntergeladen wurden. Die Hacker hinter der Ransomware CLOP verlangten **20 Millionen USD Lösegeld**, die aber offenbar nicht gezahlt wurden.



Quelle: Crowdstrike

Abb.: Microsoft

Was tun?

Um das Abfischen von sensiblen Daten und Ransomware-Angriffe grundsätzlich möglichst zu verhindern, hat sich der Fokus in Unternehmen auf das „**Zero Trust Modell**“ verstärkt. Der Security Insider beschreibt dieses Model so: „Das Zero-Trust-Modell ist ein Sicherheitskonzept, das auf dem Grundsatz basiert, **keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen**. Es erfordert umfangreiche Maßnahmen zur Authentifizierung sämtlicher Anwender und Dienste sowie zur Prüfung des Netzwerkverkehrs.“[14]

Gerade in Zeiten von Home Office und VPN-Zugängen in die Unternehmen müssen verstärkte Sicherheitsstandards gelten. Dazu gehört auch unbedingt, dass nicht mehr alle Mitarbeiter - bzw. am besten kein Mitarbeiter über seinen Standard-Account - direkten Zugang zu sensiblen und personenbezogenen Daten hat, dass **Backups und Archive verschlüsselt gespeichert** sind und besonders kritische Daten auf **offline-fähigen WORM-Datenträgern** ausgelagert werden. Diese Maßnahmen sind ganz generell auch im Sinne der DSGVO notwendig, die eine Speicherung „nach Stand der Technik“ vorschreibt.

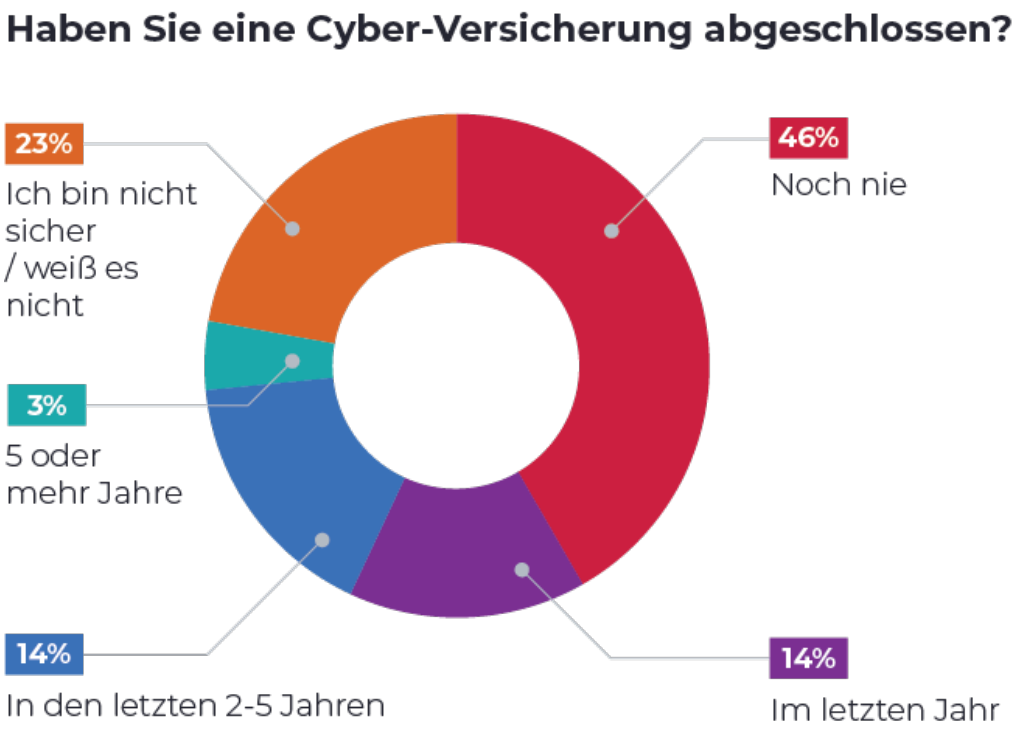
#3

Reparaturkosten

Wurde ein Unternehmen erst einmal zum Ransomware-Opfer, ist die Rückkehr zur Normalität nicht nur zeitintensiv, sondern auch mit **hohen Kosten durch Investitionen in Personal und neue IT** verbunden. Um Folgeinfektionen zu verhindern, müssen natürlich zuerst alle Sicherheitslücken geschlossen und alle betroffenen Systeme gereinigt bzw. neu aufgesetzt werden. Auch die Validität der letzten verwendbaren Backups muss geprüft werden, und nicht zuletzt müssen Daten aus diesen Backups unternehmensweit wieder restauriert werden. Theoretisch ist der Betrieb dann wieder operabel.

Viele Unternehmen, aber auch Behörden und Gesundheitseinrichtungen, reizen jedoch die Lebensdauer ihrer IT maximal aus, **investieren zu wenig** in interne Expertise und schieben **notwendige Aktualisierungen für Hardware und Software** vor sich her. Dies rächt sich im Fall eines Ransomware-Angriffs doppelt, da die dann notwendige Aktualisierung parallel zur Wiederherstellung und unter enormen Zeitdruck erfolgen muss. Besonders stark schlagen die in vielen Fällen benötigten Experten zu Buche. Jake Williams, Gründer einer Cybersecurity-Firma beschreibt das Problem dabei so: „**Notfallsupport und Überstunden kosten phänomenal mehr** als die reine Bearbeitung der Probleme. Mit anderen Worten: Upgrades, die bei normaler Budgetierung vielleicht 100.000 USD gekostet hätten, können in einem Notfall 300.000 USD und mehr kosten.“

Dass auch eine Migration „in die Cloud“ nicht vor hohen Folgekosten schützt, zeigt der Fall von Atlanta (Georgia, US). Der eher moderaten Lösegeldforderung von 50.000 USD stehen am Ende **Gesamtkosten von über 2,6 Millionen USD** gegenüber[15]. Insgesamt mussten 8 Notfallverträge geschlossen werden, die das Finden und Schließen der Sicherheitslücken, zusätzliches Personal und Microsoft **Cloud Expertise** umfassten - und direkt damit beschäftigt waren, Daten wiederherzustellen, die durch die Hacker verschlüsselt wurden. Weitere 650.000 USD wurden für Krisenkommunikation ausgegeben.



Quelle: NinjaRMM

Hauptproblem:

Nachlässiger Umgang mit Updates

Überhaupt zeigt sich, dass erschreckend viele Unternehmen und Behörden **wichtige Updates** nicht zeitnah einspielen - was nur an fehlender Expertise liegen kann. Nachlässiger Umgang mit Software- und Firmware-Updates ist das #1 Einfallstor in Unternehmen. Dazu empfiehlt es sich auch, die **spannende Geschichte von Marcus Hutchins** zu lesen bzw. anzusehen, dem jungen Hacker, der den **WannaCry**-Angriff im Alleingang stoppen konnte. Zahlreiche Unternehmen auf der ganzen Welt zählten zu den Opfern von WannaCry. Einfallstor war eine **Sicherheitslücke in Windows**, die Microsoft bereits geschlossen hatte, und die von der von der NSA entwickelten Malware „EternalBlue“ ausgenutzt werden konnte[16] [17] [18].

Gegenmaßnahmen

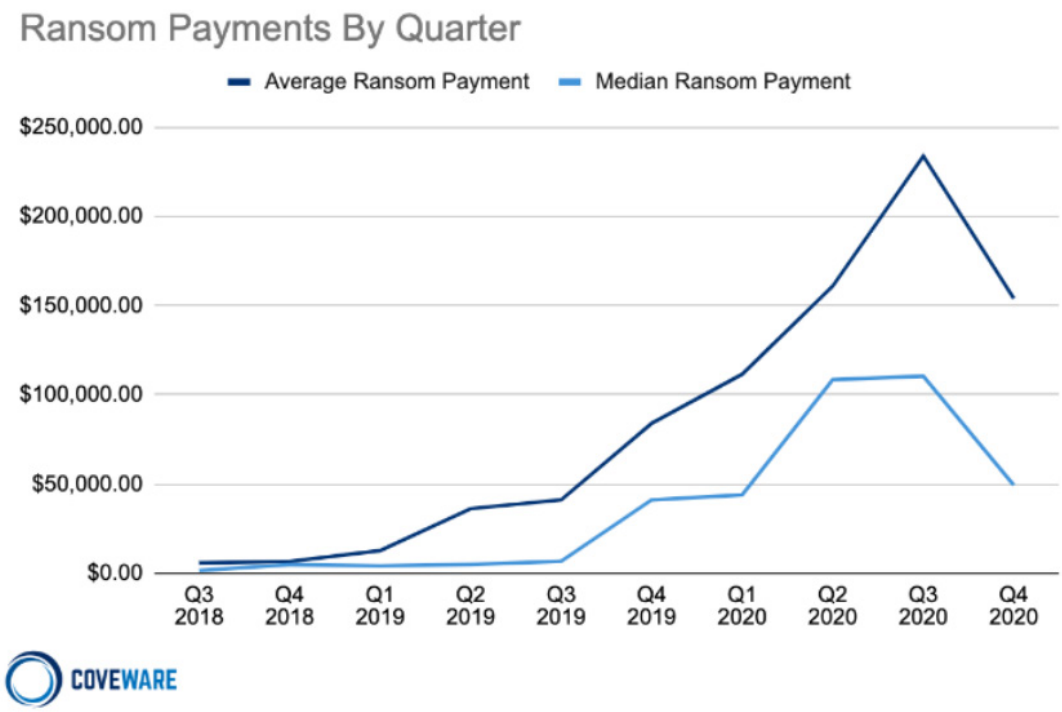
Die wichtigste Maßnahme zur Reduzierung von Folgekosten ist deshalb: Unbedingt **alle sicherheitsrelevanten Updates** auf PCs, Servern und anderen Geräten - Switches, NAS, Firewalls, usw. - zu installieren. Dazu sollte unbedingt internes Wissen aufgebaut werden oder zumindest eine vertrauenswürdige IT-Firma beauftragt werden. Äußerst empfehlenswert ist auch der **Abschluss einer Cyber-Versicherung**, die im Ernstfall große Teile der entstehenden Folgekosten übernimmt. 2020 hatten jedoch fast die Hälfte der IT-Dienstleister keine Cyber-Versicherung[19].

#4

Lösegeld

Und ja - auch die reinen Lösegeldforderungen steigen weiter an. Die durchschnittlichen Forderungen erhöhten sich von 84.000 USD im Q4/2019 auf über 230.000 USD im Q3/2020, auch wenn der Wert im Q4/2020 wieder auf gut 150.000 USD sank - offenbar war die **Schmerzgrenze erreicht**, bis zu der Unternehmen noch in Erwägung ziehen, das Lösegeld tatsächlich zu bezahlen[20].

Was man im Vergleich zum Median desselben Zeitraum sieht: Es gibt offenbar viele **Ausreißer nach oben** (Durchschnitt deutlich über dem Median). Durch weniger, aber gezieltere Angriffe auf große Unternehmen und Behörden und die Möglichkeit der Doppelerpressung kamen viele Fälle mit sehr hohen Forderungen bis hin in den **Millionenbereich** hinzu.



Quelle: Coveware

Es gibt zahlreiche Listen mit „den **höchsten Lösegeldforderungen 2020**“. Unter vielen Fällen sticht vielleicht der Befall der Outdoor-Firma Garmin hervor, da er durch die Exponiertheit der Marke tatsächlich relativ öffentlich ablief. Experten sind sich einig: Garmin hat die **geforderten 10 Millionen USD wohl bezahlt** - oder zumindest einen großen Teil davon. Für die eingesetzte Malware namens WastedLocker existiert kein Universalschlüssel. Dass Garmin nach 4 Tagen Downtime plötzlich wieder vollständig operabel war, kann nur eins bedeuten: es musste ein funktionierender Schlüssel gekauft worden sein[21].

Ganz aktuell sorgt eine neue Rekordsumme für Aufsehen: die Computerfirma ACER soll sich einer 50-Millionen-Dollar-Forderung ausgesetzt sehen, nachdem offenbar eine Lücke im **Exchange-Email-Server** ausgenutzt werden konnte[22]. Dabei zeigen sich die Angreifer flexibel: 20 Prozent Skonto bei Zahlung innerhalb von 3 Tagen, aber **Verdopplung auf 100 Millionen USD** bei Verschleppung um mehr als zwei Wochen. Was daraus wurde, ist leider unklar.

Gegenmaßnahmen

Grundsätzlich gehen viele Firmen und Behörden davon aus, dass sie den Ausfall der IT durch Zahlung des Lösegeldes massiv verkürzen können. Sophos schreibt im Report „The State of Ransomware 2020“, dass 26% der befragten Unternehmen Lösegeld bezahlt haben[23]. Allerdings erhöhten sich die Gesamtkosten, die durch einen Angriff erzeugt wurden, ziemlich genau um den Betrag des Lösegeldes. **Die Zahlung hat also in den meisten Fällen keinen Einfluss** auf den großen Restanteil des entstehenden finanziellen Verlustes. Es gilt also weiterhin der dringende Aufruf, **kein Lösegeld zu bezahlen**, so lange es irgendeine andere Möglichkeit gibt, die Daten wiederherzustellen - was über die Hälfte der befragten Unternehmen aus Backups tun konnten

#5

Reputationsverlust

Ein kaum exakt zu beziffernder aber nicht minder signifikanter finanzieller Faktor nach einem erfolgten Ransomware-Angriff dürfte der **weitreichende Imageverlust** sein. Nicht nur, dass während der Downtime Geschäfte platzen und Wartungsverträge nicht eingehalten werden können, zwei Drittel der Kunden wandern auch direkt zur Konkurrenz ab und **60% meiden ganz allgemein Firmen**, die es mit der Sicherheit offenbar nicht so genau nehmen, wie eine Studie von Arcserve belegt[24]. Und obwohl viele Sicherheitslücken nach wie vor verschwiegen werden dürften, wird es zunehmend schwieriger, erfolgte Angriffe und Datenlecks vor der Öffentlichkeit zu verbergen.

Aktiennotierte Unternehmen müssen Faktoren, die die Bilanz betreffen, sowieso veröffentlichen (siehe software AG), Verstöße gegen die DSGVO werden ebenso veröffentlicht, und die Hacker selbst tun ihr übriges, aus ihrer Sicht **erfolgreiche Attacken publik zu machen**, um den Druck zu erhöhen.

Quelle.: Arcserve

Gegenmaßnahmen

Kommunizieren Unternehmen schlecht oder gar nicht, übernimmt dies die Community im Internet. Dabei melden sich naturgemäß verstärkt diejenigen zu Wort, die irgendwann einmal schlechte Erfahrungen mit dem betroffenen Unternehmen gemacht haben. Schnell geht es nicht mehr um den eigentlichen Fall, sondern ganz grundsätzlich um den Ruf des Opfers, wie Diskussionen auf Reddit über den Fall ACER (s. o.) zeigen[25]. Problematisch dabei ist, dass diese Diskussionen dann in Suchergebnissen bevorzugt auftauchen können - und somit den Ruf nachdrücklich beschädigen können.

Achten Sie also unbedingt darauf, offen und umfassend zu kommunizieren.

Fazit

Der größte Kostenfaktor sind die durch den **Ausfall der IT** verursachten Folgekosten. Fehlender Umsatz, Strafzahlungen, die Kosten zur Wiederherstellung der IT und für die Bezahlung kurzfristig zu beschäftigender Experten schlagen höher zu Buche als die ebenfalls steigenden Lösegeldforderungen - die Sie unter allen Umständen vermeiden sollten.

Ein schlüssiges und stets zu hinterfragendes **Backup**-Konzept inklusive Restore, der auch ohne Verbindung nach außen die unternehmenskritischen Daten zu 100% wiederherstellen kann, sind der beste Schutz gegen hohe Kosten. Eine **Cyber-Versicherung** kann zudem helfen, im Ernstfall nicht auf horrenden Personal- und IT-Kosten sitzenzubleiben. Am Ende gilt es, in allen Belangen **gut vorbereitet** zu sein, da die Meinung vieler Experten lautet: Es ist keine Frage mehr, ob, sondern nur noch wann man zum Opfer einer Ransomware-Attacke wird.

Bild: Darknet Diaries

Hintergrund-Tipp: Der schlimmste Hack aller Zeiten – NotPetya

Auch ganze Staaten können Angreifer und Opfer in einer Ransomware-Attacke sein - so geschehen beim mutmaßlich russischem Angriff auf die Infrastruktur der Ukraine durch die Malware **NotPetya**. Diese wurde durch das Kapern des Update-Servers der Steuer-Software, die quasi die gesamte Ukraine einsetzt, eingeschleust, und verbreitete sich in rasender Geschwindigkeit im ganzen Land. Da das Ziel aber nicht die Erpressung von Lösegeld sondern maximales Chaos war, gab es keinen einfachen Ausweg. Hintergründe können Sie auf Youtube sehen[26] oder im Podcast hören[27] - **spannend und empfehlenswert**.

Quellenangaben

1 https://www.skyboxsecurity.com/trends-report/
2 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
3 https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue
4 https://www.datto.com/blog/downtime-the-true-cost-of-a-ransomware-attack
5 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#costs
6 https://www.bbc.com/news/business-48661152
7 https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
8 https://de.wikipedia.org/wiki/Disaster_Recovery
9 https://www.veeam.com/de/news/cxo-research-58-percent-of-data-backups-are-failing-creating-data-protection-challenges-and-limiting-digital-transformation-initiatives.html
10 https://fastlta.com/veeam-de
11 https://www.zdnet.com/article/capcom-confirms-ransomware-attack-potential-theft-of-customer-employee-data/
12 https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/
13 https://secure-technology.de/news/interne-daten-der-software-ag-nach-ransomware-angriff-veroeffentlicht/
14 https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/
15 https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
16 https://www.youtube.com/watch?v=yewkv8pTAu0
17 https://www.youtube.com/watch?v=vveLaA-z3-o
18 https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/
19 https://www.ninjarmm.com/de/blog/der-ransomware-report-2020/
20 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
21 https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/
22 https://www.security-insider.de/ransomware-angriff-acer-soll-50-millionen-us-dollar-zahlen-a-1010194/
23 https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
24 https://info.arcserve.com/en/thank-you-ransomwares-stunning-impact-on-consumer-loyalty-and-purchasing-behavior
25 https://www.reddit.com/r/worldnews/comments/ma8a54/computer_giant_acer_hit_by_50_million_ransomware/
26 https://www.youtube.com/watch?v=KODpP29AHD4
27 https://darknetdiaries.com/episode/54/

FAST LTA
Wir sichern Petabytes.

Design,
Entwicklung
und Support
in **Deutschland**

FAST LTA | Rüdesheimer Str. 11 | 80686 München | info@fast-lta.de | **www.fast-lta.de**