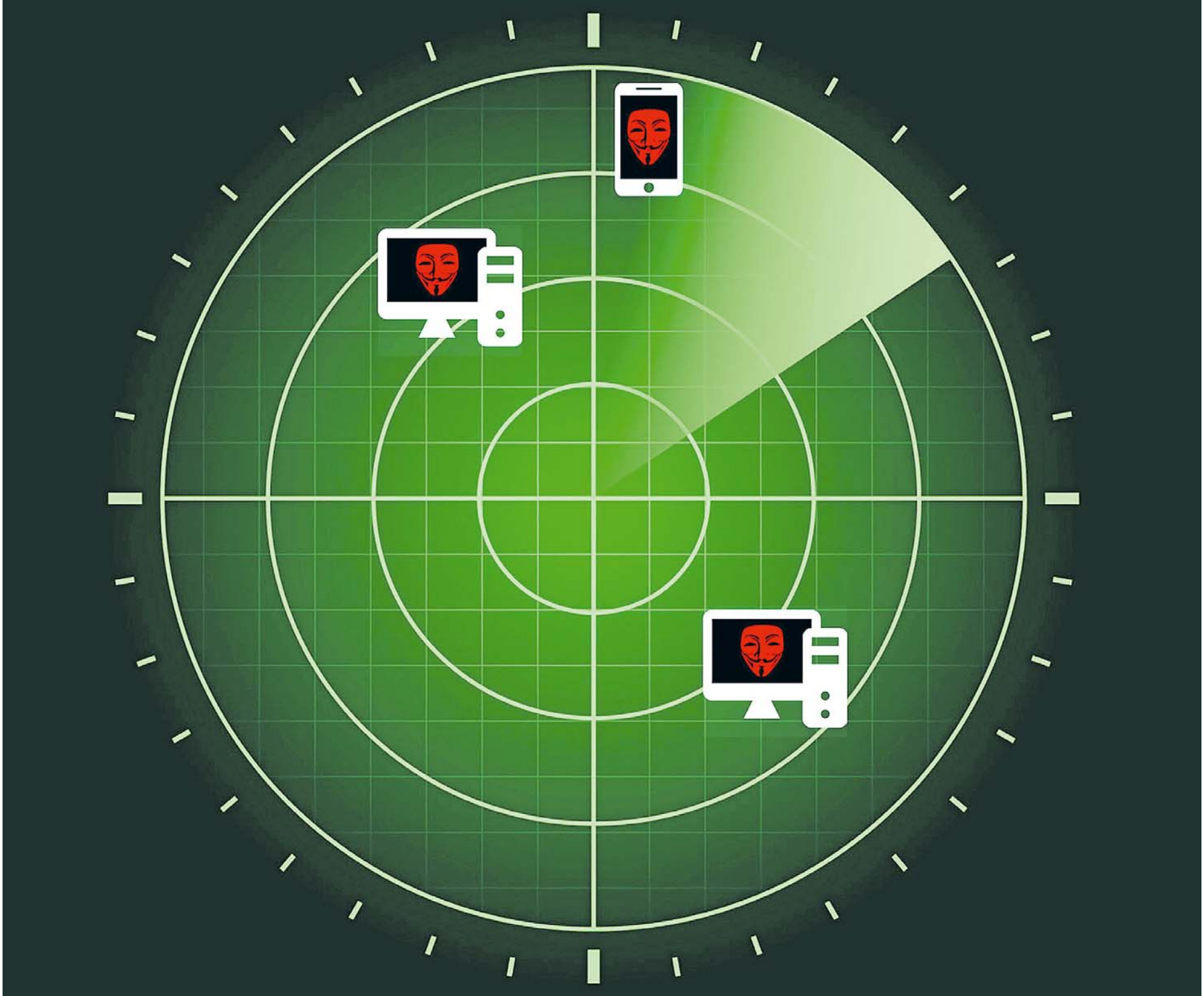
Handelsblatt
WOCHENENDE 22./23./24. OKTOBER 2021, NR. 205
*

IT-Sicherheit

Angriff aus dem Dunkeln



Eine beispiellose Welle von Cyberattacken trifft derzeit deutsche Fabriken, Krankenhäuser und Behörden. Hackerbanden erpressen Millionenbeträge – die Ermittler können meist nur zuschauen.

Getty Images [M]

Christof Kerkmann, Kevin Knitterscheidt, Lars-Marten Nagel, Michael Verfürden
Düsseldorf, Berlin, San Francisco

An einem Dienstag um 7 Uhr in der Früh entwickelten die Drucker der Softing AG plötzlich ein Eigenleben. In allen Büros und Gängen ratterten gleichzeitig die Geräte los. Zeile für Zeile druckten sie die Botschaft der Erpresser aus: „Your network was ATTACKED, your computers and servers were LOCKED, your private data was DOWNLOADED“, stand auf den Blättern.

Das Firmennetzwerk attackiert, die Rechner blockiert, die Unternehmensdaten abgegriffen: Die rund 400 Mitarbeiter des Industrie-Zulieferers aus Haar bei München fühlten sich an diesem 20. Oktober 2020, als wären sie in einen Thriller geraten.

Unterschrieben war die Botschaft mit „Egregor“. Der Name entstammt okkulten Lehren und bezeichnet die kollektive Energie einer Gruppe. Egregor verlangte drei Millionen Euro Lösegeld von der Softing AG, zu zahlen in der Digitalwährung Bitcoin. Im Gegenzug bot sie die Entschlüsselung der Daten und „volle Vertraulichkeit“. Falls kein Geld fließe, werde Egregor die sensiblen Firmendaten veröffentlichen.

„Im ersten Moment fühlt man sich, als hätte man die Kontrolle über die Firma verloren“, erinnert sich Ernst Homolka, Vorstand für Finanzen und Personal bei Softing. Allerdings hatte der Manager einen Notfallplan in der Schublade, inklusive Kontakt zu einem IT-Dienstleister. Innerhalb von zwei Stunden sei ein Notfallteam des IT-Dienstleisters Corporate Trust am Firmensitz gewesen, berichtet Homolka. Dann habe die Abwehrschlacht gegen die Erpresser begonnen.

Schnell stellte sich heraus: Begonnen hatte der Angriff um zwei Uhr in der Nacht. Egregor hatte alle Dateien in den Windows-Systemen des Unternehmens heruntergeladen und verschlüsselt – und so die digitale Macht über die Firma übernommen. Drucker, Korrespondenzen, Dokumente, Kontaktdaten, selbst die internetbasierten Festnetztelefone: Kaum etwas war mehr zugänglich, fast nichts funktionierte.

Szenen wie bei der Softing AG, die vor allem Hard- und Softwarelösungen für die Automobilindustrie liefert, spielen sich weltweit in unzähligen Unternehmen ab. „Das vergangene Jahr war geprägt von einer deutlichen Ausweitung cyberkrimineller Erpressungsmethoden“, warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) am Donnerstag. Im frisch veröffentlichten Jahresbericht 2020 bezeichnet die Behörde die digitalen Erpressungen als „größte Bedrohung“ für die Cybersicherheit in Deutschland. Die Fachleute sprechen bei solchen Erpressungen von Ransomware-Angriffen, darin steckt das englische Wort für Lösegeld: „ransom“.

Laut BSI verschlüsseln Kriminelle immer häufiger Daten von Unternehmen und Institutionen in ausgefeilten mehrstufigen Angriffen, um anschließend Geld für deren Freigabe zu erpressen. Die Zahl der Ransomware-Angriffe steigt seit Jahren. Im ersten Halbjahr 2021 waren es laut IT-Sicherheitsdienstleister Sonicwall weit mehr als 305 Millionen und damit so viele wie im gesamten Vorjahr. Am stärksten betroffen seien die USA, Großbritannien und Deutschland. Der Technologieverband Bitkom warnte die deutsche Wirtschaft unlängst vor einer „besorgniserregenden Wucht“.

Warum sind die Cyberkriminellen so erfolgreich? Wer steckt hinter den Attacken? Und wie gehen die betroffenen Organisationen am besten mit ihnen um? Das Handelsblatt hat zahlreiche Erpressungsfälle analysiert, Gerichtsakten gelesen und mit Opfern, Polizisten und Staatsanwälten gesprochen. Die Ermittler zeichnen das Bild einer globalen Epidemie, die gerade erst ihren Anfang nimmt – und bei deren Bekämpfung die Behörden erschreckend machtlos sind.

Die Täter sind meist global operierende Banden, die auf eine eigene Zulieferbranche zurückreifen können. Spezialisierte Programmierer liefern die nötige Ransom-Software, und auch die Erpressung selbst lässt sich auslagern – gegen Erfolgsbeteiligung. Welche Summen inzwischen im Spiel sind, hat IT-Sicherheitsspezialist Coveware für die Hackergruppe REvil kalkuliert: Allein im ersten Halbjahr 2021 soll sie knapp 100 Millionen Dollar Lösegeld kassiert haben.

Für einen erfolgreichen Angriff brauchen die Cyber-Erpresser nur einen gefrusteten Mitarbeiter, der einen USB-Stick in den richtigen Rechner steckt oder die entscheidenden Zugangsdaten kennt. Noch einfacher wird die Digitalattacke bei den erschreckend vielen Unternehmen, die ihre IT-Sicherheit nicht im Griff haben. Dann reicht schon ein unvorsichtiger Angestellter, der auf einen infizierten E-Mail-Anhang klickt (Wie Unternehmen sich am besten gegen Cybererpressungen wappnen können und wie sie sich im Ernstfall verhalten sollten, lesen Sie auf Seite 51).

„Im ersten Moment fühlt man sich, als hätte man die Kontrolle über die Firma verloren.“

Ernst Homolka,
Vorstand für Finanzen und Personal bei der Softing AG

```
*
-----------------
| What happened? |
-----------------

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

---------------------
| What does it mean? |
---------------------

It means that soon mass media, your partners and clients WILL KNOW about your

-------------------------
| How it can be avoided? |
-------------------------

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the

----------------------------------------
| What if I do not contact you in 3 days? |
----------------------------------------

If you do not contact us in the next 3 DAYS we will begin DATA publication.

----------------------------
| I can handle it by myself |
----------------------------

It is your RIGHT, but in this case all your data will be published for public

------------------------------
| I do not fear your threats! |
------------------------------

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR
That is the EXACT AMOUNT of money you will spend for recovery and payouts beca

--------------------------
| You have convinced me! |
--------------------------

Then you need to CONTACT US, there is few ways to DO that.

I. Recommended (the most secure method)

   a) Download a special TOR browser: https://www.torproject.org/
   b) Install the TOR browser
   c) Open our website with LIVE CHAT in the TOR browser: http://egregor4u5ipd
   d) Follow the instructions on this page.

II. If the first method is not suitable for you

   a) Open our website with LIVE CHAT: https://egregor.top/2315BA555CDEECF6
   b) Follow the instructions on this page.

Our LIVE SUPPORT is ready to ASSIST YOU on this website.

--------------------------------------
| What will I get in case of agreement |
--------------------------------------

You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTIN
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for

And the FULL CONFIDENTIALITY ABOUT INCIDENT.

-------------------------------------------------------------------------------
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
4YHjlyyptqiEulH1F8y4XCHUIN6R92vg0zAhup2g+KcTvP+weGX6ryzR3wmMkyPrjuMO4Sdf3MXxC2
---EGREGOR---
```

Erpresserschreiben an die Softing AG (Auszug): Detaillierte Anweisungen für die Kontaktaufnahme.

Ausgebaute Server der Softing AG: Innerhalb weniger Stunden stand die Gegenstrategie.

Softing AG (3)

1 Die Opfer: Angriff auf die digitale Gesellschaft

Die Liste der geschädigten Unternehmen ist prominent besetzt.

- Die Finanzbranche erwischte es Anfang 2020: Mitarbeiter von Travelex mussten wieder zu Stift und Papier greifen, um weltweit Tausende Kunden zu bedienen. Hacker hatten mit Ransomware die Systeme des Devisenhändlers lahmgelegt. Lösegeldforderung: sechs Millionen Euro.

- Im Juni 2021 sah sich die im MDax gelistete Brenntag AG außer Gefecht gesetzt. Der Chemikalienhändler soll den Angreifern umgerechnet 4,4 Millionen US-Dollar Lösegeld gezahlt haben.

- Einen Monat später musste das Personal im Klinikum Wolfenbüttel zeitweise mit Klemmbrett und Kugelschreiber arbeiten, weil die IT nach einer Cyber-Erpressung stillstand.

- Die internationale Wirtschaftskanzlei CMS Hasche Sigle war im August gezwungen, alle Netzwerkverbindungen nach außen zu trennen. Ein Angriff habe dem Netzwerk der deutschen Standorte gegolten, teilte die Kanzlei mit.

- Selbst bei der Unternehmensberatung Accenture, die Kunden in Sachen IT-Sicherheit berät, drangen vor einigen Wochen Täter in die Systeme ein und spotteten anschließend über angeblich schwache Schutzmaßnahmen.

- Schlagzeilen machte auch der US-amerikanische Pipelinebetreiber Colonial, als er im Frühjahr nach einem Cyberangriff eine wichtige Versorgungsleitung für die Ostküste der USA außer Betrieb nehmen musste.

Der Direktor der US-Bundespolizei FBI, Christopher Wray, verglich die Bedrohung mit den Terroranschlägen vom 11. September. Nur dass der Behördenchef die Täter nicht im arabischen Raum vermutet – sondern größtenteils in Russland, wo der Kreml die Hacker angeblich gewähren lasse, solange sie nur im Ausland zuschlagen. Cyberangriffe könnten die Amerikaner jederzeit treffen, an der Zapfsäule oder wenn sie einen Hamburger kaufen, sagte Wray dem „Wall Street Journal“.

Spätestens der Fall Colonial zeigt: Es geht bei Ransomware-Erpressungen nicht nur um den finanziellen Schaden einiger Unternehmen. Gefährdet sind die Lebensgrundlagen einer industriellen Gesellschaft, zu denen eben auch die reibungslose Versorgung mit fossilen Brennstoffen zählt. Und wenn Kliniken Patienten wegschicken müssen, weil die IT nicht läuft, können sogar Menschen in Lebensgefahr geraten. FBI-Chef Wray: „Ich glaube, es gibt jetzt ein wachsendes Bewusstsein dafür, wie sehr wir alle gemeinsam in diesem Kampf stehen.“

Ein Kampf, der gerade erst beginnt. „Wir sind mittendrin in einer starken Digitalisierung – wenn wir da nicht die Informationssicherheit von vornherein mitdenken, werden wir große Herausforderungen haben“, sagt BSI-Präsident Arne Schönbohm. In der heutigen Zeit wird schließlich praktisch alles vernetzt, vom Auto übers Heizthermostat bis zum Beatmungsgerät.

Auch Angriffe auf IT-Dienstleister werden immer populärer, weil die Schadsoftware so gleich in mehrere Unternehmen gestreut werden kann.

Handelsblatt
WOCHENENDE 22./23./24. OKTOBER 2021, NR. 205

Als Hacker Mitte des Jahres den US-Dienstleister Kaseya angriffen, mussten in Schweden die Supermärkte von Coop schließen, weil deren Kassensystem nicht mehr funktionierte. In jedem Fall gilt: Ransomware-Banden nehmen bevorzugt große, finanzstarke Organisationen ins Visier. Das BSI spricht von „Big Game Hunting“, von Großwildjagd.

Krankenhäuser, Behörden, Industriebetriebe, Dienstleistungsunternehmen: Sie alle haben in den vergangenen Jahren ihre Prozesse immer stärker digitalisiert. Sind Rechner und Daten blockiert, geht nichts mehr. Viele zahlen daher lieber das Lösegeld, das mehrere Millionen Euro betragen kann, als sich auf lange Verhandlungen einzulassen. Jede dritte Organisation gehe auf die Lösegeldforderung ein, hat der IT-Sicherheitsspezialist Sophos ermittelt.

Dazu war die Softing AG nicht ohne Weiteres bereit. Das Unternehmen richtete im Keller der Firmenzentrale einen „War Room“ ein, ein Lagezentrum, in dem das eilig einbestellte Notfallteam des IT-Dienstleisters und das Softing-Management zusammenkamen. Ein großer Konferenztisch in der Mitte, eilig zusammengestöpselte Laptops, Bildschirme und Router auf den Schreibtischen drumherum. An der Seite Whiteboards, auf die Abwehrideen standen. Zum wichtigsten Kommunikationsmittel entwickelten sich die Smartphones der Firma. „Die waren von der Verschlüsselung nicht betroffen“, sagt Vorstand Ernst Homolka.

An ihrem provisorischen Arbeitsplatz, zwischen Kaffeekannen und Süßigkeiten, entdeckten die IT-Forensiker bald das Tatwerkzeug: Es war eine E-Mail mit einer Excel-Tabelle im Anhang. Als ein Softing-Mitarbeiter die Datei öffnete, startete er damit das Angriffsprogramm – und das lud heimlich weitere Software aus dem Internet nach. Die Hacker waren ins Firmennetzwerk eingedrungen.

Solche Angriffe nennen Fachleute „Phishing“. Sie sind ein häufiger Einfallsweg, bei dem die Hacker ihre Opfer, in diesem Fall den Softing-Mitarbeiter, zu dem einen verhängnisvollen Klick auf ein Attachment verleiten.

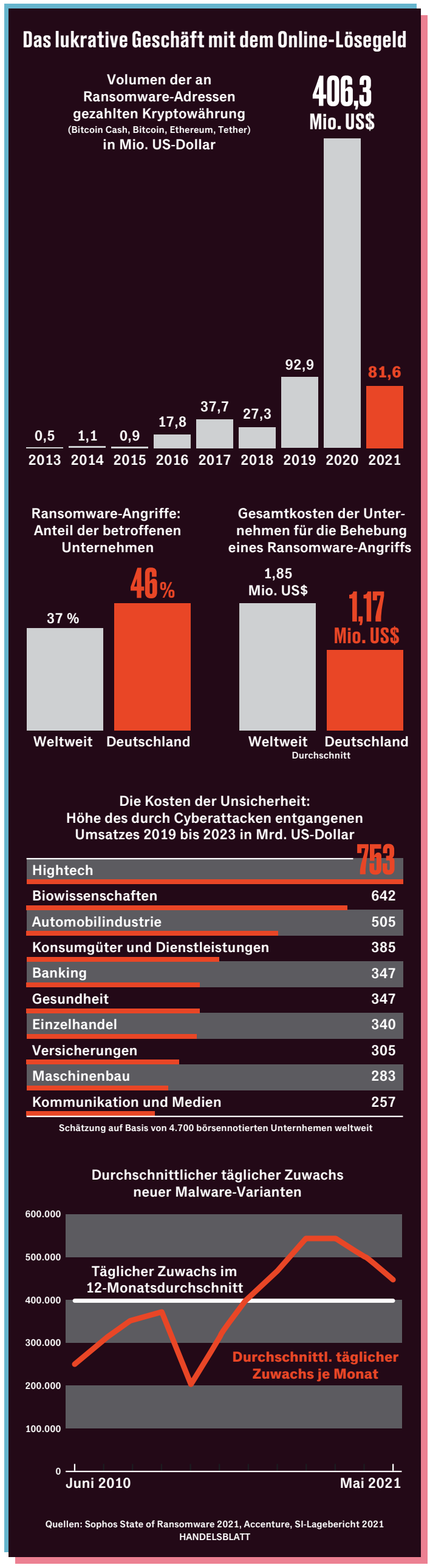
Innerhalb einiger Stunden verschlüsselten die Angreifer fast alle Softing-Systeme, die mit dem Betriebssystem Windows liefen. Glück für die Softing AG: Die Windows-Geräte kamen überwiegend für administrative Aufgaben zum Einsatz, die Entwickler arbeiteten zum Großteil auf Linux-Servern. „Den Tätern war es offenbar zu aufwendig, ihre Software für das andere Betriebssystem zu übersetzen“, sagt Homolka. Die wichtigsten Geschäftsgeheimnisse der Softing AG blieben dadurch geheim, immerhin. Erstes Durchatmen im „War Room“.

2 Die Schäden: Mangelnde Vorsorge rächt sich

Nicht immer geht es so glimpflich aus. Die durchschnittlichen Lösegeldforderungen an Unternehmen bei Ransomware-Erpressungen lag im ersten Halbjahr 2021 bei 5,3 Millionen US-Dollar. Das ist mehr als viermal so viel wie der Durchschnittswert im Jahr 2020, wie das kalifornische IT-Sicherheitsunternehmen Palo Alto Networks ermittelt hat. Die durchschnittliche Zahlung wiederum stieg um 82 Prozent auf 570.000 US-Dollar.

Oft noch teurer als die Lösegelder sind die Zwangspausen für die Betriebe: Die Ausfallzeiten belaufen sich im Schnitt auf 21 Tage, können sich mitunter aber auch über Monate ziehen. Die Kosten hat der Versicherer Hiscox am Beispiel eines exportstarken Mittelständlers mit 150 Millionen Euro Umsatz nachgezeichnet, bei dem der Betrieb mehrere Wochen lang eingeschränkt war: Allein der Schaden durch den Ertragsausfall belief sich auf 1,7 Millionen Euro. Krisenmanagement, IT-Forensik und die Wiederherstellung der Daten schlugen mit 650.000 Euro zu Buche, ebenso der Aufbau eines Ersatz-IT-Systems mit 550.000 Euro.

Inklusive Ausgaben für einen Datenschutzanwalt, Krisenkommunikation und die Information der Kunden summierte sich der Aufwand auf drei Millionen Euro. Da kann ein kühl kalkulierender Geschäftsmann schnell auf die Idee kommen, lieber gleich auf die Forderung der Erpresser einzugehen.



Am billigsten ist es, den Erpressern das Eindringen möglichst schwer zu machen. Doch selbst Unternehmen mit großer IT-Abteilung kommen kaum hinterher, ihre komplexen und vernetzten Systeme zu schützen. In kleinen Organisationen mangelt es erst recht an Budget und Personal für den Schutz der IT. Ein Drittel der Mittelständler mit bis zu 250 Mitarbeitern hat keinen Verantwortlichen für die IT-Sicherheit, jedes fünfte Unternehmen verzichtet auf eine wöchentliche Sicherung der Daten, wie der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) erhoben hat. Einen Notfallplan in der Schublade oder zumindest einen auf Notfälle spezialisierten IT-Dienstleister bei der Hand hat nur jedes zweite Unternehmen. Dabei können bereits solche elementaren Vorsichtsregeln Erpresserattacken zwar nicht verhindern, aber doch ihre Folgen wesentlich abmildern.

Viele Manager seien verblüfft, dass ausgerechnet ihr Unternehmen angegriffen werde, sagt Mike Hart, Vizepräsident für Zentral- und Osteuropa beim amerikanischen IT-Sicherheitsunternehmen Fire-Eye. „Mit dieser Geisteshaltung werden sie für Hackergruppen zur leichten Beute.“

Zwischen dem, was an IT-Sicherheit möglich ist, und dem, was tatsächlich umgesetzt wird, hat sich eine bedenkliche Kluft aufgetan. Während die Anbieter von IT-Sicherheitstechnologie für Abwehrsysteme mit Künstlicher Intelligenz werben und klangvolle Konzepte wie „Zero Trust“ propagieren, haben viele IT-Abteilungen schon Probleme damit, all die Updates einzuspielen, mit denen Microsoft Sicherheitslücken in seinen Systemen wie Windows oder Sharepoint schließt. Von den Hunderten Programmen anderer Hersteller, die in Unternehmen zum Einsatz kommen, ganz zu schweigen.

„Cybersicherheit ist schwer – zu schwer“, meint der IT-Sicherheitsspezialist Kevin Beaumont, der nach einer Station bei Microsoft nun beim britischen Modehändler Arcadia das „Security Operations Centre“ leitet. Systeme für Identitäts- und Berechtigungsmanagement beispielsweise seien für viele Organisationen schlicht zu kompliziert. Manche Hersteller lieferten zudem Produkte von schlechter Qualität, die neue Sicherheitslücken aufrissen.

Als wäre das nicht genug, kommt nun auch noch die Coronakrise hinzu, Millionen Menschen greifen vom heimischen Küchentisch oder Arbeitszimmer aus auf die IT ihres Arbeitgebers zu. Wenn das Homeoffice zum Firmennetz gehört – teils mit privaten PCs, oft mit schwachen Passwörtern fürs WLAN, fast immer mit neuen Diensten wie Teams, Slack oder Zoom –, wird es noch schwieriger, Angriffe abzuwehren.

3 Die Täter: Viele Spuren führen nach Osten

Mitte Juni stellte die ukrainische Polizei einen fünfminütigen Clip auf Youtube. Er zeigt einen vermummten Polizisten, der breitbeinig vor einer Haustür steht, in der Hand eine glühend rote Flex, die Funken schlägt. Links und rechts von ihm stehen Spezialkräfte mit Maschinenpistolen.

Gemeinsam mit südkoreanischen Ermittlern durchsuchten die ukrainischen Behörden 21 Immobilien im Großraum Kiew. Sie stellten elektronische Geräte, Plastiksäcke voller Bargeld und mehrere Luxusautos sicher. Die Polizisten nahmen sechs Personen fest. Sie sollen zu der Ransomware-Gruppe gehören, die hinter der Schadsoftware „Cl0p“ steht.

Die Bande hatte in den vergangenen Monaten immer wieder Schlagzeilen gemacht. Zu ihren Opfern gehörten die US-Universität Stanford, der niederländische Ölkonzern Shell und die internationale Kanzlei Jones Day. Auch in Deutschland schlug „Cl0p“ zu. Die Gruppe griff unter anderem den SAP-Konkurrenten Software AG und die Technischen Werke Ludwigshafen an. Ermittler beziffern den von Cl0p verursachten Gesamtschaden mit 500 Millionen Dollar.

Sosehr die ukrainische Polizei den Coup zelebrierte, so sehr zeigt der Fall auch das Dilemma, vor dem Behörden weltweit stehen. Wenige Tage nach den Razzien veröffentlichte „Cl0p“ die Daten neuer Opfer. Die Ermittler in der Ukraine hatten offenbar nur die Geldwäscher der Bande erwischt.

Klinikum Wolfenbüttel, Softing AG, Xinhua / eyevine / laif, Brenntag AG

Erpressungsopfer Brenntag, Colonial, Klinikum Wolfenbüttel, Softing (im Uhrzeigersinn): Es geht nicht nur um Geld, sondern auch um die Energieversorgung und im Extremfall sogar um Menschenleben.

Experten glauben, dass der harte Kern der „Cl0p"-Gruppe in Russland sitzt. Im Gegensatz zur Ukraine ist der Kreml bislang nicht gewillt, gemeinsam mit dem Rest der Welt gegen die Cyberkriminellen vorzugehen. Die Experten von Malwarebytes haben die öffentlich bekannten Attacken im ersten Halbjahr 2021 ausgewertet. Das Ergebnis: Die 13 aktivsten Erpresserbanden haben ihre Schadsoftware so programmiert, dass sie Computer in Ländern der Gemeinschaft Unabhängiger Staaten (GUS) verschont. In der GUS haben sich Nachfolgestaaten der Sowjetunion zusammengeschlossen. Russland war ein Gründungsmitglied.

Auch die „Cl0p"-Gruppe agiert verdächtig russlandfreundlich. Beobachter haben festgestellt, dass die Hacker an russischen Feiertagen nicht arbeiten. Zudem prüft ihre Schadsoftware, ob infizierte Rechner auf Russisch oder auf die Sprache eines mit Moskau verbündeten Landes eingestellt sind. Ist das der Fall, löscht sich das Programm von selbst. Die US-Regierung wirft Russlands Präsident Wladimir Putin vor, beide Augen zuzudrücken, solange die Ransomware-Attacken andere Staaten treffen. US-Präsident Joe Biden forderte Putin deshalb auf, härter durchzugreifen.

Ohne nennenswertes Risiko, für die Erpressungen tatsächlich im Gefängnis zu landen, nähert sich die ökonomische Logik der Ransomware-Banden der von normalen IT-Unternehmen an. Weil sich das Geschäft lohnt, steigen die Investitionen der Hacker – etwa für die Entwicklung von Einbruchs- und Verschlüsselungswerkzeugen oder für den Kauf von Informationen über Sicherheitslücken auf dem Schwarzmarkt. „Das wird rein betriebswirtschaftlich betrachtet. Man investiert mehr, bekommt aber auch viel mehr heraus", sagt BSI-Präsident Schönbohm.

So beobachtet das BSI, dass es Angriffsprogramme gibt, die Sicherheitslücken von gleich mehreren populären Systemen wie Windows, Microsoft Office oder Citrix ausnutzen. Das Repertoire der Kriminellen erinnert an einen Werkzeugkasten, in dem Einbrecher neben ihrem Brecheisen eine Dietrich-Sammlung, eine Bohrmaschine oder eben die digitale Flex transportieren: Irgendetwas wird schon funktionieren.

Zudem sind die Hacker flexibel und reagieren innerhalb von Tagen: Als am Jahresanfang bekannt wurde, dass es im E-Mail-System Exchange von Microsoft eine schwerwiegende Sicherheitslücke gab, die Tausende Unternehmen in aller Welt betraf, kursierte schon bald darauf eine passende Ransomware. Gelegenheit macht Erpresser – mit dem Prinzip „Versuch und Irrtum" probieren die Gruppen neue Geschäftsmodelle aus. Was funktioniert, wird von anderen kopiert und adaptiert.

4 Die Dienstleister: Erpressungssoftware zum Mieten

Vertiefte IT-Kenntnisse sind dabei nicht unbedingt erforderlich. Jörg Asma, Partner bei PwC Deutschland, sagt über Cyber-Erpresser: „Entgegen vielfachen Erwartungen müssen Kriminelle keine Hacker sein." Im Internet gebe es zahlreiche Foren, wo man kriminelle Dienstleistungen einkaufen könne – wenn man nur ausreichend Bitcoin hat. „Crime as a Service" nennen IT-Sicherheitsspezialisten das Phänomen.

Asma sitzt im Kölner Büro der Wirtschaftsprüfungsgesellschaft, hinten die Fenster zum Rhein, vorn sein großer Bildschirm. Er scrollt durch die Angebote in einem Untergrundforum: Ein Nutzer bietet den „zuverlässigsten Service", Facebook-Nutzerkonten zu hacken. Ein anderer verspricht einen „Crypto Pump & Dump Bot", also ein Programm, das automatisch den Preis einer Kryptowährung manipulieren soll.

Dazwischen steht ein Angebot für „Ransomware as a Service": Erpressungssoftware zum Mieten. Man suche „zuverlässige und hochmotivierte Partner", es gehe um eine Partnerschaft „zum beiderseitigen Vorteil", heißt es in dem Inserat. Ein Programmierer stellt die Erpressungssoftware zur Verfügung, jemand anders verbreitet sie – und das Lösegeld wird geteilt.

Das Programm werde kontinuierlich weiterentwickelt und laufe auf allen Windows-Systemen. Es umgehe die meisten Schutzmechanismen und nutze einen fortschrittlichen Verschlüsselungsalgorithmus. Eine Website in zwölf Sprachen erläutert den Opfern, was passiert ist und wie sie das Lösegeld zahlen können. Und wenn der Partner Fragen hat, könne er sich per Chat melden, auf Englisch oder Russisch.

„Das läuft hoch arbeitsteilig ab", sagt Asma. Auch alles, was es für Cyberangriffe braucht, könne man kaufen oder mieten. Gekaperte PCs zum Beispiel, die massenhaft E-Mails verschicken, Botnetze genannt. Die gebe es „mit fehlerfreier Logistik", sagt der IT-Experte, einschließlich Statistiken, wie viele Nachrichten verschickt und angeklickt werden.

Die meisten Marktplätze der Untergrundwirtschaft liegen im Darknet, einem versteckten Teil des Internets. Wer sich dort umsehen will, benötigt einen speziellen Browser, der die digitalen Spuren verwischt.

Die Gruppe „Lockbit 2.0" , die ebenfalls aus dem russischsprachigen Raum operieren soll, hat „Ransomware as a Service" perfektioniert. Sie programmiert die Schadsoftware und stellt die Infrastruktur für die Kommunikation mit betroffenen Organisationen sowie für die Bezahlung der Lösegelder.

Für den Einbruch selbst engagiert sie aber Partner. Die bekommen dafür einen Anteil des Lösegelds, nach Angaben der auf Ransomware spezialisierten Sicherheitsfirma Emsisoft bis zu 80 Prozent. „Das Einzige, was Sie tun müssen, ist, sich Zugang zum Kernserver zu verschaffen, während Lockbit 2.0 den Rest erledigt", werben die Erpresser auf ihrer Website im Darknet.

Ermittler nennen externe Helfer „Affiliates". Mit ihnen lässt sich das Geschäftsmodell Cyber-Erpressung skalieren – ganz ähnlich wie im Geschäft mit legalen IT-Dienstleistungen. Unter den Banden ist ein regelrechter Kampf um die talentiertesten Geschäftspartner entbrannt. „Lockbit

Handelsblatt
WOCHENENDE 22./23./24. OKTOBER 2021, NR. 205

2.0“ trommelt deshalb auf unterschiedlichen Kanälen für die eigene Organisation – und gegen die Konkurrenz.

Als digitale Litfaßsäule dienen ihr auch infizierte Rechner. Die Schadsoftware tauscht automatisch das Hintergrundbild aus. In schwarzer Schrift auf weißem Grund steht dann, dass die „Lockbit“-Gruppe Personen rekrutiert, die Zugang zu den „wertvollsten Daten“ einer Firma verschaffen können – Branche und Größe egal. Wer „Millionen US-Dollar verdienen“ will, könne sich jederzeit über einen anonymen Messenger melden.

Um eine noch größere Reichweite zu erzielen, gibt die Gruppe sogar Interviews. Russische Blogger und Youtuber veröffentlichen die anonymisierten Gespräche, die sich vor allem um angebliche Wettbewerbsvorteile gegenüber anderen Banden drehen. Die Experten der Firma Advintel sprechen von „Ransomware Promo“, die neue Partner locken soll.

Diese Art von Öffentlichkeitsarbeit, sagen die Experten, sei bei professionellen Gruppen inzwischen üblich. Ein Mitglied von „Lockbit 2.0“ prahlte erst Ende August in einem Interview: „Niemand kann uns schlagen, wenn es um die Geschwindigkeit der Verschlüsselung geht.“ Das steigere die Produktivität und minimiere das Risiko – auch für potenzielle Geschäftspartner.

Um moralische Zweifel möglicher Affiliates aus dem Weg zu räumen, präsentieren sich die Kriminellen dabei als eine Art Robin Hood der digitalen Unterwelt. „ACHTUNG!!! Wir haben nie Krankenhäuser, Pflegeheime oder Wohltätigkeitsorganisationen angegriffen und werden dies auch nicht tun“, heißt es auf der Website von „Cl0p“. Angriffe auf Pharmakonzerne seien aber okay. Sie seien schließlich „die Einzigen, die von der Pandemie profitieren“.

Auch die Gruppe „Lockbit 2.0“ gibt vor, eine ethische Agenda zu haben. „Medizinische und Bildungseinrichtungen sowie Wohltätigkeitsorganisationen werden von uns nicht angegriffen“, sagte ein Mitglied der Gruppe, das einem russischen Blogger kürzlich ein Interview gegeben hat. „Wir greifen nur Geschäftshaie an, die so sind wie wir.“

„Lockbit 2.0“ machte Mitte August Schlagzeilen, als die Gruppe Tausende Dokumente der IT-Beratungsfirma Accenture mit Sitz im irischen Dublin veröffentlichte. Der Angriff war nicht nur besonders dreist, weil er einen der größten Dienstleister für Cybersicherheit traf. Er zeigt auch, dass Unternehmen eine zusätzliche Gefahr fürchten müssen – eine, die in den eigenen Reihen lauert.

Die Gruppe spricht gezielt Insider in Konzernen an. Sie sollen den Zugang zum Firmennetzwerk verschaffen und dafür einen Teil der Beute bekommen. Ausgerechnet bei Accenture soll das geklappt haben. „Ich hoffe, dass ihre Dienste besser sind, als das, was ich als Insider gesehen habe“, zitiert die Gruppe den angeblichen Helfer bei Accenture auf ihrer Darknet-Website.

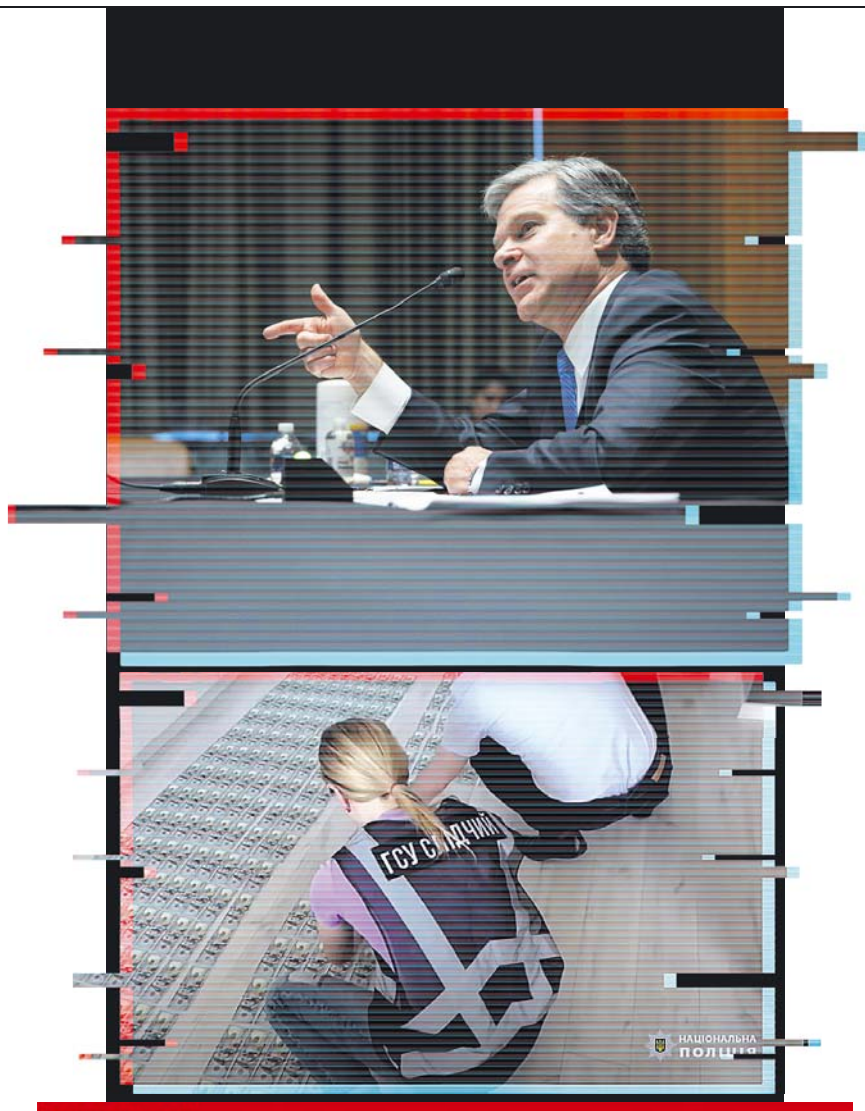
5 Die Ermittler: Geschnappt werden meist nur Amateure

Die USA haben im Mai einen Russen abgeschoben, der versucht hatte, einen Mitarbeiter des US-Elektroautobauers Tesla zu bestechen. Der Russe bot dem Tesla-Angestellten 500.000 US-Dollar dafür, eine Schadsoftware in das Netzwerk der Gigafactory in Nevada einzuspielen. Der Russe gab an, mit einer großen Ransomware-Gruppe zusammenzuarbeiten. Tesla-Chef Elon Musk nannte den Plan einen „ernsthaften Angriff“.

Um überhaupt mal einen solchen Fahndungserfolg gegen die globale Ransomware-Szene zu erzielen, brauchen die Ermittlungsbehörden technisches Know-how, internationale Zusammenarbeit, viel Personal und eine erhebliche Portion Glück. Und selbst dann werden meist nur die Handlanger oder Amateure geschnappt.

So auch bei einem der spektakulärsten je aufgeklärten Ransomware-Angriffe. Es ging zwar nur um die überschaubare Forderung von 61.000 US-Dollar. Doch der politische Druck war hoch: Die Weltmacht USA fühlte sich angegriffen.

Die Polizei in Washington, D.C. hatte wenige Tage vor der Amtseinführung von Donald Trump die Kontrolle über 126 Überwachungskameras in der Stadt verloren. Hacker hatten die Steuerungscomputer verschlüsselt. Vor dem Großereignis im Jahr 2017, zu dem Hunderttausende Besucher erwartet wurden, war die Ordnungsmacht erblindet.



FBI-Direktor Christopher Wray, ukrainische Razzia gegen die Hackerbande Cl0p, Text der ersten Digital-Erpressung von 1990: Ein Gewerbe, fast so alt wie der PC selbst.

Noch während der Angriff lief, übernahm der United States Secret Service (USSS) die Ermittlungen. Die Agenten des Secret Service sind unter anderem für den Schutz des Präsidenten zuständig. Bald stand fest, dass weder russische Hacker die nationale Sicherheit bedrohten noch aggressive Trump-Gegner die Amtseinführung sabotieren wollten: Zwei Kleinkrimelle hatten sich schlicht verhoben, wie Gerichtsdokumente belegen.

Mihai I. und Eveline C. waren keine 30 Jahre alt und schlugen sich mit digitalem Identitätsdiebstahl und Kreditkartenbetrug durch. Vom Umstieg auf digitale Erpressung versprach sich das Paar aus Rumänien höhere Gewinne. Den Schadcode hatte es in der „Underground Economy“ gemietet. Sie mussten dafür eine Gebühr von bis zu 30 Prozent der Einnahmen weiterleiten.

Die mit dem Schadcode infizierten E-Mails verschickten die beiden an die Liste mit 179.616 E-Mail-Adressen, die sie in einem Forum gekauft hatten. Dass darauf auch Polizeicomputer in Washington standen, dürften sie nicht geahnt haben. Auch rächte sich für die Täter, dass sie miteinander, aber auch mit infizierten Rechnern, über Google-Accounts kommunizierten.

Ausgerechnet Google, beheimatet in den USA: Leichter hätten es die beiden Möchtegern-Erpresser dem Secret Service nicht machen können. Stück für Stück puzzelten die Fahnder IP-Adressen und andere Informationen zusammen. Eine Bestellung bei „Andys Pizza“ in Bukarest brachte den Durchbruch. Im Dezember 2017 nahmen Fahnder das Paar fest.

Ein Jahr später gestand Eveline C. in einem Deal mit der US-Justiz. Weil sie auspackte und nur eine Nebenrolle gespielt haben soll, wurde sie abgeschoben. Mihai I. sitzt derzeit wegen anderer Taten in Rumänien für vier Jahre in Haft.

5,3

Millionen US-Dollar
betrug im ersten Halbjahr 2021 die durchschnittliche Lösegeldforderung von Ransomware-Erpressern.

Quelle: Palo Alto Networks

Doch es ist ein besonderer Fall. Die Täter waren Amateure, und es ging um die „Nationale Sicherheit“ der Weltmacht USA. Dass staatliche Behörden mit vergleichbarer Vehemenz Cyberkriminellen nachsetzen, die Firmen erpressen, sollten die Opfer besser nicht erwarten.

6 Fazit: Nur wer sich selbst schützt, verhindert das Schlimmste

Die Computerkriminalität ist dabei fast so alt wie der PC selbst. Erste Computerviren verbreiteten sich bereits in den 1980er-Jahren über Disketten mit illegalen Softwarekopien. Im Jahr 2000 überschrieb ein vermeintlicher Liebesbrief, millionenfach per E-Mail verschickt, Daten auf den Festplatten der Empfänger und legte viele E-Mail-Server lahm.

Dann kamen Banden hinzu, die Bankdaten stehlen. Hochstapler, die sich als nigerianische Prinzen ausgeben. Gelegenheitsganoven, die unter falschem Namen Smartphones bestellen. Und hochprofessionelle Auftragsspione, die Nationen oder Konzerne ausforschen.

Mit der Ransomware hat die Internetkriminalität seit etwa 2017 ein neues Level erreicht. Die digitale Erpressung wurde zur weltweiten Plage und hat wie andere Seuchen inzwischen zahlreiche Mutationen hinter sich. Es war tatsächlich ausgerechnet ein Evolutionsbiologe, der den mutmaßlich ersten Ransom-Virus in die Welt setzte.

Das geschah im Jahr 1989, als Joseph Popp ein Job bei der Weltgesundheitsorganisation WHO versagt blieb. Aus Frust habe er weltweit 20.000 manipulierte Disketten an Wissenschaftler verschickt, heißt es. Angeblich sollten die 5,25-Zoll-Datenträger Informationen zur Immunschwächekrankheit Aids beinhalten.

Stattdessen infizierten die Disketten die Computersysteme mit Schadcode. 89-mal konnten die Rechner eingeschaltet werden, beim 90. Mal waren sie eingefroren. Eine Botschaft auf dem Bildschirm versprach die Freigabe der Festplatten nur gegen eine dreistellige Lizenzgebühr in US-Dollar, die per Scheck oder internationaler Zahlungsanweisung an ein Postfach in Panama zu schicken sei.

Die Behörden fassten den Biologen und klagten ihn in Großbritannien an. Popp zog sich im Gerichtssaal Kondome über die Nase und drehte sich Lockenwickler in den Bart, angeblich um sich gegen Strahlung zu schützen. Das Verfahren wurde aus Rücksicht auf seinen psychischen Gesundheitszustand eingestellt.

Popp fehlten damals zwei entscheidende Instrumente, die Cyber-Erpresser heute so erfolgreich machen: Digitalwährungen wie Bitcoin, mit denen die Täter bei Lösegeldzahlungen anonym bleiben können – und das Internet, mit dem sich Viren verbreiten lassen, ohne durch Datenträger Spuren zu hinterlassen. Wenn die Tätergruppen dann noch untereinander via Darknet kommunizieren und ihr Geschäft aus einem Staat heraus betreiben, der Cybererpresser bestenfalls halbherzig verfolgt, können die Ermittler in den meisten Fällen nur auf Fehler der Täter hoffen, um sie zu schnappen.

Angesichts dieser Asymmetrie gilt für Unternehmen bis auf Weiteres: Nur wer sich selbst schützt, kann das Schlimmste verhindern.

Die Softing AG ist ein gutes Beispiel dafür. Sie kam glimpflich davon, weil sie auf den Angriff vorbereitet war. Lösegeld zu zahlen sei zu keiner Zeit eine ernsthafte Erwägung gewesen, sagt Vorstand Homolka. „Wir haben da nicht lange nachdenken müssen. Auch weil unsere Daten alle 24 Stunden auf Magnetband als Back-up gespeichert werden.“ Regelmäßige Sicherheitskopien gelten als beste Vorbereitung auf den Ernstfall. Die Softing AG war zudem gegen Ransomware-Angriff versichert.

Während die Chatnachrichten mit den Erpressern hin und her flogen, sei den Chefs immer klarer geworden, „dass die erbeuteten Daten weitgehend irrelevant waren“. Erleichtert begannen sie mit der Wiederherstellung der Systeme. Homolka: „Am Ende hat uns das Neuaufsetzen unserer Systeme deutlich weniger gekostet, als eine Entschlüsselung der Systeme wie von den Hackern angeboten“.

Aus dem „War Room“ der Softing AG wurde schon bald wieder ein normaler Besprechungsraum.

Wikipedia, Cyberpolice Ukraine, imago images/UPI Photo