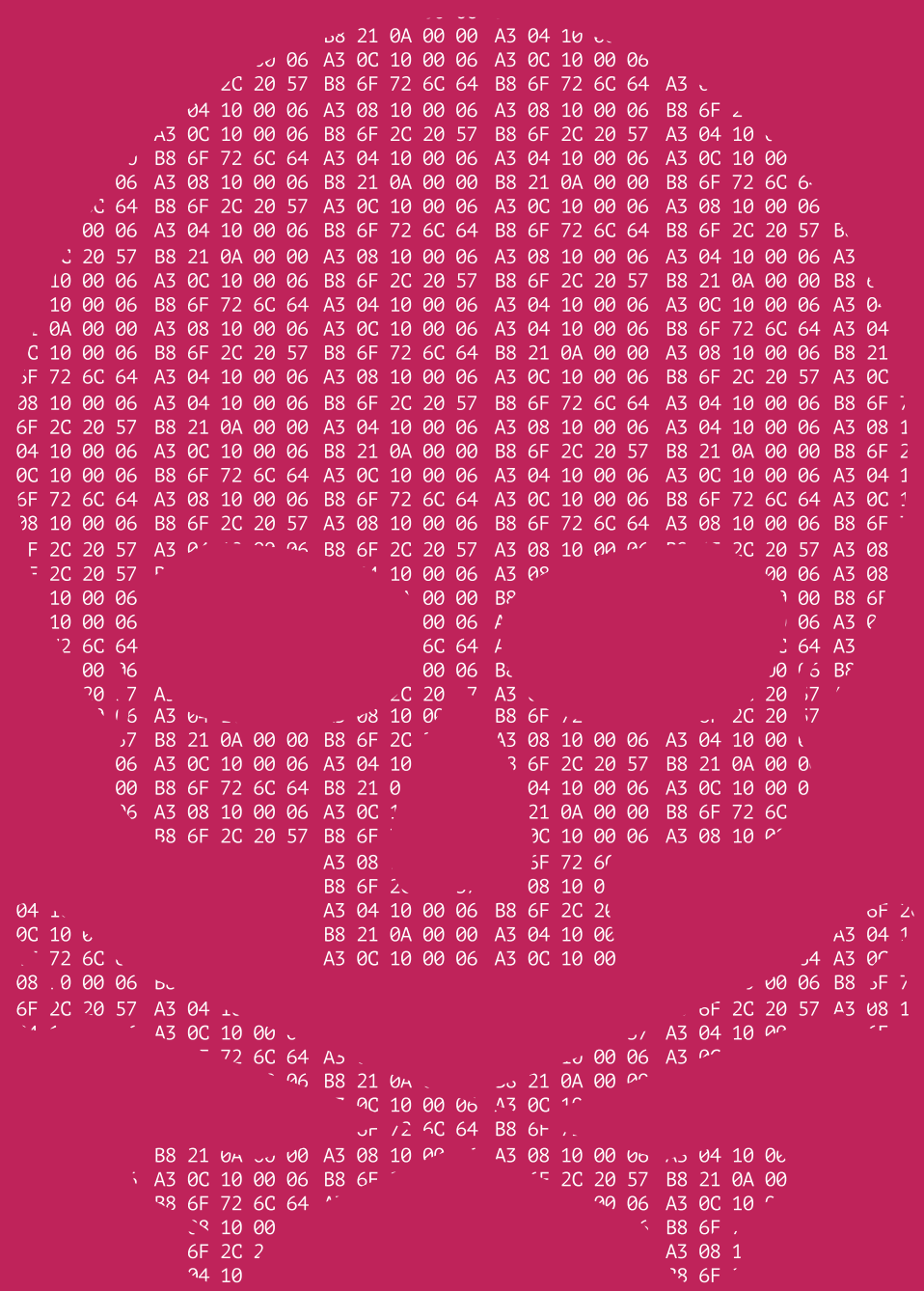


LEIDER GEHACKT

Text: Lazar Backovic

IT-SICHERHEIT Vielen ist es schon einmal passiert, darüber sprechen wollen die wenigsten: Vier Unternehmer erzählen, wie sie Opfer eines Cyberangriffs wurden. Experten erklären, wie Sie Ihre Firma schützen

Die Experten *Edgar Scholl (o.) berät internationale und mittelständische Firmen vor und nach Cyber-Angriffen. Sebastian Schreiber (u.) ist Gründer und Geschäftsführer der IT-Sicherheitsfirma Syss. Er ist regelmäßig als Experte im Fernsehen zu sehen und führt Live-Hacks vor*

Das war alles andere als ein guter Morgen für Christoph Brandstätter. Der Chef des Kärntener Seehotels Jägerwirt war schon zweimal von Hackern angegriffen worden, als er sich eines Morgens wieder nicht an seinem PC anmelden kann – und an den anderen elf Computern in seinem Hotel auch nicht. Statt des Startbildschirms erscheint an diesem Tag auf den Hotelrechnern die sarkastische Frage: „GOOD MORNING?“ – gefolgt von einer Lösegeldforderung. Erst nach Zahlung würden die Computer wieder freigegeben. Doch das Hotel benötigt seine IT, um Gäste ein- und auszuchecken und Schlüsselkarten für die Zimmer auszustellen. Wenn ein Gast mit einer Frage kam, hätten sich sein Team und er „wie im Blindflug“ gefühlt, erinnert sich Brandstätter an den Tag (den ganzen Fall lesen Sie auf Seite 60).

Mit seiner Geschichte steht der Familienunternehmer keineswegs allein da. Immer häufiger sehen sich Mittelständler Cyberattacken ausgesetzt. 2016 sei bereits jedes fünfte Unternehmen gehackt worden, ergab eine Umfrage des Beratungshauses Pricewaterhouse Coopers unter 400 Firmen mit weniger als 1000 Mitarbeitern. Im Jahr zuvor sei nur jede zehnte Firma betroffen gewesen. „Während die meisten Konzerne sich immer besser vor Cyberangriffen schützen, werden Mittelständler für Hacker ein zunehmend attraktiveres Ziel“, sagt Sebastian Schreiber, Geschäftsführer der Tübinger IT-Sicherheitsfirma Syss. Viele hätten ihre IT-Sicherheitsbudgets in den vergangenen Jahren sogar zusammengestrichen, sagt Schreiber – Motto: „Was gibt es bei mir schon zu holen?“

Geld her, sonst Daten futsch

Auf Brandstätters Geräten hat sich Ransomware breitgemacht, ein Verschlüsselungstrojaner, der Daten nur gegen Geldzahlung freigibt. Solche Erpresser-Viren grassieren derzeit im Netz und legen auch Betriebe lahm, die nicht voll durchdigitalisiert sind – manchmal für Tage. Auch der Verschlüsselungstrojaner Wannacry, der im Mai unter anderem die Deutsche Bahn befiel, funktionierte nach diesem Prinzip. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät dringend davon ab, auf die Lösegeldforderungen einzugehen – um weiteren kriminellen Machenschaften den Nährboden zu entziehen. „Doch wenn Sie ohne jede Sicherung Ihres Systems nicht mehr an Ihre Daten kommen, ist dieser Rat gerade für kleine Unternehmen wenig praxisnah“, meint Schreiber und kennt einige Fälle, in denen Unternehmen Tausende Euro an Cybererpresser zahlten.

Doch welche Bedrohungsszenarien gibt es eigentlich, und wie erkenne ich sie? Auf den nächsten Seiten schildern vier Unternehmer, wie sie oder ein Geschäftspartner gehackt wurden. Experten ordnen die Fälle ein und geben Tipps für mehr IT-Sicherheit in Ihrer Firma. >

Ein Monat offline

14. DEZEMBER 2015 Einer unserer Stammkunden, ein Hotel aus der Region, hat einen Lieferschein nicht erhalten. Ein Mitarbeiter mailt den Beleg erneut an den Kunden.

15. DEZEMBER, 11.18 UHR Ein Stahlverarbeiter aus dem Ruhrgebiet ruft an und fragt, warum wir ihm einen Lieferschein schicken. Die genannte Kundennummer entspricht der des Hotels, das den Tag zuvor angerufen hat. Wir erklären, dass es sich um ein Missverständnis handeln muss und legen auf.

15. DEZEMBER, 11.30 UHR Noch mehr Anrufer melden sich und fragen nach dem Lieferschein. Einige drohen mit Anwälten, andere beschimpfen uns wüst und legen dann auf. Allmählich dämmert uns: Jemand verschickt Mails in unserem Namen.

15. DEZEMBER, 12.10 UHR Das Telefon steht nun nicht mehr still. Die Telekom meldet sich, um uns mitzuteilen, dass die vielen Anrufe unsere Leitung überlasten. Wir ziehen alle Stecker und nutzen den Moment, um uns zu besprechen.

15. DEZEMBER, 12.30 UHR Unser IT-Dienstleister erklärt uns, dass jemand unsere Mailadresse gekapert und Hunderttausende Mails verschickt hat – mit immer gleichem Inhalt: „Sehr geehrte Damen und Herren, in der Anlage erhalten Sie wie gewünscht den aktuellen Lieferschein. Bei Fragen stehen wir Ihnen gern zur Verfügung. Mit freundlichen Grüßen, Textilreinigung Klaiber“. Wer den Lieferschein öffnet, läuft Gefahr, Schadsoftware in die eigene IT einzuschleusen. Wir veröffentlichen auf unserer Homepage, dass wir Opfer eines Hackerangriffs sind und das Problem beheben.

15. DEZEMBER, 14.40 UHR Weil die Kriminellen Sende- und Lesebestätigung angefordert haben, bekommen wir für jede gelesene Viren-Nachricht zwei E-Mails. Anfangs trudeln etwa 85000 solcher Rückläufer-Mails ein – pro Stunde. Das lässt unseren Mailserver fast abstürzen. Unsere Mailadresse ist mit dem Angriff unbrauchbar geworden – bei den meisten Anbietern würden wir ohnehin im Spam-Ordner landen, erklärt unser IT-Service.

Torsten Klaiber, 39, Villingen-Schwennigen

Die Firma *Textilreinigung Klaiber, 30 Mitarbeiter, Umsatz: etwa 2 Millionen Euro*

Der Angriff *„Ein Hacker hat Hunderttausende Mails in unserem Namen versendet. Ich selbst habe die Mail erhalten.“*

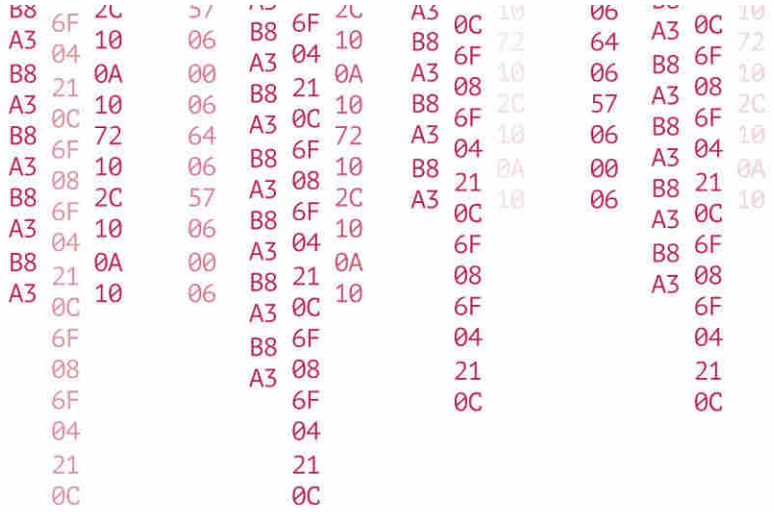
Der Schaden *Etwa 15000 Euro, plus 5 Prozent des Umsatzes wegen Verlust eines Kunden*

Anfangs trudelten etwa 85000 E-Mails bei uns ein – pro Stunde

Torsten Klaiber *über den Cyberangriff auf seine Firma*

15. DEZEMBER, 15 UHR Ich bin auf der Polizeiwache und erstatte Anzeige gegen unbekannt.

16. DEZEMBER Jeder Versuch, die Telefonanlage wieder anzuschließen, führt zu Dauerklingeln. Wir entscheiden, die nächsten Tage in der Firma ohne Telefon und Internet zu arbeiten. Die Vorweihnachtstage können wir glücklicherweise damit füllen, bestehende Aufträge abzuarbeiten. Die Lieferscheine stellen wir wie früher per Hand aus und kleben sie auf die Wäsche. Um bei Fragen erreichbar zu sein, gebe ich meine persönliche Handynummer und Mailadresse raus.



23. DEZEMBER 2015 Wir sind nach wie vor offline, auch das Telefon bleibt ausgestöpselt. Unser IT-Dienstleister löscht alle ankommenden E-Mails und setzt eine neue Mailadresse für uns auf, mit der wir im neuen Jahr arbeiten können.

10. JANUAR 2016 Wir können wieder Mails verschicken und empfangen. Einen Tag später schalten wir die Telefonanlage ein. Ab und zu melden sich noch Leute wegen der dubiosen Mail. Insgesamt ist es ruhig. Das Hotel, an das der Lieferschein ging, hat nach dem Vorfall die Kundenbeziehung zu uns beendet – bis heute ein bitterer Einschnitt.

Das sagen die Experten

SEBASTIAN SCHREIBER: Zwei Dinge können hier passiert sein: Entweder die Angreifer haben die Mailadresse tatsächlich übernommen oder schlicht den Absender gefälscht. Gegen Ersteres helfen sichere Passwörter und aktuelle Mailserver, gegen Letzteres nur komplexere Maßnahmen. Geholfen hätte hier vielleicht auch ein besserer Mailfilter oder ein externer Provider, der die eingehenden Mails vorsortiert. Eine Notfalladresse bei einem großen Mailanbieter wäre auch hilfreich, dann dürfte es nicht ganz so lange dauern, den Normalzustand wiederherzustellen.

EDGAR SCHOLL: Eine Horrorerfahrung, da bleibt einem in der Situation außer Stecker ziehen wenig übrig. Gut gefallen hat mir, dass der Unternehmer offen kommuniziert hat, was ihm passiert ist. Damit distanziert er sich von der Viren-Mail und warnt gleichzeitig Kunden und Betroffene. Eine Frage bleibt dennoch: Warum hat die Textilreinigung ihren eigenen Mailserver? Große Anbieter wie die Deutsche Telekom haben deutlich mehr Möglichkeiten, gegen Massen-Spam vorzugehen als ein Betrieb mit 30 Mitarbeitern. Das hätte die Spamwelle zumindest eindämmen können. >

Der gestohlene Einkäufer

3. SEPTEMBER 2015 Eine langjährige Geschäftspartnerin, die deutsche Marketingchefin eines US-Konzerns, will uns einem Kollegen in Paris empfehlen. Wir freuen uns über die Chance zu wachsen.

10. SEPTEMBER Der Kontakt aus Paris mailt uns. Mein Geschäftspartner ruft die Nummer in der Signatur an. Der Herr stellt sich als Einkäufer für das französischsprachige Afrika vor. Für eine Werbeaktion in Togo will er 20000 USB-Sticks ordern.

25. SEPTEMBER Die Bestellung geht per Fax bei uns ein. Alles läuft wie bei früheren Aufträgen. Wir bedanken uns bei der deutschen Tochtergesellschaft für die Empfehlung. Denen ist der Name des Einkäufers geläufig. Wir sichern unsere Forderungen dennoch über einen Kreditversicherer ab.

2. OKTOBER Der Einkäufer benötigt für eine ähnliche Aktion im Senegal noch einmal 30000 USB-Sticks. Der Kreditversicherer gibt sein Okay.

28. OKTOBER Unser Produzent liefert die Ware für Togo und den Senegal aus. Wir schicken die Rechnung via Mail und Brief nach Paris.

30. OKTOBER, 11.05 UHR Ein Finanzmanager der Pariser Tochter meldet sich. Er sehe die Rechnung, aber keinen Auftrag. Wir sind schockiert. Erst auf Nachfrage erklärt er, dass die Firma gehackt und die Identität des Einkäufers offenbar gestohlen wurde. Später entdecken wir: Die Adresse des Betrügers unterscheidet sich marginal von der tatsächlichen Webadresse des Konzerns.

30. OKTOBER, 11.15 UHR Während des Telefonats verfolgen wir die Sendung. Eine Maschine ist schon unterwegs nach Togo, den Senegal-Auftrag können wir noch im Zoll stoppen. Der Kreditversicherer deckt Betrug nicht ab. Uns droht ein Schaden von 200000 Euro. Wir erstatten Anzeige. Sechs Wochen später wird das Verfahren eingestellt.

4. NOVEMBER Wir holen die gesamte Ware nach Deutschland. Der Produzent verlängert die Zahlungsziele freundlicherweise bis weit ins nächste Jahr. Die 50000 USB-Sticks füllen nun ein Lager im Schwarzwald. Wir starten einen Notverkauf und verkaufen die USB-Sticks zu einem Stückpreis von 5 Euro oder weniger – je nach Menge. Das mindert den entstandenen Schaden schrittweise.

Carsten Lenz, 48, Meerbusch

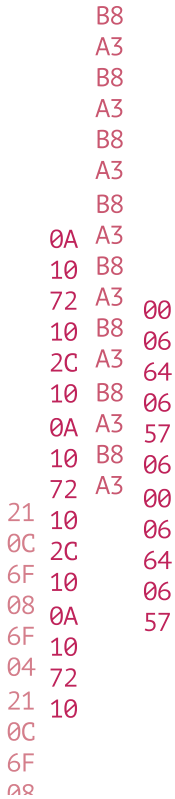
***Die Firma** S&P Werbeartikel, 6 Mitarbeiter, Umsatz: 2 Millionen Euro*

***Der Angriff** „Ein Betrüger hat sich als Geschäftspartner ausgegeben und uns mit einer sehr großen Bestellung beauftragt. Der Auftrag platzte, als die Ware schon unterwegs war.“*

***Der Schaden** Etwa 175000 Euro*

Das sagt der Experte

EDGAR SCHOLL: Auch wenn es nach einer Verkettung mehrerer Zufälle aussieht, so ist in diesem Fallbeispiel der größte und einzige Problemfaktor der Mensch. Wir alle sind manipulierbar. Diese Schwäche hat der Betrüger hier in eindrücklicher Weise für sich genutzt, wobei mir sein Motiv nicht ganz klar ist: Wollte er der Pariser Konzerntochter schaden, dem Mittelständler oder beiden? War womöglich ein Konkurrent im Spiel, der Böses vorhatte? Durch zwei Dinge hätte der Schwindel auffliegen können: durch einen Anruf in der Pariser Zentrale und den kleinen Unterschied in der Mailadresse. Hier lässt sich das Bewusstsein des Unternehmers (und das der Mitarbeiter) trainieren! In den Einstellungen jedes Mailprogramms lässt sich konfigurieren, dass statt des Namens die Mailadresse des Absenders angezeigt wird. Das hätte vielleicht früher Fragezeichen aufgeworfen.



Unternehmen (2)

Kleiner Fehler, 1500 Euro Schaden

13. SEPTEMBER 2014 In Vorbereitung auf eine wichtige Fachmesse bearbeite ich meine neue Webseite photolodge.de, ein Nebenprojekt, mit dem ich vor allem Privatpersonen für Fotografiekurse begeistern möchte. Im Administratorenbereich der Wordpress-Seite installiere ich ein Plug-in, ein kleines Zusatzprogramm, mit dem ich Bilder auf der Seite bearbeiten kann. Weil die Installation hakt, setze ich die Zugriffsrechte der Seite für kurze Zeit auf die niedrigste Stufe. So lässt sich das Plugin installieren. Ein Fehler, wie sich herausstellt.

14. SEPTEMBER Google warnt nun Nutzer vor meiner Seite. Ich prüfe Inhalt und Optik auf meinem Rechner. Alles sieht normal aus.

15. SEPTEMBER Die Firma, die meine Internetdomain verwaltet, teilt mir per Mail mit, dass sie meine Seite bis auf Weiteres vom Netz genommen hat. Begründung: „unsichere Skripte". Kommentar: „In Ihrem Webspace wurde Fremdcode eingeschleust." Insgesamt sollen mehr als 30 Dateien infiziert sein – und heute ist Messeeröffnung.

16. SEPTEMBER Ich kontaktiere einen IT-Service, den mir ein Freund empfohlen hat. Die Experten erklären mir, dass das Plug-in, das ich installiert habe, veraltet war und Hacker die Sicherheitslücke genutzt haben, um einige Besucher meiner Seite auf Pornoseiten weiterzuleiten.

19. SEPTEMBER Der IT-Service hat meine Seite komplett neu aufgesetzt und beantragt die Entsperrung meiner Seite bei der Firma, die meinen Webspace verwaltet. Kurz darauf ist photolodge.de wieder online. Insgesamt hat mich mein Fehler rund 1500 Euro gekostet.

Stephen Petrat, 43, Köln

Die Firma *Freier Fotograf, Umsatz: 125000 Euro*

Der Angriff *„Hacker haben meine Seite so manipuliert, dass sie vom Netz genommen wurde. Es handelte sich aber zum Glück nur um ein Nebengeschäft. Der Schaden hielt sich in Grenzen."*

Der Schaden *Etwa 1500 Euro für die Wiederherstellung der Seite*

Das sagen die Experten

SEBASTIAN SCHREIBER: Webseiten werden regelmäßig automatisch auf Schwachstellen gescannt und vollautomatisch angegriffen, auch kurzzeitige Lücken sind deshalb gefährlich. Die Seite des Fotografen wurde gekapert, um offenbar Besucherströme umzuleiten. Die Angreifer verdienen dann zumeist Geld mit eingeblendeter Werbung oder infizieren die Rechner der Besucher mit Schadsoftware. Meine Tipps: Erstens, Content-Management-Systeme wie Wordpress oder Typo3 immer aktuell halten und Plug-ins nur mit Bedacht installieren, weil solche Fremdprogramme per se ein Sicherheitsrisiko darstellen. Zweitens: Bei komplexen Arbeiten an der eigenen Homepage unbedingt jemanden hinzuziehen, der sich wirklich mit der Materie auskennt. Und drittens: immer eine aktuelle Sicherung der eigenen Webseite vorhalten.

EDGAR SCHOLL: Häufig wird es Cyberkriminellen leicht gemacht, so auch in diesem Fall. Webdesign und Shop-Programmierung gehören grundsätzlich in Expertenhände. Denn so ein scheinbar kleiner Fehler wie im Fallbeispiel kann große Auswirkungen haben. Wen Google einmal als schadhafte Seite einstuft, sammelt Maluspunkte und taucht in den Suchergebnissen für einige Zeit weiter hinten auf als gewohnt. Das scheint der Unternehmer offenbar noch abgewendet zu haben – Glück im Unglück! >

Wenn der Hacker vier Mal anklopft …

2. SEPTEMBER 2016, 9.31 UHR Die Rezeptionistin öffnet eine Mail, scheinbar von der Post. Als sie einen Link anklickt, installiert sich ein Trojaner, der nach und nach alle Dateien auf dem Rechner verschlüsselt. Wir trennen den PC vom Netzwerk und informieren unseren IT-Service. Der spielt eine Sicherungskopie unseres Systems auf. Der befallene Rechner läuft am nächsten Tag wieder.

7. SEPTEMBER In Absprache mit dem IT-Service schulen wir unsere Mitarbeiter; erklären, woran sie Schad-Mails erkennen und wie sie darauf reagieren sollen. Unsere Passwörter haben nun 16 Stellen. Zudem werden im Mailprogramm nun nicht mehr die Namen, sondern die Adressen der Absender angezeigt. Das enttarnt einige dubiose Anfragen.

17. SEPTEMBER Der Hacker hat sich scheinbar eine Hintertür offengehalten. Ein anderer PC ist nun mit dem Verschlüsselungstrojaner infiziert. Die Mitarbeiter ziehen sofort alle Stecker, wie sie es in der Schulung gelernt haben. Der IT-Service tauscht auf allen zwölf Firmenrechnern die Festplatten aus und stellt das System per Back-up wieder her. Nach anderthalb Tagen können wir wieder normal arbeiten.

2. DEZEMBER, ABENDS Es muss kurz nach Feierabend sein, als der Hacker ein drittes Mal zuschlägt. Diesmal hat er es auf unseren Server geschafft. Weil wir an diesem Wochenende geschlossen haben, hat der Hacker nun gute zwei Tage Zeit, um auf unserem Server zu wüten.

5. DEZEMBER, 7.21 UHR Unsere PCs lassen sich nicht hochfahren. Auf dem Bildschirm erscheinen groß die Worte „GOOD MORNING?“ – gefolgt von einer Lösegeldforderung – Höhe unbekannt – und der Aufforderung, binnen 24 Stunden Kontakt zum Hacker aufzunehmen, sonst würde sich die Forderung verdoppeln. Ich bleibe ruhig, wir haben ja unsere Sicherungskopien, denke ich. Doch auch die sind inzwischen verschlüsselt. Wir haben keine Chance mehr, an unsere Daten zu kommen.

5. DEZEMBER, 8.16 UHR Ich frage den Hacker per Mail, wie viel er für die Entschlüsselung meiner Daten verlangt. Ich gebe mich bewusst als Privatmann aus und hoffe, dass die Lösegeldforderung so nicht ganz so hoch ausfällt.

5. DEZEMBER, 8.38 UHR Der Hacker schreibt. Er fordert zwei Bitcoins, damals etwa 1500 Euro. Überweisungen in der Digitalwährung lassen sich nicht zurückverfolgen. Der Hacker schickt mir einen Link zur Zahlung. Ich schicke ihm das Lösegeld.

5. DEZEMBER, 9.28 UHR Wir erhalten einen Entsperrcode und ein Programm, das die Daten wieder lesbar macht. Allein die Entschlüsselung dauert

Christoph Brandstätter, 38, Turrach/Österreich

***Die Firma** Seehotel Jägerwirt, 40-60 Mitarbeiter (je nach Saison), Umsatz: knapp 4 Millionen Euro*

***Der Angriff** „Hacker haben vier Mal die Computer meines Hotels gekapert und mich erpresst.“*

***Der Schaden** Etwa 15000 Euro*

> *Solange unsere IT lahmliegt, agieren wir wie im Blindflug: Wir wissen nicht, wer ankommt und wer abreist*
>
> ***Christoph Brandstätter***
> *Seehotel Jägerwirt*

Sissi Furgler Fotografie

0A
10
72
10
2C
10
0A
10
72
21 10
0C 2C
6F 10
08 0A
6F 10
04 72
21 10
0C
6F
08

anderthalb Tage. Solange unsere IT lahmliegt, agieren wir wie im Blindflug: Wir wissen nicht, welche Gäste ankommen und abreisen, auch Rechnungen können wir keine ausstellen – genauso wie Schlüsselkarten für die Zimmer. Will ein Gast aufs Zimmer, muss ein Mitarbeiter die Tür öffnen. Die Kunden nehmen es gelassen, die meisten sind zum Skifahren hier und in Urlaubsstimmung.

22. JANUAR 2017 Als das Fernsehen über unseren Fall berichten will, erleben wir einen vierten Angriff. Die Journalisten bekommen live mit, was passiert. Der Hacker hat eine Sicherheitslücke in unserer Firewall ausgenutzt, erneut verschlüsselt ein Trojaner unsere Daten. Unser IT-Service kann die Dateien diesmal jedoch selbst entschlüsseln. Wenige Stunden später läuft alles wie gewohnt. Wir überlegen inzwischen, zu normalen Zimmerschlüsseln zurückzukehren – für die braucht man keinen PC.

Das sagt der Experte

SEBASTIAN SCHREIBER: Vier Mal gehackt, vier Mal auf sehr ähnliche Weise – das ist auf gut Deutsch gesagt richtig doof gelaufen. Digitale Erpressungen über sogenannte Ransomware stellen derzeit das größte Bedrohungsszenario für Unternehmen dar (mehr im Kasten rechts). Einige Virenprogramme erkennen ältere Verschlüsselungstrojaner automatisch, darauf verlassen sollte man sich aber nicht. Der effektivste Schutz sind Mitarbeiterschulungen und regelmäßige Sicherungskopien, sogenannte Back-ups. Diese sollten unbedingt so abgelegt werden, dass sie nicht einfach überschrieben werden können – externe, nicht immer eingesteckte Festplatten helfen hier. ■

UNTERM STRICH Cyberattacken können einen kleinen Betrieb zeitweise lahmlegen oder vollständig ruinieren. Viele Unternehmer unterschätzen die Gefahr aus Unwissenheit oder Leichtsinn.

DIE DUNKLEN BEDROHUNGEN

Drei beliebte Cyberangriffe – und was dann zu tun ist

Botnet
Ein Botnet besteht aus Tausenden gekaperten internetfähigen Geräten, die Hacker als Infrastruktur für bestimmte Cyberangriffe nutzen – etwa zum Versand von Spam-Mails. Die Geräte sind vergleichbar mit Schläferzellen, ihre Besitzer merken in der Regel nichts von dem Missbrauch. **Das sollten Sie sofort tun:** Auf **botfrei.de** bietet der Internetverband Eco das Gratisprogramm EU-Cleaner an. Damit lässt sich ein infiziertes Gerät säubern.

DDoS
Steht für Distributed Denial of Service. Dahinter verbirgt sich das gezielte Überlasten eines Webdiensts oder einer Webseite durch Tausende Einzelanfragen, meist gesteuert über ein Botnet. **Das sollten Sie sofort tun:** Provider kontaktieren. Manchmal können dort die Anfragen blockiert werden.

Ransomware
Lösegelderpressungen per Verschlüsselungstrojaner sind derzeit en vogue unter Hackern. Die Bausteine dafür lassen sich im Darkweb, dem unkontrollierten Teil des Internets, für ein paar Hundert Euro ordern. Hauptziel sind Windows-Computer, es gibt aber auch Erpressungstrojaner, die Linux- oder Mac-Systeme befallen. **Das sollten Sie sofort tun:** Sämtliche Stecker ziehen, das stoppt die Verschlüsselung. Haben Sie ein Back-up, sollten Sie damit Ihr System neu aufsetzen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät, jede Ransomware-Attacke anzuzeigen und kein Lösegeld zu zahlen.

VORSICHT STATT NACHSICHT

So können Sie Cyberangriffen vorbeugen und sich wappnen

Back-ups
Sicherungskopien sind der effektivste Schutz gegen Hacker, lässt sich mit ihnen doch meist der Normalzustand wiederherstellen. Auf Windows erstellen Sie ein Back-up zum Beispiel über Systemsteuerung/System und Sicherheit/Sichern und Wiederherstellen. Auf Mac OS hilft das Dienstprogramm Time Machine. **Tipp:** Führen Sie einen Back-up-Tag in der Woche ein, an dem Sie Ihre Daten sichern.

Passwort
Gut ein Drittel aller Deutschen nutzt für mehrere Onlinedienste das gleiche Passwort. Ein Krimineller kann sich dann einfach den schwächsten Onlinedienst heraussuchen und erlangt so Zugriff auf mehrere Konten – von der E-Mail bis zum Online-Banking. Besser sind verschiedene Passwörter. Die sollten laut BSI mindestens acht Stellen sowie Sonderzeichen, Groß- und Kleinbuchstaben enthalten. **Tipp:** Passwortkarten (etwa diese: **tinyurl.com/passwortkarte**) helfen Ihnen dabei, ein sicheres Kennwort zu erstellen.

Updates
Basisprogramme für den Virenschutz und Firewalls halten etwa 80 Prozent aller Angriffsszenarien ab, schätzen Experten – aber nur, wenn die Schutzsoftware auf dem neuesten Stand ist. Halten Sie deshalb Schutzprogramme, aber auch Ihr Betriebssystem und den Browser aktuell. **Tipp:** Der Browser Google Chrome installiert Updates automatisch.