A1 Cybercrime Stories

Barbara Wimmer

Einfach lahmgelegt

EINFACH LAHMGELEGT

EINE A1 CYBERCRIME-STORY

BARBARA WIMMER

1

»Wir sind drin«, rief Milan. »Ich habe eben eine Benachrichtigung von unserem System erhalten, das wir auf den Router-Hersteller Figgio angesetzt haben. Du hattest Recht: Dieser Heinrich vom Vertrieb hat auf unseren E-Mail-Link geklickt und das angehängte .docx geöffnet.«

»Immerhin sind wir endlich drin im Firmennetz!«

»Du installierst die Ransomware und ich grabe mich tiefer rein ins System.«

»Klar! Wie immer.«

»Wir sind einfach ein gutes Team! Was meinst Du? Wie hoch setzen wir die Lösegeldforderung an?«

»Ich würde sagen 15 Prozent vom Umsatz aus dem letzten Jahr?«

»Klingt fair. So viel muss es ihnen schon wert sein, dass wir die technischen Dokumente, die wir zur Hardware finden werden, nicht an die Konkurrenz weitergeben.«

»Bin ich voll bei dir.«

»Na dann … Lass uns anfangen!«

. . .

Milan platzierte mehrere Schadprogramme auf den Firmenrechnern von Figgio, während bei Dennis am Rechner die Commandozeilen herunterliefen, als er die Systeme des Router-Herstellers durchforstete. Sie waren ihrem Ziel, eine weitere Firma erfolgreich lahmzulegen, nahe. Der Plan war, die Auslieferung des Routers an die Kunden zu stoppen und die neuen Dokumente der zukünftigen Modelle an die Öffentlichkeit zu leaken. Dafür würde Figgio fix Lösegeld zahlen, dachte Dennis. Zumindest hatten das die Betriebe, die sie in den vergangenen Wochen erpresst hatten, alle still und heimlich getan. Dennis zündete sich eine Zigarette an, während er darauf wartete, dass ein zugekauftes Hacker-Tool ganze Listen von Passwörter durchprobierte, um in weitere Systeme einzudringen. Noch waren sie nicht am Ziel. Es würde noch zirka zwei Wochen dauern, bis sie sich einen ausreichenden Überblick über die IT-Infrastruktur des Router-Herstellers von innen verschafft hatten, um dann zuzuschlagen. Bis dahin hatten sie alle Dokumente abgesaugt und waren bereit, ihre Präsenz im Firmennetz von Figgio zu erkennen zu geben. Denn aktuell wusste niemand, dass sie drin waren. Am Ende war es nur ein Knopfdruck, mit dem sie das komplette System lahmlegten und Lösegeld in Bitcoin fordern würden. Dennis freute sich schon jetzt auf diesen Tag.

2

Zwei Wochen später.

Heinrich rief in einer Excel-Tabelle die Bestellungen ihres brandheißen, neuen Router-Modells auf. Diese liefen wie am Schnürchen. Der Telekom-Betreiber N35 wollte 500.000 Stück mit seinem Namen und Logo drauf, der Betreiber Mobility S bestellte 280.000 Stück, ebenfalls mit seinem Namen und Logo. Die Aufträge waren fix, in einer Woche sollten sie liefern. Sie hatten einen echten Generationensprung geschafft mit der Hardware, die sie deutlich von der Konkurrenz abhob. Das wurde nun belohnt. Heinrich schickte gerade die Aufträge der Firmen an die Produktion weiter, als plötzlich sein Bildschirm schwarz wurde und eine Meldung in einem gelben Rahmen kam. »Your personal files are encrypted« stand da. Heinrich versuchte das schwarze Fenster wegzuklicken, doch es gelang ihm nicht. Egal, dachte er, und ging eben kurz aufs WC.

. . .

Als der Vertriebsmitarbeiter zu seinem Platz zurückkam, war der Bildschirm noch immer schwarz. Und mittlerweile auch der des Kollegen. Und des Kollegen neben diesem. Alle waren aufgesprungen und liefen wild umher. Einer telefonierte bereits mit der IT-Abteilung. Die Anweisung lautete: »Sofort alle Rechner, die noch laufen, herunterfahren, und den Schaden begrenzen!« Heinrich verstand nicht, warum es helfen sollte, alle Rechner abzudrehen, aber er machte mit. Als das geschafft war, fragte er: »Und nun?«

»Die IT-Abteilung muss versuchen, die Ursache zu finden. Wir sind wohl irgendwie gehackt worden. Wir können in der Zwischenzeit für heute nach Hause gehen und sollen telefonisch erreichbar bleiben. Auf unsere Firmen-Mails können wir derzeit nicht zugreifen«, sagte sein Kollege.

»Juhu, Feierabend!«, rief Heinrich laut. Er hatte in den letzten Wochen wahrlich genug Überstunden angehäuft wegen des bevorstehenden Launch-Termins. Der Zeitpunkt war allerdings ungünstig, denn die Bestellungen mussten schleunigst weiter bearbeitet und verteilt werden. An das .docx-File, das er vor zwei Wochen geöffnet hatte, dachte er zu diesem Zeitpunkt nicht mehr.

3

Bei Martina Meier, Head of IT und Security bei Figgio, läutete seit Stunden ohne Unterbrechung das Telefon. Die Telefon-Anlage war eines der wenigen Dinge, die beim Router-Hersteller nicht vom Ausfall betroffen war, obwohl auch diese mittlerweile über Voice over IP lief. Eigentlich ein Wunder, dachte Martina, und ein Teil von ihr wünschte sich, dass auch die Telefone still standen, denn sie hatte es derzeit eher unlustig. Der CEO der Firma forderte unverzüglich einen »Übersichtsbericht«, und zwar innerhalb der nächsten Stunde. Dabei war ihre Abteilung gerade noch dabei, herauszufinden, was eigentlich passiert war. Fest stand bisher nur, dass sie sich eine Ransomware eingefangen hatten und Erpresser Lösegeld verlangten. Das Vorgehen war ihr bekannt, es hatte bereits zahlreiche Unternehmen in Österreich und im Ausland getroffen. Martina dachte eigentlich, dass es sie bei Figgio nicht treffen würde, denn sie hatten zumindest am Papier ein gutes Konzept dafür ausgearbeitet. Sie hatte sogar extra ein IT-Security-Seminar an der Fachhochschule zu dem Thema besucht und alles davon umgesetzt. Martina musste die Eintritts-

pforte finden und schließen, denn sonst könnte sich der Vorfall jederzeit wiederholen.

Doch erst einmal ging es um Schadensbegrenzung. Der CEO machte enormen Druck. Die Erpresser verlangten ganz klassisch Lösegeld dafür, dass sie die Zugriffe auf die IT-Systeme wieder freigeben und die Dateien wieder entschlüsseln würden. Doch sie hatten sich auch etwas ausgedacht, dass Martina so noch nicht kannte: Sie wollten das Geld auch dafür, dass bestimmte technische Details ihres nächsten Produkts nicht an die Öffentlichkeit gelangten. Figgio stellte schließlich nicht nur Router her und es wäre eine Katastrophe, wenn gewisse Dinge, auf die sie extrem stolz waren, jetzt schon herauskämen. Die Konkurrenz würde sich die Finger lecken und alles sofort nachbauen, während sie selbst noch gar nicht soweit waren mit der Produktion der nächsten Produkte. Ein großes Dilemma.

»Meier, weil Sie nicht ans Telefon gehen, komme ich jetzt zu Ihnen«, sagte der Chef, der plötzlich im Büro der Abteilungsleiterin stand, und ihr über die Schulter blickte. Komisch, dass sie ihn gar nicht gehört hatte.

»Wie Sie sich denken können, habe ich alle Hände voll zu tun.«

»Wissen Sie schon, was passiert ist?«

»Ja. Wir sind Opfer von Erpressern geworden.«

»Erpressern? Etwa solche, die auch die Apple-Zulieferer angegriffen haben? Oder diese Pipeline in den USA, wo es tagelang kein Benzin gab?«

»Genau, von solchen.«

»Aber haben Sie nicht immer gesagt, dass uns das nicht passieren kann?«

»Das dachte ich auch. Aber da hat uns wohl jemand wochen-

lang ausspioniert. Das belegen unsere Logfiles, jetzt wo wir wissen, wonach wir suchen mussten. Gegen so etwas ist man machtlos.«

»Das ist schlecht, ganz schlecht. Wofür bezahle ich Sie eigentlich, wenn Sie da nicht früher draufkommen? Sie sind doch IT-Profi!«

»Es gibt keine hundertprozentige Sicherheit. Wir können es den Angreifern nur so schwer wie möglich machen und sie möglichst früh in unseren Systemen entdecken.«

»Und was bringt uns das jetzt?«

Der Chef hatte Recht mit seiner Frage. Die hochgewachsene, schlaksige IT- und Security Leiterin hatte allerdings ordentlich damit zu kämpfen, trotz des persönlichen Angriffes höflich zu bleiben. Statt einer allgemeinen Diskussion über Sicherheit sollte sie mit ihrem Team eigentlich an der konkreten Problemlösung arbeiten.

»Sie haben Recht: Es bringt uns nichts. Deshalb würde ich gerne in Ruhe weiterarbeiten und mich in drei Stunden mit Ihnen, dem Entwickler-Team und unseren Firmen-Anwälten im Meeting-Raum treffen. Bis dahin kann ich Ihnen viel mehr sagen. Etwa, was die Erpresser genau wollen. Und wir haben bis dahin einen Zeithorizont in Aussicht, wann wir die Systeme wieder zum Laufen bringen können. «

»Verstehe. Dann machen Sie, Meier! Ich verlasse mich auf Sie!«

Zwei Stunden später.

Martina Meier und ihr Team hatten sich über die Sachlage ein Bild machen können. Leider war das Ausmaß der Cyberattacke auf Figgio viel größer, als sie selbst ursprünglich angenommen hatte. Mittlerweile hatten mehrere Mitarbeiter aus den Produktionsstätten angerufen. Das bedeutete: Nicht nur Marketing, Vertrieb und die Entwicklung standen still, sondern auch die Ausrüstung

der bestellten Router mit den jeweiligen Anforderungen der Partnerunternehmen. Das war der Super-Gau. Die verschlüsselten Dateien, die würden sie schon in den Griff bekommen, wusste Meier. Aber bis die Produktionsstätten wieder am Netz hingen, das würde dauern. Sie wusste, dass die Zeit drängte.

Eine weitere Stunde später.

Im Meetingraum hatten sich insgesamt zwölf Anzugträger und eine Anzugträgerin versammelt, alle mit weißem Hemd und schwarzem Sakko. Martina Meier war die Einzige, die den Raum mit Laptop und nicht im »vorstandstauglichen« Outfit betrat. Sie hatte am Tagesbeginn ja auch nicht wissen können, dass sie der Chefetage heute noch derart schlechte Nachrichten überbringen musste. Alle im Raum schwiegen und starrten gebannt auf sie. Martina tat so, als würde sie es nicht bemerken, stellte den Laptop ab, steckte ihn auf Anhieb am richtigen Kabel an, und am großen Monitor poppte eine Präsentation auf. Die Aufmerksamkeit der zwölf Anzugträger und der Anzugträgerin wanderte schlagartig zum Bildschirm und Martina atmete tief durch.

»Meine Damen und Herren. Ich habe leider schlechte Nachrichten für Sie. Beim Ransomware-Angriff auf unser System wurden nicht nur Dateien auf unserem Computersystem verschlüsselt, sondern auch gestohlen und die Erpresser drohen damit, diese zu veröffentlichen. Es handelt sich dabei um eines unserer Produkte, das gerade noch in Entwicklung ist und das nach den Routern, die nächste Woche ausgeliefert werden sollten, unser neues Flaggschiff werden sollte.«

Meier zeigte am Bildschirm Auszüge der Dateien, die sie persönlich in ihrer Rolle als Security Chefin von den Erpressern erhalten hatten. Darauf waren sämtliche Produkt-Spezifikationen mit allen technischen Details zu erkennen. »Es liegt nicht in meinem Ermessen, zu beurteilen, ob eine Zahlung in diesem Fall

angemessen ist, oder nicht. Früher gab es generell seitens der Polizei die klare Empfehlung, nicht zu zahlen. Aber jede Situation ist individuell und entscheiden müssen das am Ende Sie, meine Damen und Herren. Der Polizei und dem lokalen Computer Emergency Response Team wurde der Vorfall bereits gemeldet. Ich bin außerdem mit externen Security-Spezialisten in Kontakt, die wir hinzuziehen könnten, damit es schneller geht. Doch das kostet.«

»Was zur Hölle….«, fluchte der CEO und lockerte seine Krawatte.

Der Entwicklungschef rutschte auf seinem Sessel unruhig von links nach rechts und klopfte mit seinen Fingern am Tisch herum. Ansonsten sagte keiner etwas, es war mucksmäuschenstill im Raum. Martina Meier fuhr fort: »Außerdem muss ich Ihnen mitteilen, dass wir mindestens sieben Tage brauchen werden, um die gesamten IT-Systeme neu aufzusetzen. Dieser Prozess ist leider notwendig geworden, weil die Erpresser nicht nur Dateien gestohlen, sondern sich in unsere Infrastruktur eingenistet haben. Auch in die der Produktion.«

»Sieben Tage? Aber da muss die Auslieferung der Router schon lange laufen!« Der CEO wurde leichenblass im Gesicht.

»Ich weiß…«

»Das ist unser Ruin«, rief er. »Was bedeutet das konkret in Zahlen, wenn sich unsere Auslieferung um sieben Tage verzögert?«

Der Finanzchef, der stocksteif dasaß, zuckte mit den Achseln und sagte, dass er das erst in Ruhe ausrechnen müsse.

»Ich kann Ihnen nur sagen, was aus Sicht der IT Stand der Dinge ist. Vielleicht geht es zwei Tage schneller, wenn unser Team eine externe Unterstützung erhält. Allerdings sind die mit unseren Systemen nicht so vertraut und es wird schwierig, jemanden auf Abruf zu finden. Ransomware-Experten sind meistens gut ausgelastet«, ergänzte Meier.

»Und jetzt noch die Frage aller Fragen: Wie hoch ist die Lösegeldforderung?« Der CTO hatte Unterlagen ausgepackt, und diese zusammen mit einem Taschenrechner vor sich aufgestapelt.

»15 Prozent vom Vorjahresumsatz in Bitcoin.«

Es entstand eine lange Pause, in der alle schwiegen. Der CEO von Figgio trank sein Wasserglas leer, das vor ihm stand. Dann richtete er sich auf, kreiste einmal mit seinen Schultern und sagte: »Danke, Meier. Jetzt weiter an die Arbeit. Jede Minute zählt … Wir werden uns unterdessen beraten und Sie dann über unsere Entscheidungen in Kenntnis setzen.«

Martina Meier stecke das Kabel aus, das ihren Laptop mit dem Monitor verband, nickte den zwölf Herren und der Dame in Anzug zu und war froh, den Raum wieder verlassen zu können. Da arbeitete sie doch wesentlich lieber mit ihrem Team zusammen, als derartige Entscheidungen treffen zu müssen, die den Herrschaften jetzt blühten. Wenigstens hatte ihr keiner buchstäblich den Kopf abgerissen. Das passierte ja Überbringern schlechter Nachrichten häufig. Sie hoffte, dass es dabei blieb.

4

Drei Tage später.

»Haben wir schon etwas von Figgio gehört?«, fragte Dennis seinen Erpresser-Kollegen.

»Moment, ich sehe mal nach, ob bereits eine Zahlung eingelangt ist, oder wir eine E-Mail an das Postfach erhalten haben, das ich für den Fall eingerichtet habe.«

Kurze Zeit war nur zu hören, wie Dennis den Rauch seiner Zigarette ausblies. Die Tastatur von Milan machte keine Geräusche.

»Nichts.«

»Och, schade! Glaubst du, die zahlen noch?«

»Bestimmt. Solche Firmen brauchen immer. Bis das Geld freigegeben wird und alles. Das dauert.«

»Wie sieht es im Netz aus?«

»Wir sind bereits draußen. Sie haben alles neu aufgesetzt. Da dürften sie offenbar ein paar externe Profis dazu geholt haben.«

»Hoffen wir auf das Beste. Oder glaubst du, sollten wir ihnen noch weitere Dokumente, die wir erbeutet haben, als Beweis schicken?

»Erst einmal nicht. Warten wir noch drei Tage, dann holen wir das nach«, sagte Milan.

»Ok, dann machen wir einstweilen bei Duffle weiter.«

»D'accord.«

5

Sabine und Vanessa aus der Marketing-Abteilung schrieben sich über den Messenger Signal Nachrichten, da die firmeninterne Plattform noch immer offline war. Sie konnten auch noch nicht in die Firma zurück, um an ihren Rechnern zu arbeiten. Zwar waren sie eingeteilt worden, zwischen 9 und 13 Uhr den Vertrieb dabei zu unterstützen, die Kundenkommunikation telefonisch aufrechtzuerhalten, aber die restliche Zeit war als Zeitausgleich zu konsumieren. Nichts ging. Mail-Anweisungen bekamen sie teils auf ihren privaten Geräten auf ihre privaten E-Mail-Adressen geschickt, ansonsten fand die Kommunikation hauptsächlich per Diensthandy statt.

»Hast du den Bericht über uns in der Zeitung gelesen?«, fragte Vanessa ihre Kollegin.

»Ja, da steht, dass wir erpresst werden und es um einen Millionenschaden geht.«

»Ich hätte mir nicht gedacht, dass uns das passieren könnte!«

»Ich auch nicht. Ist schon krass, was da abgeht.«

»Glaubst du, könnte das was mit der Phishing-Mail zu tun haben, die in meinem Namen verschickt worden ist?«

»Was? Nein, wieso?«

»Wer weiß. Vielleicht hatte das etwas damit zu tun.«

»Glaube ich nicht, das ist doch schon so lange her«, antwortete Sabine.

Auch Sabine hatte drei Wochen zuvor von ihrer Kollegin Vanessa eine merkwürdige E-Mail erhalten. Der Betreff: »Re: Dokument«. Der Text: »Liebe beide, könnt ihr mit dem Dokument was anfangen?« Die E-Mail war an Heinrich vom Vertrieb und an Sabine gegangen. Unterzeichnet war sie mit dem Namen von Vanessa. Doch die hatte zu dem Zeitpunkt gerade in der Küche einen Kaffee zubereitet. Das hatte Sabine merkwürdig gefunden und sie hatten den Vorfall an die Security-Abteilung gemeldet.

Vanessa suchte sich Heinrichs Klappe aus dem ausgedruckten Telefonverzeichnis und rief Heinrich an. All ihre Firmentelefone waren auf die Diensthandys umgeleitet. Der Vertriebsmitarbeiter hob nach drei Mal Läuten ab.

»Hallo, Heinrich! Kann ich dich kurz etwas fragen?«

»Ja, was denn?«

»Hast du vor ein paar Wochen von mir eine Mail gekriegt mit einem Anhang?«

»Ja. Da hast du mir ein leeres Dokument geschickt. Was sollte das eigentlich?«

»Die Mail war nicht von mir, das war Phishing. Da hast du drauf geklickt?«

»Ja, klar. Phishing? Das glaube ich nicht. Die Mails, die wir in der Schulung durchgenommen hatten, sahen ganz anders aus! Warum hast du mir das geschickt, Vanessa?«

»Noch einmal: Ich war das nicht.«

»Da stand aber dein Name drauf!«

»Hast du das wenigstens der IT-Abteilung gemeldet? Vielleicht hat es was mit dem Erpresser-Vorfall zu tun.«

»Ach, das war doch schon vor drei Wochen. Ich würde jetzt gerne weiterarbeiten. Ich habe derzeit genug damit zu tun, Kunden und Partner zu beruhigen.«

Heinrich Winter drückte mit Wut im Bauch den roten Knopf. Er musste sich beruhigen. Diese Vanessa war offenbar eine von der Sorte, die alles besser wusste. *Ihr* hätte so etwas sicher nicht passieren können, so obergescheit, wie sie daher redete! Er würde auch sicher *nicht* die Security-Abteilung anrufen, die hatte wahrlich gerade ganz andere Sorgen. Schließlich musste sie dafür sorgen, dass diese Erpresser endlich ihre Kohle bekamen, damit hier alle wieder weiterarbeiten konnten. So stellte sich Heinrich das zumindest vor. Oder warum sonst konnten sie noch immer nicht wieder auf ihre Daten zugreifen? Er verstand außerdem nicht, warum auch die Produktion still stand. Die war doch gar nicht in Wien, sondern saß im 200 Kilometer entfernten Wels, in einer eigenen Produktionshalle. Sein Klick auf das leere Word-Dokument war sicher nicht schuld daran, dass dort keine Router mehr gebrandet werden konnten! Das Dokument war doch außerdem leer gewesen? Was konnte da schon passieren?

Vanessa sah das offenbar anders. Sie rief Martina Meier sofort an. Die Marketing-Mitarbeiterin fiel auch gleich mit der Tür ins Haus. »Erinnerst du dich daran, dass Sabine und ich dir vor rund zwei Wochen eine Mail weitergeleitet hatten, die auf den ersten Blick so aussah, dass ich sie verschickt hätte?«

»Ja, ich erinnere mich dunkel, aber ich hatte damals keine Zeit, mir das näher anzusehen. Ich hatte es glaube ich Klaus auf den

Schreibtisch gelegt. Wieso? Ich dachte, Sabine hätte nicht drauf geklickt?«

»Sabine nicht, aber Heinrich Winter aus dem Vertrieb.«

»Oha!«

»Jedenfalls hat er mir gerade bestätigt, dass er das Word-Dokument geöffnet hat. Er sagte, dass es leer war.«

»Leer? Das muss ich mir jetzt doch näher ansehen und bei Klaus nachfragen. Bisher bin ich so beschäftigt gewesen damit, unser System wieder zum Laufen zu bringen, dass ich noch nicht rausfinden konnte, was eigentlich der Auslöser für den Ausfall des Systems war.«

»Das heißt, es könnte wirklich für die Erpressungsgeschichte relevant sein?«

»Ja, der Vorfall könnte eine Rolle spielen. Das muss ich mir genauer ansehen. Danke für deinen Anruf, Vanessa«, sagte Martina.

»Wie läuft es diesbezüglich?«

»Der Chef hat sich noch immer nicht entschieden, ob wir das Lösegeld bezahlen, oder nicht. Wir sind gerade dabei, mit externen Ransomware-Spezialisten alle Systeme komplett neu aufzusetzen. Mit der Produktion sind wir fast durch, die kann als Erstes wieder starten, ich schätze am Samstag. So wie es aussieht, werden die Mitarbeiter da auch das ganze Wochenende durcharbeiten, um die verloren gegangene Zeit aufzuholen.«

»War die Polizei eigentlich auch da?«

»Ja klar. Sie haben alles aufgenommen. Das Cyber-Team hat auch einen Blick darauf geworfen, aber nur, um uns zu bestätigen, dass es sich um eine bestimmte Sorte Ransomware handelt.«

»Und dann?«

»Naja, Anzeige gegen Unbekannt. Den Rest müssen wir selbst erledigen.«

»Spannend! Wie in einem echten Krimi.«

»Für mich ist es das auch: ein Krimi. Und Figgio ist das

Opfer.«

»Noch eine letzte Frage: Wann sind wir dran mit unserer Abteilung? Also wann können wir wieder arbeiten?«

»Der Rest der Firma ist sicher nicht vor nächster Woche wieder am Start. Wir können nur Schritt für Schritt vorgehen, und in der aktuellen Phase ist die Produktion wichtiger.«

»Verstehe ich. Glaubst du, wird es Figgio überleben?«

»Denke schon, aber ich bin keine Finanzexpertin.«

»Ach, ist das spannend! Darf ich dich noch was fragen?«

»Geht schon. Aber schnell«, lachte Martina und blickte auf die Uhr. Das Team neben ihr arbeitete fleißig, da konnte sie sich eine kurze Telefonpause gönnen.

»Wer steckt eigentlich dahinter? Wo sitzen die Erpresser, wer sind sie? Haben sie irgendwas von sich preisgegeben? In der Zeitung stand nur, dass es eine ganze Gang sein soll.«

»Das ist schwer zu sagen. Es gibt seitens der Polizei natürlich einen Verdacht, den Vorfall einer konkreten Gruppe zuzuordnen, aber da kann auch jemand ein Täuschungsmanöver durchgeführt haben. Im Cyber-Bereich ist das oft nicht so einfach zu erkennen.«

»Haben die Russen ihre Finger im Spiel?«

»Immer diese Geopolitik! Die Ransomware, die eingesetzt worden ist, ist tatsächlich von Russen geschrieben worden, aber das heißt nichts. Die ist nur ein Baustein von vielen … Der Angriff scheint insgesamt lange Zeit geplant gewesen. Das heißt auch, dass die Mail an Heinrich sicherlich nur ein Baustein war im Puzzle.«

»Aber warum ausgerechnet wir?«

»Du fragst mich schon genau dasselbe wie unser CEO, der am ersten Tag ordentlich die Nerven weggeschmissen hatte. Die Wahrheit ist: Es kann jeden treffen.«

Schweigen.

»Ich muss jetzt wieder weiter machen«, sagte Martina.

»Klar. Alles Gute noch«, antwortete Vanessa. »Toi toi toi!«

6

Vier Tage später.

Milan und Dennis klatschten ab. Beide lachten und freuten sich lautstark. Die Bezahlung von Figgio war auf ihrer Bitcoin-Wallet eingetroffen. Zehn Bitcoin hatten sie gefordert, das waren umgerechnet etwa 400.000 Euro, zumindest mit dem heutigen Tag. Der Kurs der Kryptowährung schwankte täglich. Für Figgio hatten die beiden eine eigene Wallet eingerichtet, damit Forensiker keine Rückschlüsse ziehen konnten, wenn sie das Kryptogeld weiterüberwiesen. Denn alle Bitcoin-Transaktionen sind öffentlich. Zwar weiß niemand, welches Pseudonym zu welcher realen Person gehört, aber trotzdem können Forensiker anhand digitaler Spuren Zahlungsflüsse nachvollziehen. Milan und Dennis wurden bisher aber nicht erwischt. Sie hofften, dass das mit ihrem ausgefinkelten System, wie sie mit den Bitcoins weiter verfuhren, auch so blieb. Am Ende würden ihnen rund 350.000 Euro übrig blei-

ben. Dennis plante mit dem Geld einen Urlaub in der Karibik, Milan wollte es in einen Wohnungskauf investieren. Die beiden Cybergangster jubelten, dass ihre Strategie Erfolg hatte. Jetzt blieb es nur noch zu hoffen, dass sie keine Spuren hinterlassen hatten.

7

Heinrich Winter nippte an seinem Cappuccino. Im Büro schmeckte er zwar nicht so gut wie zu Hause mit seinem Vollautomaten, aber er war trotzdem froh, wieder zurück zu sein, auch wenn sie jetzt, wo die Produktion wieder voll angelaufen war, viel Arbeit hatten. In seinem E-Mail-Postfach fand er eine Nachricht vom Chef: »Liebe Mitarbeiterinnen und Mitarbeiter! Wir sind zurück. Damit alle Systemabläufe wieder reibungslos funktionieren, ist es allerdings erforderlich, dass sie auf diesen Link klicken, um ihre Zugangsdaten zu bestätigen.« Heinrich wurde stutzig. Erst gestern war er von Martina Meier persönlich angerufen worden, in ihrer Rolle als Head of IT- und Security von Figgio. Diese hatte ihm mitgeteilt, dass seine vermeintlich leere Phishing-Mail nicht unwesentlich dazu beigetragen hatte, dass das Unternehmen erpresst worden war. Es drohen ihm keine Konsequenzen, hatte es geheißen und Heinrich war enorm erleichtert gewesen. Aber eine Standpauke hatte er sich trotzdem anhören dürfen und das Schulungsvideo zu Phishing musste er sich erneut ansehen. Diese Mail mit den Mitarbeiterinnen und Mitarbeitern kam ihm komisch vor, denn er hatte seine Zugangs-

daten bereits eingeben müssen, als er sich ins System eingeloggt hatte. Warum jetzt noch einmal? Martina Meier hatte ihm aufgetragen, ihr sofort alles zu schicken, was ihm merkwürdig vorkam und das tat er jetzt besser. Seinen Job würde er nämlich gerne behalten, falls Figgio diesen Vorfall finanziell überlebte. Er hatte wirklich nicht gedacht, dass wegen so einer Mail an ihn die gesamte Produktion stillstehen könnte und die Kunden nicht zu ihren Routern kämen. Heinrich griff zur Kaffeetasse, trank einen Schluck und atmete tief durch. Dann schickte er Martina Meier die Mail mit dem Betreff: »Phishing-Mail?«.

»Gut gemacht! Du hast dieses Mal das Richtige getan«, schrieb sie ihm zurück. Was Heinrich allerdings nicht wusste: Auch die Mail an die »lieben Mitarbeiterinnen und Mitarbeiter« hatte sie ihm höchstpersönlich ganz gezielt geschickt, um ihn zu testen. Aber das würde Martina dem lieben Heinrich selbstverständlich nicht verraten.

Nach dem Ransomware-Vorfall war das Unternehmen in einer schweren Krise, aber es sah vorerst nicht so aus, als würde irgendjemand akut seinen Job verlieren. Auch Martina – die Überbringerin der schlechten Nachrichten – konnte mit dem Verbleib in der Firma rechnen. Sie war sogar ausgesprochen gelobt worden für ihre professionelle Herangehensweise. Mit dem CEO hatte sie vereinbart, die Mitarbeiterschulungen aufzustocken und für alle Cybernotfälle ein Art »Stufenplan« zu erstellen sowie die Abwehrmaßnahmen zu stärken. Martina hatte zudem richtig entschieden, auch externe Security-Spezialisten hinzuzuziehen, denn so konnten die Erpresser wesentlich schneller aus dem internen Firmennetz zurückgedrängt und der Schaden so gering wie möglich gehalten werden. Der CEO dankte es ihr, indem er sie und ihr Team zu einem Abendessen einlud. Ganz nach dem Motto »auf die paar Euro kommt es jetzt auch nicht mehr an«, denn dass

sie das Geld an die Erpresser überweisen mussten, tat finanziell am meisten weh.

Doch Figgio konnte es sich nicht leisten, dass die Dokumente über ihre kommenden Produkte wirklich an die Öffentlichkeit gerieten. Es war die richtige Entscheidung gewesen, auch wenn die Polizei das freilich ein wenig anders sah und wenig begeistert davon gewesen war. Für das Cyber-Team bedeutete die Überweisung der Bitcoin freilich auch weitere Arbeit: Ein Team aus Forensiker hängte sich an das Bitcoin-Konto, um weitere Transaktionen zu beobachten. Schließlich war Figgio nicht die einzige Firma, die dieses Jahr bereits erpresst worden war. International war Ransomware zu einem immer größeren Problem geworden und die Cybereinheiten der Behörden arbeiteten hier über Ländergrenzen hinweg daran, die Netzwerke der Kriminellen zu entlarven.

8

Bei Milan und Dennis blinkte es am Bildschirm. Sie hatten eine Notiz erhalten, dass wieder jemand Login-Daten in ihrer Maske eingetragen hatte. »Wir haben Zugriff auf einen Account bei Mobility S«, sagte Dennis, als er an seiner Zigarette zog.

»Ja, dann, auf ein Neues!«

Was Milan und Dennis zu diesem Zeitpunkt noch nicht wissen konnten, war, dass ihnen über die Eingabemaske selbst jemand eine Schadsoftware untergejubelt hatte. Das würden sie erst in einigen Wochen merken, wenn sie plötzlich Besuch von der Polizei bekommen würden - nicht virtuell auf ihren Computern, sondern tatsächlich vor ihrer Haustür.

ÜBER DIE AUTORIN

Barbara Wimmer ist preisgekrönte Journalistin, Autorin und Speakerin. Sie schreibt und spricht über Netzpolitik, Datenschutz, Algorithmen, Künstliche Intelligenz, Social Media, Digitales und alles, was (vermeintlich) smart ist.

https://barbara-wimmer.net