KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen

Cyber-Erpressungen – Hacker-Angriffe auf Unternehmen

Von Jörg Hommer

Sendung vom: Dienstag, 14. September 2021, 8:30 Uhr
Redaktion: Gábor Paál
Regie: Günter Maurer
Produktion: SWR 2021

Leere Regale in Supermärkten, Benzin-Engpässe – Auch Verbraucher bekommen Cyber-Erpressungen zu spüren. Es geht um Riesen-Summen. Fachleute sind sich einig: In Deutschland wird noch zu wenig dagegen getan.

MANUSKRIPT

Musikakzent

Sprecherin:
Ein Hacker-Angriff auf das Firmennetzwerk. Die Daten verschlüsselt, unter Kontrolle von Erpressern.

O-Ton Thomas Pilz:
Der Ablauf war kinoreif. Der Leiter der IT-Abteilung hat mich gegen 15 Uhr angerufen, da war ich gerade bei „Julius Zappelquatsch“ mit meiner Tochter, und da habe ich gehört, wir haben einen Cyber-Angriff und wir sind alle in der Firma.

Sprecherin:
Thomas Pilz eilt in die Firmenzentrale, ahnt Schlimmes. In den Büros herrscht Panik. Auf jedem Bildschirm die gleiche Meldung: „Ihre Daten wurden verschlüsselt“.

O-Ton Thomas Pilz:
Erst als ich dann in der Firma war und gesehen habe, wie alle rumrennen und Stecker ziehen, war bei mir klar: Jetzt brennen wir, und zwar lichterloh. Unsere gesamte Arbeit der letzten Jahre ist fort. Wir können gerade mal von null anfangen, wenn wir die Daten nicht wiederbekommen.

Ansage:
Cyber-Erpressungen – Hacker-Angriffe auf Unternehmen. Von Jörg Hommer.

Sprecherin:
Der US-amerikanischen Daten-Plattform „chainalysis“ zufolge wurden allein im Pandemiejahr 2020 umgerechnet über 334 Millionen Euro Lösegeld an Cyberkriminelle in Kryptowährungen gezahlt. Eine Verdreifachung zum Vorjahr. Die Zahlen sind letztlich unsicher – zu groß ist die Dunkelziffer. Viele Betroffene melden einen Cyberangriff erst gar nicht – aus Angst vor Reputationsschäden.

O-Ton Carsten Meywirth:
Wir konnten in den vergangenen Monaten schon feststellen, dass insbesondere die Bedingungen der Corona-Pandemie ein Beschleuniger für Cybercrime gewesen ist. Denn Kriminellen haben sich durch die Digitalisierungsnotwendigkeiten viel mehr Möglichkeiten geboten, vielmehr Angriffsflächen. Und die haben das sehr gut ausgenutzt.

Musikakzent

Sprecherin:
Das Bundesamt für Sicherheit in der Informationstechnologie, kurz BSI, in Bonn fand in einer aktuellen, repräsentativen Umfrage unter 1000 Unternehmer heraus, dass fast jedes zehnte Unternehmen auf Cyberangriffe während der Pandemie reagieren musste. Davon gaben rund ein Viertel der Befragten an, dass sie durch Cyber-Angriffe schwere oder existenzbedrohende Schäden erlitten.

Die Digitalisierung der Gesellschaft durchdringt mehr und mehr alle Lebensbereiche. Das Corona-Jahr 2020 sorgte für einen regelrechten Boom in der digitalen Kommunikation. Allerdings steigt damit auch das Risiko, Opfer von Cyberkriminellen zu werden.

Ende April 2021 schlagen Hacker bei der deutschen Supermarktkette „tegut“ zu. Die anonymen Hacker fordern Lösegeld für die Rückgabe der Daten. Ungewöhnlich schnell informiert „tegut“ seine Kunden auf Plakaten und Stelltafeln vor und in den Supermärkten.

Zitator (Stimme verfremdet):
Unbekannte haben einen sogenannten Cyberangriff auf das IT-Netzwerk des Unternehmens verübt. Sämtliche IT-Netzwerksysteme der Zentrale sind daraufhin gemäß Notfallplan heruntergefahren und vom Netz genommen worden. Hiervon betroffen sind unter anderem die Warenwirtschaftsprogramme, die in der Logistik die Disposition steuern.

Sprecherin:
Das stürzt vor allem das Zentrallager ins Chaos. Die Folge ist für tegut-Kunden allerorts in den Filialen spürbar – wochenlang. Lieferengpässe führen zu leeren Regalen, handgeschriebene Preisschilder, keine Aktionspreise.

O-Ton Kunden:
Wenn Sie mal durchgehen, manche Regale sind einfach leer. // Hab mich nur gewundert, dass die Regale etwas leerer sind als üblich. // Hauptsächlich im Kühlthekenbereich."

Sprecherin:
Nur drei Wochen später die nächste Eskalation: Die Hacker veröffentlichen sensible Unternehmens- und Kunden-Daten im Internet. Einsehbar für jedermann, auch für die Konkurrenz. Der Gau für die milliardenschwere Supermarktkette. – In einer Pressemitteilung erklärt der „tegut“-Geschäftsführer Thomas Gutberlet:

Zitator:
Wir leisten kriminellen Machenschaften keinen Vorschub und lassen uns auf keine Verhandlungen mit Kriminellen ein. Wir sind uns gleichwohl unserer Verantwortung bewusst und unternehmen alles, um Kunden, Mitarbeiter und unsere Geschäftspartner zu schützen.

Sprecherin:
Auf keinerlei Lösegeldforderungen einzugehen, das rät auch Carsten Meywirth, der Leiter der Abteilung Cybercrime beim Bundeskriminalamt in Wiesbaden. Vor allem Attacken mit sogenannter Ransomeware haben zurzeit Hochkonjunktur.

Das Wort „Ransomeware“: setzt sich zusammen aus den englischen Wörtern „Ransome“ für Lösegeld und „Software“ für Programm.

O-Ton Carsten Meywirth:

Ransomeware ist ein Schadcode, den Täter einsetzen, um in einem Unternehmen Daten und Rechnersysteme zu verschlüsseln. Die Täter gehen regelmäßig so vor, dass sie entweder im Darknet oder einer anderen Varianten kompromittierende Zugangsdaten einkaufen, diese dann nutzen, um in die Unternehmens- oder Behördennetzwerke einzudringen. In der ersten Zeit schauen sie sich da um in diesen Netzwerken und sammeln Informationen, gucken, wo sie da angekommen sind, wieso und solvent das Unternehmen ist, wo vielleicht das größte Erpressungspotenzial liegt anhand der Daten, die sie dort auffinden.

Musikakzent

O-Ton Carsten Meywirth:
Ganz häufig befinden sich die Täter mehrere Wochen, bevor das Opfer dann auch die Kenntnisse erhält von der Verschlüsselung der Daten, in dem Unternehmensnetzwerk. Die Täter exfiltrieren dann die Daten, um eine spätere Erpressung vorzubereiten. Wir hier bewerten diese Angriffe als größte Bedrohung für die Wirtschaft im Augenblick.

Sprecherin:
2020 zählten deutsche Sicherheitsbehörden mehr als hunderttausend Cyberangriffe in Deutschland. Knapp 300 pro Tag. In einer Studie des Vereins „Deutschland sicher im Netz“ gaben 46 % der Unternehmen an, schon mindestens einmal von Cyberkriminellen angegriffen geworden zu sein.

Niemand scheint mehr sicher vor der Gefahr aus dem Netz: Ob globaler Konzern, kleiner Handwerksbetrieb oder öffentliche Verwaltung. - Wenn Hacker angreifen, tickt die Uhr für ihre Opfer: Wie lange kann sich ein Unternehmen den Produktionsausfall leisten? Was passiert mit den geklauten Daten? Lösegeld zahlen – ja oder nein?

Moderationscollage Tagesschau:
„Hacker haben eine US-Pipeline lahmgelegt. Der Transport von Benzin und Diesel musste eingestellt werden.“ (9.5.21)

„Die Behörden haben im Zusammenhang mit der Bundestagswahl vor Cyberangriffen und Desinformations-Kampagnen gewarnt.“ (25.5.21)

„Ein Hacker-Angriff in den USA hat auch in Europa Folgen. Auch in Deutschland könnten nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik morgen Auswirkungen spürbar werden.“ (4.7.2021)

Sprecherin:
Immer häufiger bekommen auch Kundinnen und Kunden von Unternehmen Cyberangriffe direkt zu spüren, werden quasi zu Opfer zweiten Grades. Das erhöht den Druck wiederum bei den Erpressten Unternehmen. Offenbar mit Erfolg: Nach tagelangen Benzin-Engpässen an Tankstellen, zahlt der erpresste US-amerikanische Öl-Pipeline-Betreiber „Colonial“ Lösegeld in Millionenhöhe. Und nur wenige Wochen später trifft es „JBS“, den größten Fleischkonzern der Welt.

O-Ton Felix Freiling:

Der Großteil der Schadsoftware-Infektionen passiert dadurch, dass die Opfer die Schadsoftware selbst installieren, dadurch, dass sie reingelegt worden sind im guten Glauben, irgendwas anderes zu installieren, installieren Sie dann eine Schadsoftware.

Sprecherin:
Felix Freiling von der Friedrich-Alexander-Universität in Erlangen erklärt, dass ein Cyber-Angriff jedem passieren kann, niemand davor wirklich geschützt ist.

O-Ton Felix Freiling:
Also es geht zum Beispiel dadurch, dass man E-Mails bekommt, die einem irgendetwas versprechen, wenn man auf einen Anhang klickt oder eine Software installiert. Oder wenn man auf einer Webseite geht, die einem suggeriert, dass der eigene Rechner von Schadsoftware befallen ist, und um die Schadstoffsoftware loszuwerden, muss man eine Software installieren. Und das ist Paradoxe. Durch die Installation dieser Software kriegt man eigentlich erst die Schadsoftware, die man eigentlich suggeriert bekommt loszuwerden.

Atmo:
Produktionshalle Firma Pilz

Sprecherin:
So oder ähnlich muss es auch beim schwäbischen Mittelständler Pilz aus Ostfildern gewesen sein. Das Familienunternehmen ist Spezialist für Automatisierung von Maschinen und Transportmittel, wurde im Herbst 2019 Opfer eines gewaltigen Hacker-Angriffs. Wir treffen die Geschäftsführer Thomas Pilz und Susanne Kunschert zum ersten Mal rund zehn Wochen nach der Verschlüsselungs-Attacke. Sie gehören zu den wenigen Unternehmern, die offen über einen Cyberangriff auf ihren Betrieb sprechen.

O-Ton Thomas Pilz:
Das ist, wie wenn man in einem Albtraum ist, den schlimmsten Albtraum, den man sich vorstellen kann, nur dass der dann real ist. Unsere gesamte Arbeit der letzten Jahre ist fort. Wir können gerade nochmal von vorn anfangen, wenn wir die Daten nicht mehr bekommen.

Musikakzent

Sprecherin:
Mit der Verschlüsselung der Daten beginnt ein Wettlauf gegen die Zeit. Thomas Pilz ruft persönlich die 42 Niederlassungen weltweit an. Eine emotionale Achterbahnfahrt zwischen Hoffen und Bangen beginnt.

O-Ton Thomas Pilz:
Ja, wir haben noch Computer..., super aufpassen, wir haben einen Cyber-Angriff. Nächster Anruf. England, habt Ihr noch Computer? Ist England noch da? Ja, England ist noch da. Okay. Eine Stunde später ruft England an: Tut uns leid, wir sind auch weg. Wir haben auch verschlüsselte Rechner. Dann kommt Amerika, Amerika ist

weg... China ist weg. Und dann kriegen Sie da so eine Liste taktaktaktaktak. Und dann guckt man sich an und sagt im Lagezentrum, verdammt, die haben uns alle. Und dann sind Sie erst mal fertig mit der Welt.

Sprecherin:
Das millionenschwere Unternehmen in der Hand von kriminellen Erpressern. Tagelang stehen im Oktober 2019 die Maschinen und Rechner still. Die Lage ist unübersichtlich. 2500 Mitarbeiter bangen um ihren Arbeitsplatz.

O-Ton Mitarbeiter*innen der Firma Pilz:
Die normalen Sachen, die du immer hast, Deinen PC, Deinen Rechner war plötzlich aus. Und da habe ich mir eigentlich gedacht, au, jetzt wird's happig. Und nachdem wir dann gehört haben, dass die Programme einfach weg sind, dass du sie nicht mehr benutzen kannst … // Dass es heißt, das war´s. Die Firma kriegen wir so nicht mehr zu laufen. Das waren eigentlich meine Ängste. // Was für Leute machen sowas, und setzen im Prinzip deinen Arbeitsplatz, den Arbeitsplatz von Tausenden von Leuten aufs Spiel?

O-Ton Thomas Pilz:
Für mich war es das Schwierigste, die Leute wieder nach Hause schicken zu müssen."

O-Ton Susanne Kunschert:
Die Ängste in der Zeit, die waren enorm bei den Mitarbeitern. Sicherlich, das war schon traurig und beängstigend, auch den leeren Parkplatz einfach zu sehen.

Sprecherin:
Ähnlich erging es dem Unternehmen Marabu aus Tamm bei Ludwigsburg. Gegen einen Hacker-Angriff wähnte man sich hier eigentlich in Sicherheit, erklärt York Boeder, der Geschäftsführer.

O-Ton York Boeder:
Ich will nicht sagen, dass wir vorher völlig unbesorgt waren. Aber es war weit weg. Wir haben uns bewusst eine Cyberattacke mal auf uns simulieren lassen, das Ergebnis dieses externen Angriffs war, unsere Systeme funktionieren.

Musikakzent

Sprecherin:
Bis zum 29. November 2019. Ein Freitag. Mitten im Weihnachtsgeschäft. Die Produktion läuft in Doppelschichten auf Hochtouren, auch am Wochenende. – Und scheinbar von einem Moment auf den anderen übernehmen Hacker in rasender Geschwindigkeit die Kontrolle über das Unternehmen, verschlüsseln alle Daten und schalten alles ab.

Atmo:
Produktionshalle von Marabu

Sprecherin:
In der IT-Abteilung von Marabu herrschte das blanke Entsetzen, erinnert sich Stephan Württemberger:

O-Ton Stephan Württemberger:
Kein Telefon, kein Produktionsband, keine Maschine, die Farbe herstellt, keine Schranke, keine Türe, die mehr aufgeht. Man kann es sich vorstellen: Alles ist dunkel. Es hat uns wirklich eiskalt erwischt. Ich glaub niemand ist auf sowas wirklich vorbereitet. Wenn Sie gehacked werden, dann haben Sie ja gar keine Kontrolle mehr drüber, was geht oder was geht nicht?

Sprecherin:
Aus der Original-Erpresser-Nachricht:

Zitator verfremdet:
Wir sind in Ihr Netzwerk eingedrungen. Alle Daten sind in Ihrem Netzwerk verschlüsselt. Alle Back-Ups ebenfalls, oder gelöscht. Wir haben exklusiv die Entschlüsselungssoftware für Sie. Sie werden keine andere öffentlich zugänglich finden. Sie sollten innerhalb der nächsten 48 Stunden mit uns Kontakt aufnehmen, je schneller sie Kontakt aufnehmen, desto geringer der Preis.

Atmo:
Produktionshalle von Marabu

Sprecherin:
Wie bei Pilz kann auch hier und an den zwölf Niederlassungen weltweit kein Auftrag bearbeitet werden. Tagelang verlässt keine Ware das Lager. Und mit jedem weiteren Tag steigt der Druck.

O-Ton York Boeder:
Der Druck seitens der Kunden war immens. Wir waren mitten in der Hochsaison. Wir haben tatsächlich einige Kunden gehabt, die uns nicht gedroht haben, aber die uns gesagt haben, wenn Ihr jetzt nicht schafft, lieferfähig zu werden wieder, dann werden wir keine andere Alternative mehr haben, als notgedrungen umzustellen und dahin große Kunden dran. Also große, renommierte Spielzeughersteller, große, renommierte Automobilkonzerne, die gesagt haben, Ihr müsst jetzt liefern. Wenn Marabu über einen langen Zeitraum tatsächlich nicht lieferfähig wäre, dann wäre sein Unternehmen tatsächlich in seiner kompletten Existenz vernichtet.

Sprecherin:
Genau wie Pilz ist auch Marabu im Herbst 2019 in seiner Existenz gefährdet. Das wissen die anonymen Erpresser aus dem Internet. Die Zeit ist ihr Komplize, ihre Geisel die existenziellen Daten des Unternehmens. In ihrem Erpresserbrief schreiben die Cyberkriminellen wortwörtlich:

Zitator (verfremdet):
Je schneller sie uns kontaktieren, desto niedriger der Preis.

Sprecherin:
Es folgen genaueste Instruktionen, wie ein Geschäft zustanden kommen kann.

O-Ton York Boeder:
Die, die Sie da erpressen, die Sie auch sabotiert haben, agieren eigentlich mehr wie ein freundlicher Dienstleister. Man benutzt auch nicht das Wort Erpressung, sondern in der Regel ist es eher so, dass die Ihnen Hilfe anbieten, dass man wieder alles zum Laufen bringen kann. Wir haben denen gesagt, wir werden nicht verhandeln. Wir werden einen eigenen Weg wählen. Wir lassen uns nicht erpressen, und die haben gesagt: Seien Sie vorsichtig. Sie werden ihre Entscheidung möglicherweise in ein paar Tagen noch einmal überdenken wollen.

Sprecherin:
York Boeder kann sich ausrechnen, was jeder einzelne Tag Produktionsausfall das Unternehmen kostet. Was ist der beste Weg: den Erpressern nachgeben oder zahlen, um sich so schnell wie möglich aus der Existenz bedrohenden Situation zu befreien?

O-Ton York Boeder:
Das erste Bauchgefühl war: Wir lassen uns nicht erpressen. Das war die erste und ganz spontane Reaktion. Man hat ja irgendwie Prinzipien, und die stellt man erst mal im ersten Moment über alles. Aber wenn Sie ein Familienunternehmen leiten, an dem über 500 Arbeitsplätze hängen, Mitarbeiter, die seit über 30 Jahren für uns tätig sind, und Sie setzen auch diese Arbeitsplätze aufs Spiel, dann, sage ich Ihnen, fangen schlaflose Nächte an."

Musikakzent

Sprecherin:
Zurück zu Pilz: Die gesamte Existenz des Familienunternehmens hängt im Herbst 2019 an einem seidenen Faden. Die Erpresser fordern ein sechsstelliges Lösegeld.

O-Ton Susanne Kunschert:
Nur so viel ist gesagt, dass die Erpresser einen Betrag verlangen, den wir zahlen, also den wie gut hätten zahlen können. Die Erpresser verlangen so viel Geld, dass das natürlich funktioniert, weil sonst wäre es ja auch kein Erfolgsmodell, wenn sie zuviel verlangen würden. Von daher hätten wir den Betrag natürlich zahlen können.

O-Ton Carsten Meywirth:
Ich weiß, dass das für ein Unternehmen eine ganz schwierige Entscheidung ist in dieser sehr chaotischen Phase, wenn man feststellt, dass man keinen Zugang mehr zu den Daten hat. Und das ist natürlich immer irgendwo eine wirtschaftliche Abwägung für ein Unternehmen. Wir empfehlen ganz klar, kein Lösegeld zu zahlen. Sie verhandeln hier nicht mit seriösen Geschäftspartnern, sondern mit Kriminellen. Sie wissen nicht, ob Sie tatsächlich danach die Daten von den Tätern zur Verfügung gestellt bekommen. Diese Täter wissen, wenn Sie einmal gezahlt haben, zahlen Sie möglicherweise auch das nächste Mal, und kommen wieder.

Sprecherin:
Im Jahr 2021 zahlten der Pipeline-Betreiber Colonia und der Fleischkonzern JBS gemeinsam umgerechnet über 12 Millionen Euro in Kryptowährung. Und Rekordverdächtige 60 Millionen Euro in Bitcoin fordern nur kurze Zeit später im Sommer 2021 die mutmaßlichen russischen Hacker, die den US-IT-Spezialisten Keysaya angriffen haben. Und das sind nur die bekannten Fälle.

Musikakzent

Sprecherin:
Experten und Ermittler beobachten zunehmend, dass sich eine Art eigene, kriminelle Ökonomie in der Schattenwelt des Internets, dem Darknet etabliert hat, erklärt der Leiter der Abteilung Cybercrime beim BKA, Carsten Meywirth.

O-Ton Carsten Meywirth:
Was das Täterverhalten anbelangt, beobachten wir schon seit einiger Zeit, dass die Täter sich professionell organisieren. Es ist eine sogenannte Underground Economy entstanden, mit sehr vielen kriminellen Dienstleistungen, wo die Täter eine Tatplanung und Ausführung nicht mehr von Anfang bis Ende alleine durchführen, sondern wo sie Dienste anderer Krimineller in Anspruch nehmen. Beispielsweise gibt es sehr spezialisierte Tätergruppen, die Schadsoftware produzieren. Es gibt Täter, die diese Schadsoftware dann prüfen, ob sie von den gängigen Antiviren-Systemen erkannt wird.

Sprecherin:
Die sogenannte Underground-Economy macht es vor allem auch möglich, dass Kriminelle ohne Computerkenntnisse zu Cyberkriminellen werden können. Wie umfassend das Angebot von Dienstleistungen für Cyberkriminalität ist, zeigt uns Benjamin Mejri, ein Experte für IT-Sicherheit aus Kassel, auf einem riesigen Monitor in seiner Schaltzentrale.

O-Ton Benjamin Kunz-Mejri:
Hier haben wir zum Beispiel eine Kaste von Ransomware. Die wird für 320 Dollar angeboten. Dort ist es möglich, einzelne Kampagnen zu starten. Das Programm kann selber bearbeitet werden.

O-Ton Autor:
Also für 320 Dollar. Kann ich jetzt quasi schon einen Handwerksbetrieb oder eine kleine Firma lahmlegen?

O-Ton Benjamin Kunz-Mejri:
Definitiv. Sie könnten sich jetzt diese kaufen und ihre eigenen Erpressungs-Beträge, ihre eigenen E-Mail-Kontakte eintragen und könnten dann auch die Software gegen jedes Unternehmen abfeuern.“

Sprecherin:
In seiner Kommando-Zentrale für Cybersicherheit hängen sechs riesige Monitore. An einigen laufen Ticker über aktuelle Cybergefahren in Echtzeit. An anderen eine

Weltkarte die laufenden Cyberangriffe visualisiert: Wie ein Spinnenfaden spannen sich die Fäden zu einem Netz über die Erdteile zusammen.

Ein Mitarbeiter überwacht 24 Stunden, jeden Tag die Aktivitäten im Netz. Im Auftrag der Kunden von Benjamnin Mejri, deren Sicherheit er gewährleistet, und sie rechtzeitig warnen kann.

Auffallend sei, dass sich die Hacker spezialisieren. Ganz wie in der legalen Wirtschaft, sich die Arbeit aufteilen.

O-Ton Benjamin Kunz-Mejri:
Das hat zur Folge, dass die Masse auf Dauer ansteigt, weil einfach immer professionellere Verschlüsselungssoftware oder allgemein Schutz Software entwickelt wird. Und natürlich, da dadurch auch die Frequenz der Einschläge bei Unternehmen zum Beispiel steigt. Das heißt, umso mehr Ransomeware programmiert wird, umso arbeitsteiliger agiert wird. Umso schneller können diese Gruppen andere Unternehmen angreifen und umso zügiger und lukrativer wird natürlich auch das Geschäft im Allgemeinen.

Sprecherin:
Auch das trage zum Anstieg der Cyberkriminalität bei, so die Experten. Und dass die Angreifer oft aus Ländern stammen, in denen sie keine ernstzunehmende Strafverfolgung fürchten müssen.

O-Ton Felix Freiling:
Es ist kein Geheimnis, dass in bestimmten Staaten wie zum Beispiel Russland es eine sehr starke IT-Sicherheitsindustrie gibt. Es ist auch bekannt, dass diese Kompetenzen auch vom Staat genutzt werden und dass in gewisser Weise Leute auch oder Firmen zum Bruttosozialprodukt dadurch beitragen, solange sie nicht innerhalb von Russland hacken. Im Ausland ist alles okay. Insofern ist es in manchen Staaten ein nicht unerheblicher Teil des Bruttosozialprodukts, der durch Cyber-Kriminalität auch verdient wird.

Musikakzent

Atmo:
Büro Pilz, Tastaturtippen

Sprecherin:
Thomas Pilz und seine geschäftsführende Schwester wollen keinen Bitcoin dazu beitragen, dass die Kriminellen durch Erfolge bestärkt werden. Sie entscheiden sich für den riskanteren Weg: kein Kontakt zu Erpressern, keine Lösegeldzahlung. Sie machen den Cyberangriff öffentlich und schalten die Polizei ein.

O-Ton Thomas Pilz:
Als dann gezeigt wurde, da ist die Seite, da ist die Internetadresse oder Telefonnummer mit Namen, wo wir erfahren können, für welches Geld wir unsere Daten wieder zurückhaben können, bin ich in den Kampfmodus gegangen. - Wir

haben uns dann kurzgeschlossen, wie groß ist das Risiko? Ja, das Risiko ist, wir verlieren das Unternehmen. Aber nein, das geht nicht. Und da ist dann auch schon eine gehörige Portion Wut über diese unverschämten Kerle da, die einen antreibt. Und als Unternehmer hat man ja immer das Risiko, dass man einen Fehler macht, der einen das Unternehmen kostet. Und in dem Moment gab es nur eins: keinen Millimeter dem Verbrechen nachgeben.

Sprecherin:
Kriminalhauptkommissar Daniel Lorch von der Polizeidirektion Reutlingen ermittelt vom ersten Tag an im Fall Pilz. Für ihn ist der Fall um den schwäbischen Mittelständler einer der größten der letzten drei Jahre.

O-Ton Daniel Lorch:
Die Nadeln dann in diesem digitalen Heuhaufen zu finden, das ist nicht so ganz einfach.

Sprecherin:
Eigene Abteilungen für Cyberkriminalität gibt es mittlerweile in vielen Polizei-Dienststellen. Auch das ein weiteres Zeichen für die Alltäglichkeit von Hacker-Angriffen. Und wie bei Einbrüchen oder Gewaltverbrechen ist auch bei Angriffen aus dem Netz die schnelle Spurensuche fundamental wichtig. Denn auch Cyberkriminelle hinterlassen Spuren im Netz.

O-Ton Daniel Lorch:
Und dann setzt im Prinzip direkt auch schon die Ermittlungsarbeit an. Das heißt, die IT-Forensiker kommen und sagen, ich habe eine IP-Adresse, von dieser IP-Adresse aus hat der Täter auf die Firma zugegriffen.

Sprecherin:
Die Ermittlungsgruppe rund um Daniel Lorch nennt sich „Seta", zu Deutsch Pilz. Sie finden heraus, dass die Hacker bereits Monate vor dem eigentlichen Angriff in die Pilz-IT-Infrastruktur eingedrungen sind.

O-Ton Daniel Lorch:
Die Täter halten sich ja in den Ziel-Infrastrukturen auf, das hat den Hintergrund, die wollen größtmöglichen Schaden anrichten, weil wenn größtmöglicher Schaden angerichtet ist, ist die Zahlungsbereitschaft entsprechend hoch.

O-Ton Thomas Pilz:
Da ist tatsächlich ein Fremder bei uns umhergewandelt, im Internet, in der virtuellen Firma Pilz, und keiner von uns hats gemerkt, und dann hat er zugeschlagen.

O-Ton Susanne Kunschert:
Ich finde das sehr, sehr ein bedrohliches Gefühl zu wissen. Jemand beobachtet einen, und bei uns war ganz, ganz klar, dass diese Verbrecherbande uns wirklich kennt. Die kennen unsere Hierarchien, die die, die, die, die müssen alles gewusst haben von uns. Und das finde ich jetzt sehr unangenehm, unangenehmes Gefühl,

dass das jemand, der Böses im Sinn hat, einen monatelang ausspioniert, und du weißt es überhaupt nicht.

Sprecherin:
Der Wiederaufbau der gesamten IT-Infrastruktur bei Pilz ist riskant. Denn unklar ist, ob er gelingt. Über Wochen funktionieren selbst die einfachsten IT-Anwendungen nicht mehr.

O-Ton Laslo (Mitarbeiter der Firma Pilz):
Wir schwer es plötzlich ist, ein Dokument auszudrucken oder eine Datei von A nach B zu schieben, ohne IT-Infrastruktur, da kann einem schon angst und bange werden.

O-Ton Autor:
Also, wenn du hier hidden files machst, dann muss eigentlich alles da sein.

O-Ton Laslo (Mitarbeiter der Firma Pilz):
Genau da sind die Attachements, die du wieder herstellen musst, damit man wieder arbeiten kann.

Sprecherin:
Die wichtigsten Bausteine für den Wiederaufbau der IT-Infrastruktur: alte Dateien aus nicht infizierten Laptops, Sicherheitskopien, die vor dem Ersten Eindringen der Hacker erstellt wurden, und damit von der Schadsoftware nicht befallen sind.

Eine mühsame Sisyphusarbeit, die die Mitarbeiter über Wochen Im Drei-Schichtbetrieb beschäftigen wird. Manche Daten bleiben allerdings für immer verloren. Ein nicht bezifferbarer Schaden.

O-Ton Jakob (Mitarbeiter der Firma Pilz):
Plötzlich haben wir gemerkt, wir müssen von Null aufsetzen. Und das ist eine existenzielle Angst, die da entsteht. Das ist die Angst des – wenn wir jetzt alles verloren haben – wir können ja jetzt nicht alle Produkte neu entwickeln, wir können ja nicht alle bei null anfangen, wir müssen irgendwo einen Punkt finden.

Sprecherin:
Sie finden diesen Punkt. Schritt für Schritt, aber stetig geht es in den Wochen nach der Cyberattacke aufwärts bei Pilz. Nach sechs Wochen laufen wieder die ersten Maschinen. Es dauert allerdings noch Monate, bis weit in das Jahr 2020, bis der Cyberangriff vollständig überstanden ist.

Musikakzent

Sprecherin:
Mehr als ein Jahr nach der Cyberattacke sind wir wieder bei der Pilz AG. Mittlerweile hält das Corona-Virus die Welt in Atem. Pilz-Geschäftsführerin Susanne Kunschert kann dem Cyberangriff mittlerweile sogar etwas Positives abgewinnen.

O-Ton Susanne Kunschert:

Es hat uns einen unglaublichen Digitalisierungsschub gegeben, der jetzt in der Corona-Zeit unglaublich wichtig ist. D.h. groteskerweise könnte man formulieren, dass der Cyberangriff uns auf die Corona-Krise vorbereitet hat.

Sprecherin:
Auch Marabu schafft den Weg aus der Krise, ohne Lösegeld zu zahlen. Sie verlieren auch keine Kunden nach dem Produktionsausfall. Geschäftsführer York Boeder schaut allerdings Monate nach dem Angriff selbstkritisch in die Zukunft.

O-Ton York Boeder:
Man stellt sich natürlich vielfach die Frage: Habe ich denn mittlerweile genug getan, also z.B. wie beim physischen Einbruch, dass man dann vielleicht anfängt, ein paar Gitter vor die Fenster zu machen, ein zusätzliches Schloss einzubauen – genauso läuft es ja in der Cyberwelt genauso ab. Man baut dann eine zusätzliche Firewall. Man baut sich Notfallsysteme, aber letztlich weiß man, der Einbrecher ist ja weiterhin da. Man versucht, sich halt besser abzuschotten. Aber deswegen wird ja die Welt der Einbrecher nicht aussterben. Das heißt, die Einbrecher rüsten parallel ja auch auf und versuchen doch wieder, einen Eintritt in Ihr System zu kriegen.

Sprecherin:
Experten sind sich einig: In Deutschland wird noch zu wenig in IT-Sicherheit investiert, – die Gefahr durch Hacker-Angriffe unterschätzt. Ein kleiner Handwerksbetrieb mit eigener IT-Abteilung ist wohl kaum finanzierbar. Regelmäßige Sicherheitskopien wichtiger Unternehmens- und Kundendaten sind allerdings möglich.

O-Ton Felix Freiling:
Die breite Cyberkriminalität, die heute auch den großen Schaden anrichtet, ist eigentlich etwas, was man nicht durch irgendwelche Repression in den Griff bekommen kann, sondern durch Prävention. Also man muss präventives Verhalten an den Tag legen, um nicht Opfer von Kriminalität zu werden. Und das bedeutet im Prinzip, nicht auf alles zu klicken, was einem im Internet begegnet.

Sprecherin:
Felix Freiling von der Universität Erlangen ist davon überzeugt, dass vor allem die Mitarbeiter für Cyberangriffe sensibilisiert werden müssen. Und dennoch bleibt ein Restrisiko, sagt auch York Boeder, Geschäftsführer von Marabu.

O-Ton York Boeder:
Dieses unbehagliche Gefühl, man kann hier erneut angegriffen werden, das bleibt, das wird auch wahrscheinlich immer bleiben. Ich glaube, es wird nicht nochmal genauso passieren, dafür haben wir zu viele Dinge verändert und auch verbessert. Aber wer glaubt, er hat das einmal hinter sich und das passiert nie wieder, der lebt nicht in dieser Welt.

Abspann:
Musikbett mit SWR2 Wissen

Sprecherin:
Cyber-Erpressungen – Hacker-Angriffe auf Unternehmen. Von Jörg Hommer. Sprecher: Hede Beck und Rudolf Guckelsberger. Redaktion: Gábor Paál, Regie: Günter Maurer.

Abbinder

*****