„Ooops“

Internet Nach der bislang größten Cyberattacke suchen Fahnder unter Hochdruck die Urheber der Erpressungssoftware „WannaCry“. Neue Angriffswellen könnten folgen. Das Schreckensszenario eines globalen Kontrollverlusts wird vorstellbar.

Milosz Matusiak wollte abends gerade sein Notebook zuklappen und schlafen gehen, als ihm ein seltsames Symbol auf seinem Monitor auffiel: zwei sich schüttelnde Hände, wie zum freundlichen Abschluss eines guten Geschäfts, dazu ein merkwürdiger Dateiname: „Wana Decrypt0r 2.0“.

Der 30-Jährige trennte seinen Rechner sofort vom Internet. Zunächst war er nur verwundert: „Ich hatte ja keine komischen E-Mail-Anhänge angeklickt und war auch nicht auf halbseidenen Seiten unterwegs.“ Der Schock kam am nächsten Morgen. Auf dem PC seiner Mutter ging nichts mehr, von wegen freundliche Geschäfte: Der Bildschirm zeigte eine Lösegeldforderung.

Offenbar war ihr Rechner zuerst infiziert worden. Von dort hatte sich das Schadprogramm auf sein Notebook übertragen, über das gemeinsam genutzte WLAN-Netz. Lösegeld wollte die Familie nicht zahlen. Nun sind die Urlaubsfotos, Bewerbungsunterlagen und Videos der Hamburger wohl für immer weg, unleserlich gemacht. „Ich hätte nie gedacht, dass mir so etwas passieren kann“, sagt Matusiak.

Seine Mutter und er sind Opfer eines massiven Cyberangriffs, der seit einer Woche weltweit für Aufsehen sorgt – Europol zufolge ist es der bislang größte überhaupt. In die Chroniken wird er als „WannaCry“ („Willst du weinen“) eingehen, eine hämische Kurzformel des Dateinamens, den die Opfer auf ihren Rechnern fanden.

Wie eine Epidemie im Zeitraffer breitete sich der erpresserische Computercode der Gattung „Ransomware“ aus, lautlos, unheimlich und rasend schnell. Innerhalb nur einer Stunde waren weltweit bereits mehr als 7000 Rechner befallen, als die Attacke am 12. Mai begann. Danach gab es erst einmal kein Halten mehr. Je mehr Computer infiziert wurden, desto schneller breitete sich der Schädling aus.

Weltkarten der Experten zeigen das Ausmaß des Desasters: Europa ist unter zahllosen Warnpunkten verschwunden, die USA und Indien leuchten schrill, ebenso Teile Russlands, Chinas und Südamerikas.

Steckt die berüchtigte Hackergruppe Lazarus dahinter, die in der Vergangenheit für Nordkorea gearbeitet haben soll? War es eine kriminelle Cybermafia, der es um möglichst viele Bitcoins ging? Oder ein 16-jähriger Hacker in seinem Kinderzimmer?

Noch sind die Schuldigen nicht identifiziert, noch durchforsten Sicherheitsbehörden und Computerforensiker den Schadcode nach kleinsten Hinweisen – und noch ist nicht abzusehen, wie viele Angriffswellen womöglich folgen. Mindestens 150 Länder waren betroffen, Glieder einer unheimlichen Kettenreaktion. Sie konnte Anfang dieser Woche erheblich verlangsamt werden, gestoppt scheint sie indes nicht. Wie bei einem Bio-Virus kursieren bereits rund 600 „WannaCry“-Mutationen.

Nie zuvor breitete sich ein Netzstörfall derart rasant in so viele Länder aus und machte sich in so vielen Lebensbereichen bemerkbar.

Schreckensszenarien eines globalen Kontrollverlusts werden plötzlich vorstellbar: Flugzeuge heben nicht mehr ab, Züge entgleisen, Geldautomaten versagen, das Licht geht aus, Nahrungsmittel verrotten im Lager, lebenswichtige Apparate im Krankenhaus schalten sich ab. Ein Stillstand des öffentlichen Lebens, umfassend, gleichzeitig und global.

Nun wird deutlich, wie verletzlich unsere vernetzte Welt geworden ist. Und wie unser Alltag von Technologien abhängt, die wir nur scheinbar beherrschen.

1 bis 5 **Mögliche Angriffsziele Krankenhaus, Bahn, Atomkraftwerk, Flughafen, Rechenzentrum**

6 **Nachricht der Erpressersoftware „WannaCry“**

1 TIM WEGNER / LAIF

2 PAUL LANGROCK / ZENIT / LAIF

6 POLARIS / STUDIO X

3 MARIO FOURMY / LAIF

5 THOMAS TRUTSCHEL / PHOTOTHEK / GETTY IMAGES

4 EUROLUFTBILD / AKG

Die Angreifer der vergangenen Woche treffen Gesellschaften, die sich in einem enormen Tempo digital verbinden, in allen Lebensbereichen, vom „Smart Phone“ und „Smart Home“ über „Smart Cash“ bis zu „Smart City“ und „Smart Government“.

Diese Entwicklung ist politisch gewollt und gefördert, die Bundeskanzlerin beschwört die Segnungen der Industrie 4.0, das Verkehrsministerium investiert Milliarden in den Breitbandausbau, im Wirtschaftsministerium will Brigitte Zypries das „IoT“ beschleunigen, das Internet of Things, wie sie erst vorige Woche auf der Berliner Netzkonferenz re:publica erklärte: „Die Amerikaner haben das Internet, wir haben die Dinge.“

Und alle haben die Gefahr. Europäer, Amerikaner, Inder, Chinesen müssen nun, jeder für sich und gemeinsam, prüfen, wie die Lebensadern der digitalen Welt geschützt, Attacken abgewehrt und Angreifer gefasst und ausgeschaltet werden können.

„WannaCry“ ist ein Warnschuss, eine Aufforderung, über die möglichen Folgen der rastlosen Vernetzung nachzudenken. Wie viele solcher Weckrufe wird es noch geben, bevor der digitale Ernstfall eintritt? Und was können Regierungen, Unternehmen und wir Nutzer tun, um ihn zu verhindern – oder zumindest vorbereitet zu sein?

Drei Schritte stehen nun an. Zunächst braucht es ein realistisches Lagebild zu den globalen Schäden, die „WannaCry“ angerichtet hat. Gleichzeitig läuft, zweitens, die Suche nach den Schuldigen und deren Motiven. Und drittens geht es darum, die richtigen Lehren aus der Angriffswelle zu ziehen. Denn die Attacken konnte es nur geben, weil Geheimdienste ein eigenes gefährliches Spiel mit Sicherheitslücken treiben. Weil Softwareproduzenten wie Microsoft ihre Verantwortung für die Netzsicherheit nicht hinreichend wahrnehmen. Und weil viele Nutzer vorhandene Sicherheits-Updates ignorieren.

Krankenhäuser sagten Operationen ab, Autofirmen stoppten die Produktion.

Der Flächenbrand

Es war wie eine Rückkehr ins vorige Jahrhundert. Am Hauptbahnhof in Frankfurt am Main, der Stadt der Banken und Finanzdienstleister, holten Bahn-Mitarbeiter Schiefertafeln und Kreide heraus. In geschwungener Schrift schrieben sie die Abfahrtszeiten der Züge auf und stellten sie neben die Gleise: „Abf.: 11.13 nach Berlin“, „Abf.: 15.54 München“. Mehr als 20 Jahre lang hatten die Tafeln in der Ecke gelegen, nun wurden sie wieder nützlich. Eine Schiefertafel kann kein Hacker manipulieren.

Rund 450 Rechner der Deutschen Bahn (DB) waren infiziert. Die sichtbarsten Folgen: lahmgelegte Anzeigetafeln an vielen Bahnhöfen, zum Teil war noch die Botschaft der Erpresser samt Lösegeldforderung eingeblendet.

Erwischt hat es auch Videoüberwachungssysteme der DB, die Bildschirme zeigten ebenfalls Nachrichten von „WannaCry“. In Hannover traf es eine regionale Leitstelle der Bahn, die für die Disposition von Personal und Material zuständig ist. In Berlin kämpfte die S-Bahn noch eine Woche später mit Problemen bei ihren Fahrkartenautomaten.

Betroffen von der „WannaCry“-Attacke war auch ein Unternehmen aus der Ernährungsbranche, das zur kritischen Infrastruktur in Deutschland gerechnet wird. Und selbst auf medizinischen Geräten der Firma Bayer, die in US-Krankenhäusern im Einsatz sind, ploppte plötzlich die Lösegeldforderung auf. In Deutschland oder Europa seien dem Unternehmen keine Fälle gemeldet worden, hieß es bei Bayer.

Deutsche Kunden des Telefonanbieters O2 hatten ebenfalls Probleme. Der spanische Mutterkonzern Telefónica musste wegen des Cyberangriffs bestimmte IT-Systeme herunterfahren, daraufhin konnte der DSL-Kundendienst von O2 in Deutschland nicht mehr auf seine Datenbank zugreifen. Die interne Kommunikation bei O2 war durch die Attacke zwischenzeitlich gestört, E-Mail-Programme fielen aus.

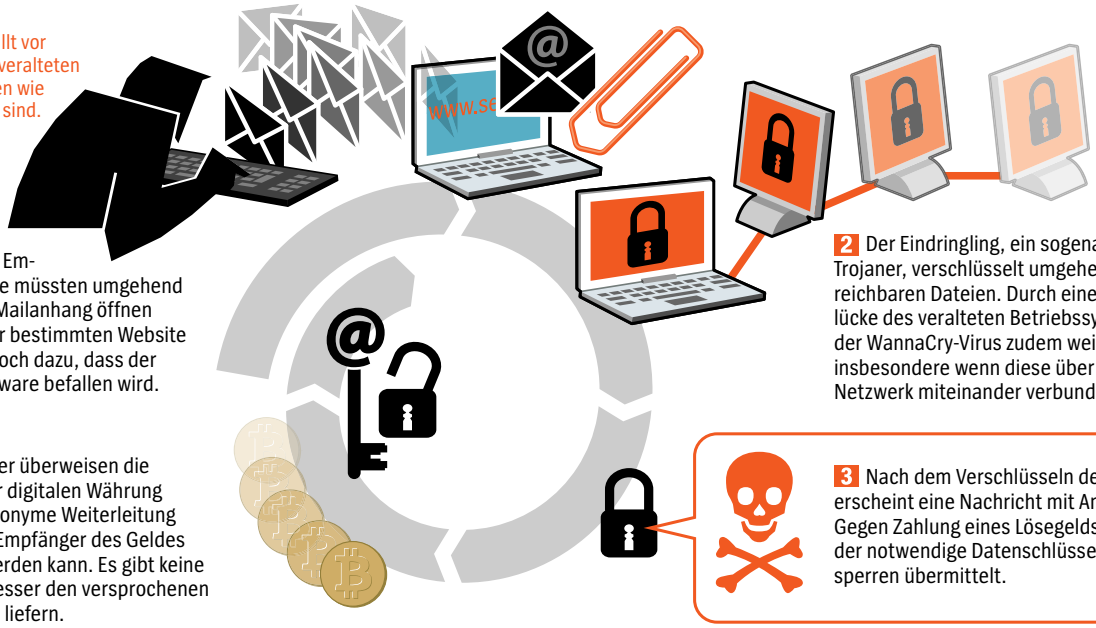
Und in Düsseldorf, Essen, Hagen und Grevenbroich durften sich Autofahrer über kostenloses Parken freuen: Eine Parkhauskette konnte wegen „WannaCry“ ihre Schranken nicht mehr schließen.

Mehr als 300 000 Rechner wurden weltweit befallen. Deutschland landete auf Platz 13 der globalen Betroffenheitscharts – und ist damit noch vergleichsweise glimpflich davongekommen.

Anderswo waren die Folgen drastischer: Britische Krankenhäuser sagten Operationen ab und schickten Krebspatienten nach Hause. In Frankreich stoppte Renault teil-

Daten in Geiselhaft Cyberattacke mit einem Verschlüsselungsvirus

Der WannaCry-Virus befällt vor allem Computer, die mit veralteten Betriebssystem-Versionen wie Windows XP ausgerüstet sind.



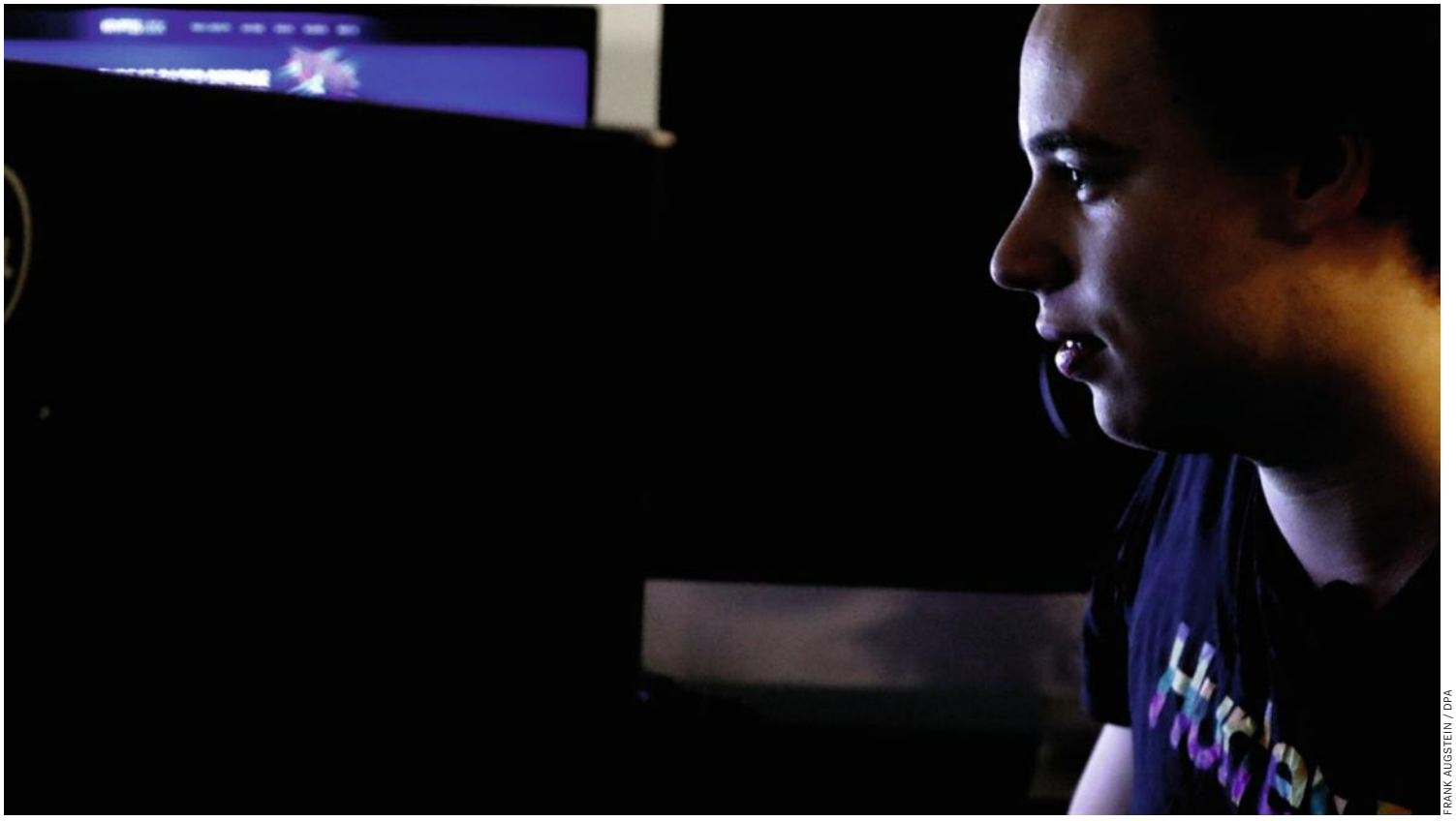
1 Kriminelle Hacker verschicken massenhaft E-Mails, die seriös und amtlich wirken und Empfängern vorgaukeln, sie müssten umgehend den darin enthaltenen Mailanhang öffnen oder einem Link zu einer bestimmten Website folgen. Beides führt jedoch dazu, dass der Rechner von Schadsoftware befallen wird.

2 Der Eindringling, ein sogenannter Krypto-Trojaner, verschlüsselt umgehend alle erreichbaren Dateien. Durch eine Sicherheitslücke des veralteten Betriebssystems infiziert der WannaCry-Virus zudem weitere Rechner, insbesondere wenn diese über ein internes Netzwerk miteinander verbunden sind.

3 Nach dem Verschlüsseln der Dateien erscheint eine Nachricht mit Anweisungen: Gegen Zahlung eines Lösegelds werde der notwendige Datenschlüssel zum Entsperren übermittelt.

4 Zahlungswillige Opfer überweisen die verlangte Summe in der digitalen Währung Bitcoin. Dies und die anonyme Weiterleitung sorgen dafür, dass der Empfänger des Geldes meist nicht ermittelt werden kann. Es gibt keine Garantie, dass die Erpresser den versprochenen Datenschlüssel wirklich liefern.

DER SPIEGEL



FRANK AUGSTEIN / DPA

IT-Experte Hutchins: Mit einem Trick gelang es ihm, die Verbreitung der Schadsoftware zu verlangsamen

weise seine Autoproduktion, in China konnten Kunden an mehr als 20 000 Tankstellen nur noch bar bezahlen. Hightechunternehmen wie der japanische Hitachi-Konzern, der US-Logistiker FedEx sowie das russische Innenministerium: Sie alle wurden Opfer jener Erpressung, deren Lösegeldforderung mit dem hämischen Wort „Ooops“ begann.

In der Bundesrepublik meldete sich am Freitag vergangener Woche um 20.30 Uhr ein Vertreter der Deutschen Bahn beim Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn. Es gebe da ein Problem.

Deutschlands Cyberabwehr war alarmiert, ähnliche Hinweise hatte das BSI von anderen Seiten bekommen. Hektisch schalteten sich die Beamten mit ihren Kollegen in Großbritannien und Frankreich zusammen. Das Bundesinnenministerium startete eine Telefonkonferenz mit allen zuständigen Behörden.

Um 21.28 Uhr schaltete sich Bundesinnenminister Thomas de Maizière (CDU) persönlich ein und rief BSI-Chef Arne Schönbohm an. Schnell wurde klar: Der Schädling verbreitete sich mit ungeheurer Geschwindigkeit.

Es sollte eine lange Nacht werden für alle Beteiligten. Um 1.30 Uhr am Samstagmorgen folgte eine weitere Telefonschalte. Um 4.20 Uhr hatten die Experten sich einen ersten Überblick über den Angriff verschafft: Allein in der Zeit seit 17.45 Uhr am Freitagabend hatte die Schadsoftware in Russland 25 875 Opfer infiziert, 22 991 in China und 7626 in Taiwan. In Deutschland gab es 604 Treffer.

Für Beruhigung sorgte das allerdings nicht. Von einem „besonders schwerwiegenden Angriff“ sollte de Maizière später sprechen. Am Samstagmorgen begann das Bundeskriminalamt zu ermitteln. Die Staatsanwaltschaft Berlin übernahm das Verfahren, dort hat die Bahn ihren Firmensitz.

Die Spurensuche

Wer die Angreifer sind, darüber gab es bis Ende der Woche eine Menge Theorien, aber wenig Gewissheit, wie so häufig im Operationsgebiet Internet, wo sich Spuren leicht verwischen und falsche Fährten legen lassen.

Der Ort der Erstinfektion konnte bislang nicht zuverlässig ermittelt werden, das würde den zahlreichen Cyberfahndern helfen, die nun nach den „WannaCry“-Machern jagen. Die Allianz der Ermittler ist so ungewöhnlich wie der Angriff selbst: Es sind die Behörden aus den betroffenen Ländern und damit staatliche Fahnder, aber auch hoch spezialisierte Teams von IT-Sicherheitsfirmen und private Computer-Nerds, die die Übeltäter jagen.

Marcus Hutchins, ein 22-jähriger Brite, schaffte es damit schon zu weltweitem Ruhm: Mit einem im „WannaCry“-Code verborgenen Trick, einer Art Notausschalter („Kill Switch“), gelang es ihm, die Verbreitung erheblich zu verlangsamen.

Wenn man in der Kette der Verantwortlichen an den Anfang geht, landet man allerdings bei einem bekannt-berüchtigten Akteur: dem amerikanischen Geheimdienst NSA.

In den Elitehackerabteilungen der National Security Agency suchen und forschen Mitarbeiter nach Sicherheitslücken für jedes erdenkliche Betriebssystem.

Diese sind Einfallstore in Geräte aller Art und in Computernetzwerke. Man kann sie mit digitalen Dietrichen vergleichen, aber auch hoch wirksame Cyberwaffen sind ohne sie nicht denkbar. Die wertvollsten von ihnen heißen „Zero-Day-Exploits“. Sie können schon ausgenutzt werden, bevor die Hersteller von ihnen wissen und eine Chance haben, sie zu schließen.

Eines dieser Instrumente aus dem NSA-Arsenal betrifft das weltweit am meisten verbreitete Betriebssystem Windows – es trug dort den Codenamen „Eternal Blue“.

Aber wie gelangte dieses Geheimwissen an die Öffentlichkeit? Die Gruppe, die sie veröffentlichte, nennt sich Shadow Brokers (Schattenhändler). Das mysteriöse Team war im vorigen Sommer wie aus dem Nichts im Netz aufgetaucht. In seltsamem Englisch boten die Shadow Brokers dort NSA-Angriffswaffen zum Kauf an. Offenbar klappte das nicht wie gewünscht, jedenfalls verfiel die Truppe bald darauf, Schadprogramme der Amerikaner tröpfchenweise zu veröffentlichen.

Am 14. April posteten die Shadow Brokers ihren neuesten NSA-Leak – darunter war auch die Sicherheitslücke „Eternal Blue“. Seither konnte jede begabte Hackergruppe sie für ihre eigene Zwecke missbrauchen.

Wie die Shadow Brokers an das streng geheime NSA-Material kamen, ist noch unklar – es gibt aber eine auffällige zeitliche Koinzidenz.

Digitaler Selbstschutz

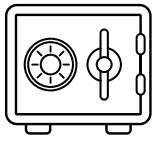
Computerviren Schadsoftware kann jeden treffen. Mit diesen Methoden schützen Sie Ihre Daten.

Die schlechte Nachricht zuerst: Wer sich ins Netz begibt, lebt gefährlich. Datenklau, Erpressungsversuche und Viren sind ein reales Risiko. Hersteller und Politik versprechen den Nutzern zwar Schutz, tun aber zu wenig dafür.

Ratsam ist deshalb die digitale Selbstverteidigung: Jeder Nutzer sollte Vorsorge dafür tragen, dass wichtige E-Mails, Hochzeitsvideos und Kinderfotos gegen eine Digital-Havarie gesichert sind.

Jeder sollte daher einen Notfallplan haben. Eine Art Rettungsboot auf stürmischer See, in dem die wichtigsten Schätze gesichert werden.

Die gute Nachricht: Drei einfache Maßnahmen reichen dafür aus – Sicherheitskopien, regelmäßige Systemaktualisierungen und Antivirensoftware.



Back-up

Haben Sie Sicherheitskopien Ihrer Daten auf einem **externen Datenträger oder Speicherdienst** abgelegt?

Sicherheitskopien bieten den einfachsten und zuverlässigsten Schutz. Wichtige Daten sollten immer auf mindestens einem zweiten, externen Speichermedium abgelegt werden. Eine Back-up-Software wie „Time Machine“ oder „Duplicati“ erledigt das fast unmerklich im Hintergrund, meist einmal pro Stunde.

Wer nur wenig am Rechner arbeitet und nur auf ein paar Textdokumente und Bewerbungen angewiesen ist, kann sie einfach regelmäßig auf einen kleinen USB-Speicherstick ziehen.

Wer dagegen Videos oder Fotos hortet, braucht dafür eher voluminöse Festplatten, gern in der Größe von ein paar Terabyte. Auf den ersten Blick mögen die über hundert Euro Anschaffungskosten teuer wirken, umgerechnet auf ein paar Jahre entspricht das eher einem Cappuccino pro Monat.

Eine kleine Warnung: Die permanente Verbindung der Sicherungskopie mit dem Rechner bringt eigene Risiken mit sich. Wenn ein Virus den Computer befällt, könnte der sich auch auf der Sicherungskopie einnisten.

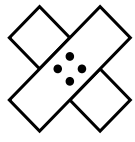
Praktisch sind daher zum Beispiel Festplatten-Dockingstationen, mit denen man relativ einfach eine Kopie der Kopie ziehen kann: also ein Back-up des Back-ups. Wer Terabyte an Daten überträgt, braucht dafür oft eine ganze Nacht, und eine Dockingstation erledigt das ganz allein, ohne dass der Rechner dafür angestöpselt sein muss.

Die Sicherungskopie der Sicherungskopie hinterlegt man dann im Schlafzimmer oder bei einem Freund, falls das Büro von Einbrechern oder einem Brand verwüstet wird. Ist das nicht paranoid? Mag sein – solange es um ein paar private E-Mails geht. Aber wenn ein Jahr Arbeit oder die Existenz einer Firma daran hängen sollte, sind 200 Euro für ein zweites Back-up fast ein Schnäppchen.

Auch Cloud-Speicher wie etwa iCloud oder Google Drive sind als Ergänzung sinnvoll, denn sie ermöglichen das Wiederfinden der Daten auch dann, wenn man unterwegs auf Geschäftsreisen den Rechner wiederherstellen oder vom Internetcafé aus auf ein paar Dokumente zugreifen will.

Doch alles hat seinen Preis: Bei der Cloud-Speicherung ist das Risiko größer, dass Unbefugte sich an den Daten vergreifen. Daher sind in der Wolke ganz besonders sichere Passwörter oder gleich ein Passwortmanager ratsam – aber zu diesem kniffligen Thema sollte man lieber in die Fachpresse schauen.

Egal für welche Methode man sich entscheidet: Man soll das Back-up nicht vor der Wiederherstellung loben. Es lohnt sich, hin und wieder zu checken, ob die Datensicherung auch wirklich so geklappt hat, wie man sich das erhofft hatte.

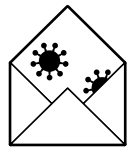


Systempflege

Ist Ihr Betriebssystem noch aktuell, sodass es vom Hersteller mit sogenannten **Patches** versorgt wird?

Die Softwareaktualisierung des Betriebssystems sollte heilige Pflicht sein. Auch sie erfolgt am besten automatisch im Hintergrund. Für aktuelle Betriebssysteme sind diese „Patches“ im Preis inbegriffen. Irgendwann läuft die Unterstützung allerdings meist aus, so auch bei Microsoft. „Never change a running system“ – dieser Spruch gilt hier leider nicht, im Gegenteil: Wer an seinem alten Betriebssystem hängt, erhöht damit die Gefahr, Opfer von Cyberangriffen zu werden. Alte Windows-Varianten wie XP sind aktuell besonders stark betroffen vom „WannaCry“-Schadprogramm.

Wer dennoch unbedingt sein altes System behalten will, vielleicht wegen eines musealen Nadeldruckers, sollte mit der Uralt-Software lieber nicht ins Internet gehen.



Virenschutz

Haben Sie einen Virenscanner installiert, der auch aktiv ist und sich **automatisch aktualisiert?**

Antiviren- und Firewallprogramme stärken sozusagen die Immunabwehr des Rechners, weil sie verdächtige Datenpakete durchleuchten und besonders schnell aktualisiert werden, wenn Würmer und Trojaner mit neuartigen „Mutationen“ auftauchen. Ein kleiner Nachteil: Manchmal zickt nach der Installation solcher Programme die eine oder andere Funktion, weil sie fälschlicherweise als feindlich erkannt wird. Aber das ruckelt sich meist schnell zurecht. Die Auswahl an Anbietern wie Bitdefender, F-Secure, Kaspersky, Symantec, Trend Micro ist groß, die monatlichen Abokosten sind meist gering.

Back-up, Systempflege, Virenschutz: Wer diese drei Regeln der Digitalhygiene beachtet, kann die lokalen Daten nicht nur vor Lösegelderpressern schützen. Sondern auch vor Verlust durch Einbruch, Feuer, Verbummeln oder einfach das Abschmieren der Festplatte.

Natürlich sollte der Selbstschutz nicht suggerieren, dass jeder für sich allein eine Insel der digital Seligen schaffen kann. Wer seine eigenen Daten in digitaler Notwehr sichert, entlässt damit nicht die Politik, die Softwarehersteller und die Geheimdienste aus ihrer Mitverantwortung an Datendebakeln wie „WannaCry“.

Und was, wenn doch einmal alle USB-Kabel reißen und Daten unrettbar verloren gehen? Vielleicht lohnt es sich für diesen Fall, wichtige Dokumente wie die Doktorarbeit oder ein Hochzeitsfoto in vorauseilendem Pessimismus auf Papier auszudrucken. Sie erinnern sich, wie man es früher einmal machte? Eine solche analoge Sicherheitskopie könnte mehr als nur eine lästige Pflicht sein: ein echter Hingucker.

Hilmar Schmundt

AARON P. BERNSTEIN / REUTERS

NSA-Chef Michael Rogers (M.): Die Sicherheitslücke stammt aus dem Arsenal des amerikanischen Geheimdienstes

Denn ausgerechnet im vergangenen August, als die Schattenhändler erstmals von sich reden machten, wurde im Bundesstaat Maryland ein Mann festgenommen, von zwei Dutzend schwer bewaffneten FBI-Beamten.

Der damals 51-jährige Harold T. Martin III hatte zu diesem Zeitpunkt eine lange Karriere für US-Dienste und deren Vertragsfirmen hinter sich, unter anderem arbeitete er mit einer hohen Sicherheitseinstufung für Booz Allen Hamilton – genauso wie vor ihm der NSA-Whistleblower Edward Snowden.

Im Februar erhob die Staatsanwaltschaft gegen Martin Anklage in 20 Punkten. Demnach habe er insgesamt über 20 Jahre die unfassbare Menge von rund 50 Terabyte mit geheimen Daten beiseitegeschafft. Sollte Martin in allen Punkten verurteilt werden, drohen ihm bis zu 200 Jahre Haft.

Es liegt nahe, dass es einen Zusammenhang zwischen Martin und den Shadow Brokers gibt; zumal das dort bisher veröffentlichte Material offenbar zu den von Martin kopierten Beständen passt. Er selbst kann allerdings kaum hinter den Veröffentlichungen stehen, denn die gingen weiter, als er längst in Haft saß. Einige Experten, darunter Edward Snowden, vermuteten hinter den Shadow Brokers in der Vergangenheit russische Interessen.

Nachvollziehbar ist damit bislang nur, wie ein virtuelles Geheimdienstinstrument der NSA womöglich auf den Markt kam. Denn die Shadow Brokers lieferten mit der Sicherheitslücke bloß die Vorlage.

Deutsche und internationale Behörden untersuchen nun, wer „Eternal Blue“ zur Cyberwaffe „WannaCry“ ausbaute – die Angriffssoftware besteht aus mehreren Modulen, welche die Fehler im Windows-Betriebssystem auf perfide und höchst effektive Weise ausnutzen.

Unter Verdacht stehen bislang vor allem Hacker, die in Diensten von Nordkoreas Diktator Kim Jong Un stehen sollen: die sogenannte Lazarus-Gruppe.

Dass sie zu spektakulären Cyberangriffen in der Lage sind, haben die Mitglieder dieser Gruppe bereits unter Beweis gestellt: Vor knapp drei Jahren versuchten sie zunächst, die Hollywoodstudios von Sony zu erpressen, nachdem diese eine Satire über den nordkoreanischen Machthaber („The Interview“) produziert hatten. Als der Konzern nicht zahlte, überfluteten die Hacker das Netz mit Tausenden teils für die Mitarbeiter peinlichen E-Mails und mit noch nicht veröffentlichten Filmen.

Auch hinter dem Onlinebankraub bei der Zentralbank von Bangladesch im vorigen Jahr sollen Hacker in Diensten von Kim Jong Un stecken; sie erbeuteten 81 Millionen Dollar.

„Man kann immer jemand anderen beschuldigen, die eigene Verantwortung leugnen.“

Mehr als Indizien aus dem Schadcode waren es bislang nicht, die zu Lazarus führen. Eine belastbare Beweisführung ist das nicht. Die schwierige Tätersuche macht die Sache für Kim Jong Un und andere Machthaber besonders interessant. „Man kann immer jemand anderen beschuldigen, man kann die eigene Verantwortung immer leugnen“, sagt der russische Geheimdienstexperte Andrej Soldatow (siehe Interview Seite 18).

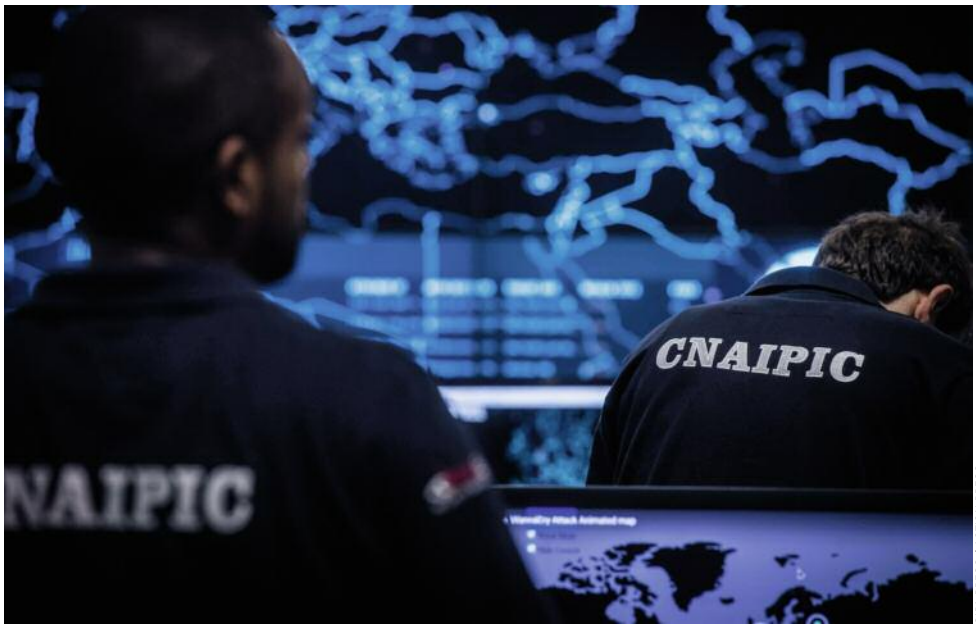
Sollten sich aber die Hinweise weiter erhärten, könnte das für Nordkorea gravierende Folgen haben. Nach dem Sony-Hack ging das gesamte Land zeitweise offline. Das war wohl kein Zufall – sondern womöglich ein deutlicher Fingerzeig westlicher Dienste.

Am Dienstag berichteten die deutschen Geheimdienste im Bundeskanzleramt von ihren Erkenntnissen. Es sei wahrscheinlich, dass ein staatlicher Akteur hinter der Attacke stecke, heißt es seither auch in deutschen Sicherheitskreisen.

Wieso sonst hätten die Angreifer einen „Kill Switch“ einbauen sollen, mit dem die Attacke beendet werden konnte? Warum so ein Aufwand für bislang rund einhunderttausend Dollar an eingetriebenen Lösegeldern?

Vielleicht war es sogar nur ein Testlauf für einen später noch geplanten, weiteren Angriff, womöglich geriet er aus dem Ruder, mutmaßten Geheimdienstler – sie müssen immer vom Schlimmsten ausgehen.

In Bonn trafen sich zur selben Zeit die wichtigsten Köpfe der Branche zu einem lange geplanten Kongress über Cybersicherheit. Gastgeber war das Bundesamt für Sicherheit in der Informationstechnik.



SIPA PRESS / ACTION PRESS

Cyberpolizisten in Rom: „Die Bedrohung ist real“

„Wir sind mit einem blauen Auge davongekommen“, sagt BSI-Chef Arne Schönbohm. Es ist Mittagspause, die Konferenzbesucher stärken sich bei Leberkäse und Kartoffeln oder haben sich in den Schatten der Bäume im Stadtpark Bad Godesberg geflüchtet.

„Ein Teil eines solchen Codes kann verräterisch sein. Oder eine mit Absicht falsch gelegte Spur“, sagt Schönbohm. Dann erzählt er eine Geschichte über die Securitate in Rumänien zu Zeiten des Diktators Nicolae Ceauşescu. Der Geheimdienst sei neben seinen eigentlichen Aufgaben damit betraut gewesen, durch Drogen- und Waffenhandel für das Regime Devisen einzutreiben. Mithilfe des organisierten Verbrechens.

Schönbohm sitzt in einem Raum in der Bad Godesberger Stadthalle, seine Behörde steht nun im Zentrum der Ereignisse. „Es hat funktioniert“, sagt er über die Krisenbewältigung am Wochenende. Aber es bleibt ein mulmiges Gefühl. „Am Ende kann ein Geheimdienst der Auftraggeber gewesen sein“, sagt Schönbohm, „oder auch nicht.“

Wie unübersichtlich die Dinge im Cyberspace geworden sind, weiß auch Rob Wainwright, der Chef der europäischen Polizeibehörde Europol. „Wenn Cyberkriminelle sich vornehmen, eine bestimmte Bank anzugreifen, kontaktieren sie über das Netz einen Hacker, der eine maßgeschneiderte Lösung für ihr Vorhaben anbietet. Die Infrastruktur, die sie brauchen, um über das Internet ihren Angriff auszuführen, mieten sie dafür einfach an“, sagte Wainwright bereits im März dem SPIEGEL.

„Ich rechne mit weiteren Angriffen”, sagt Bundesinnenminister de Maizière.

In dieser Welt kann natürlich auch ein Geheimdienst Hacker mieten – ohne dass er sich als Auftraggeber zu erkennen geben muss.

Die Aufarbeitung

Die Angriffswelle lief noch, da gab es schon Schuldzuweisungen. Microsoft beispielsweise warf den US-Geheimdiensten noch am Wochenende vor, das Netz mit dem Horten von Schwachstellen unsicher zu machen – und nicht mal in der Lage zu sein, die eigenen Erkenntnisse zu schützen. Microsoft-Manager Brad Smith schrieb, der Vorgang sei so gravierend, als wären dem US-Militär „Tomahawk“-Marschflugkörper abhandengekommen.

Tatsächlich ist die Haltung von Regierungen paradox. Einerseits geben sie Jahr für Jahr immer mehr Steuermilliarden aus, um das Netz angeblich sicherer zu machen und Sicherheitslücken zu schließen.

Auf der anderen Seite kaufen staatliche Behörden diskret Sicherheitslücken auf, um damit im Verborgenen zu operieren. Auch in Deutschland. Nach dem Vorbild der NSA nutzt der Bundesnachrichtendienst (BND) ebenfalls Schadprogramme zur Spionage und zur Terrorabwehr.

Mit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) entsteht gerade eine neue 400-Mann-Behörde, die unter anderem eigene Einbruchswerkzeuge entwickeln soll.

Doch der Kontrollverlust der Geheimdienste scheint nicht aufzuhalten zu sein. Neben den Cyberwaffen der NSA werden momentan auch die der CIA nach und nach veröffentlicht – in diesem Fall nicht durch die Shadow Brokers, sondern über WikiLeaks.

Schon seit Jahren fordern Experten deshalb, diesen gefährlichen Spielplatz von Geheimdiensten und Cyberkriminellen endlich zu schließen.

„Die US-Regierung hatte nach den Snowden-Enthüllungen versprochen, dass die Geheimdienste ihre Kenntnisse über Sicherheitslücken nicht mehr verschweigen“, sagt WikiLeaks-Gründer Julian Assange, „sondern sie den betroffenen Firmen mitteilen.“ Das sei offenbar eine Lüge gewesen (siehe Interview Seite 88).

Tatsächlich gibt es in den Vereinigten Staaten bereits ein Verfahren, in dem die NSA und andere Sicherheitsbehörden Nutzen und Gefahren von geheimen Cyberwaffen abwägen sollen. Doch die nun aufgetauchten Schwachstellen hatte die NSA für eigene Zwecke offenbar als zu wertvoll erachtet, um sie früher preiszugeben. Sie warnte Microsoft erst, als sie davon ausgehen musste, dass diese publik werden könnten.

In Deutschland forderten in dieser Woche die Grünen, den staatlichen Stellen das Ausnutzen dieser „Zero-Day-Exploits“ zu verbieten.

Neben den Geheimdiensten tragen aber auch die großen Softwarehersteller Verantwortung. Beim Marktführer Microsoft läuft die 2001 eingeführte XP-Version seines Betriebssystems vielerorts offenbar immer noch prima. Der Konzern hat den Update-Service allerdings vor drei Jahren eingestellt.

Der Jurist Michael Rustad von der Suffolk University in Boston sieht darin ein grundsätzliches Problem. US-Gerichte hätten es in der Vergangenheit zugelassen, „dass Konzerne die Risiken für ihre eigenen Sicherheitsschlampereien und Fehler auf die Kunden abwälzen – in Form von Nutzungsverträgen, die niemand liest und die meist auch unlesbar sind“. Das müsse sich dringend ändern. „WannaCry“ zeige, dass Softwarefehler schwere wirtschaftliche Schäden verursachen und sogar eine Gefahr für Leib und Leben darstellen könnten: „Dafür müssen die Hersteller in Haftung genommen werden können.“

Vorwürfe treffen überdies die infizierten Behörden und Unternehmen. Dass dort massenweise veraltete Software ohne Updates im Einsatz war, ist grob fahrlässig.

Massive Probleme zeigten sich schließlich bei jenen, die Raubkopien statt Originalsoftware benutzen und deshalb nicht auf Sicherheitsupdates der Hersteller zugreifen können. Offenbar aus diesem Grund ist Asien von der „WannaCry“-Attacke besonders betroffen.

„Ich rechne mit weiteren Angriffen“, sagt Bundesinnenminister de Maizière. „Die Cyberbedrohung ist nicht virtuell, sie ist real“, sagt Fred-Mario Silberbach, Leiter des Referats Ermittlungen Cybercrime beim BKA.

Tatsächlich wird dieselbe Sicherheitslücke bereits von einer weiteren Schadsoftware genutzt, die ohne Wissen der betroffenen Nutzer deren Computer für ein

ganz anderes Geschäftsmodell nutzt: Die Rechenleistung der infizierten Geräte wird missbraucht, um Einheiten einer Kryptowährung herzustellen.

Aus der Politik kommen nun Ankündigungen, die Vorschriften zu verschärfen, das deutsche IT-Sicherheitsgesetz sei unvollständig. Im ersten Schritt wurden seit Mai 2016 nur Firmen aus wenigen Branchen wie Telekommunikation, Energie, Ernährung und Wasser gezwungen, ihre Systeme nachzurüsten und erhebliche Cyberangriffe an die Behörden zu melden.

Andere Branchen wie die Transportindustrie wurden bislang verschont, auch weil das Verkehrsministerium von Alexander Dobrindt bremste – um Unternehmen vor hohen Kosten zu bewahren. In dieser Woche stellte sich der CSU-Politiker flugs an die Spitze der Sicherheitsfans und forderte eine umgehende Ausweitung des IT-Sicherheitsgesetzes, schließlich gehe es um „eine existenzielle Frage“.

Für Privatnutzer sind, so oder so, individuelle Schutzmaßnahmen wichtig (siehe Kasten Seite 14). Wer bereits erpresst werde, sagt Georg Ungefuk, solle „auf keinen Fall bezahlen“. Ungefuk ist Oberstaatsanwalt an der Zentralstelle zur Bekämpfung der Internetkriminalität in Hessen, er hatte schon mit verschiedenen Angriffswellen zu tun. „Im Normalfall ist das Geld weg, und die Daten werden nicht wiederhergestellt“, sagt er. Für die Täter berge die Schlüsselübergabe wegen der zusätzlichen Kommunikation die Gefahr, enttarnt zu werden. „Warum sollten sie dieses Risiko noch eingehen, wenn sie das Lösegeld erhalten haben?“

Die Shadow Brokers scheinen das Chaos, das sie produziert haben, derweil in vollen Zügen zu genießen. Anfang der Woche meldeten sie sich im Netz mit einer neuen Botschaft zu Wort oder genauer: mit einer Drohung. Darin kündigen sie an, ihre Veröffentlichungen künftig nur noch gegen ein Monatsabo für Mitglieder bereitzustellen, eine Art Spotify für streng Geheimes also.

Im nächsten Monatspaket könnten sich demnach Sicherheitslücken für das aktuelle Microsoft-Betriebssystem Windows 10 befinden, außerdem Daten von Zentralbanken und aus dem Bankennetzwerk Swift sowie Informationen über russische, chinesische, iranische oder nordkoreanische Nuklear- und Raketenprogramme.

Ein Bluff? Vielleicht. Nur haben die Shadow Brokers ihren Ankündigungen bislang immer Taten folgen lassen.

Maik Baumgärtner, Frank Hornig, Fabian Reinbold, Marcel Rosenbach, Fidelius Schmid, Hilmar Schmundt, Wolf Wiedmann-Schmidt

Video: So schützen Sie sich vor Hackerangriffen

spiegel.de/sp212017hacker
oder in der App DER SPIEGEL