Veraltete Systeme bergen grosse Gefahren

Firmen sollten Daten auf separaten Laufwerken ablegen

MICHAEL SCHILLIGER, CHRISTIAN STEINER

Das grösste Sicherheitsrisiko für Unternehmen ist der Mensch. Doch auch veraltete Computersysteme sind eine grosse Gefahr. Wie der Cyberangriff «Wanna Cry» vom Freitag zeigt, ist oft nicht einmal ein Mausklick nötig, um von der Schadsoftware befallen zu werden. Über 200 000 Systeme und Computer wurden angegriffen. Ausserdem zeigen Daten, dass über 1,3 Mio. Computer noch nicht gegen Angriffe dieser Art geschützt sind.

Was ist genau passiert?
Einer der bisher grössten Cyberangriffe weltweit hat am Wochenende über 200 000 Computer von Unternehmen und Institutionen lahmgelegt. In der Schweiz gab es im Zusammenhang mit dem Cyberangriff keine grösseren Ausfälle. Allerdings waren auch hierzulande private Computer betroffen. Sogenannte Ransomware hat in 150 Ländern ganze Rechner blockiert oder Dateien verschlüsselt und die Nutzer zur Zahlung eines Lösegeldes aufgefordert.

Was ist Ransomware?
Ransomware ist eine Schadsoftware, die den Zugang zu einem Computer oder zu bestimmten Daten auf einem Computer blockiert und vom Nutzer Geld für die Entschlüsselung oder Freigabe verlangt. Hierzu wird Ransom auf den Computer geschleust.

Wie wirkt «Wanna Cry»?
Wird Schadsoftware auf einem Computer aktiv, verschlüsselt sie die Dateien des betroffenen Systems. Danach lässt sie auf dem Computer eine Mitteilung aufscheinen, in der sie die Benutzer zu einer Zahlung von etwa 300 Fr. in Bitcoins auffordert – andernfalls würden die Dateien zerstört.

Wie konnte der Cyberangriff gestoppt werden?
Im Code der Ransomware ist ein Abschaltmechanismus eingebaut: Sobald sich die Software installiert, versucht sie, eine Domain zu erreichen. Wenn das der Fall ist, schaltet sich die Ransomware ab. Die Hacker hatten die Adresse allerdings nicht registriert. Ein Sicherheitsexperte fand die Adresse im Code – rein zufällig, wie er erklärte –, kaufte die Domain, aktivierte sie und stoppte so die Ausbreitung von «Wanna Cry».

Wie konnte es zum Angriff kommen?
Im April veröffentlichte eine anonyme Gruppe, genannt «Shadow Brokers», Daten, die sie nach eigenen Angaben dem amerikanischen Geheimdienst NSA gestohlen hatte. Darunter befand sich eine Hackingsoftware, mit der weitere Programme auf fremde Microsoft-Systeme geladen werden konnten. Sie nutzt eine Sicherheitslücke in Windows-Systemen aus. Die Sicherheitslücke ist inzwischen für neuere Windows-Versionen geschlossen, nicht aber auf allen Rechnern der älteren Version Windows XP. Das Problem von Windows XP ist, dass seit April 2014 von Microsoft keine neuen Sicherheitsupdates mehr erstellt werden. Der Software-Anbieter hat aber reagiert und am Freitag ein «einmaliges» Update zur Verfügung gestellt. Doch dieses ist auf über 1 Mio. Computern noch nicht installiert.

Wer steckt hinter dem Angriff?
Auch wenn ursprünglich die Gruppe «Shadow Broker» mit ihrem Leak im April die Basis für den Angriff gelegt haben dürfte, ist nicht klar, wer hinter dem Angriff am Freitag steckt. Ebenso unklar ist, wer sich hinter dem Namen «Shadow Broker» verbirgt. Zu Beginn vermutete man einen Mitarbeiter der NSA oder der CIA. Doch eine Festnahme eines Vertragsmitarbeiters der NSA beendete die Leaks nicht.

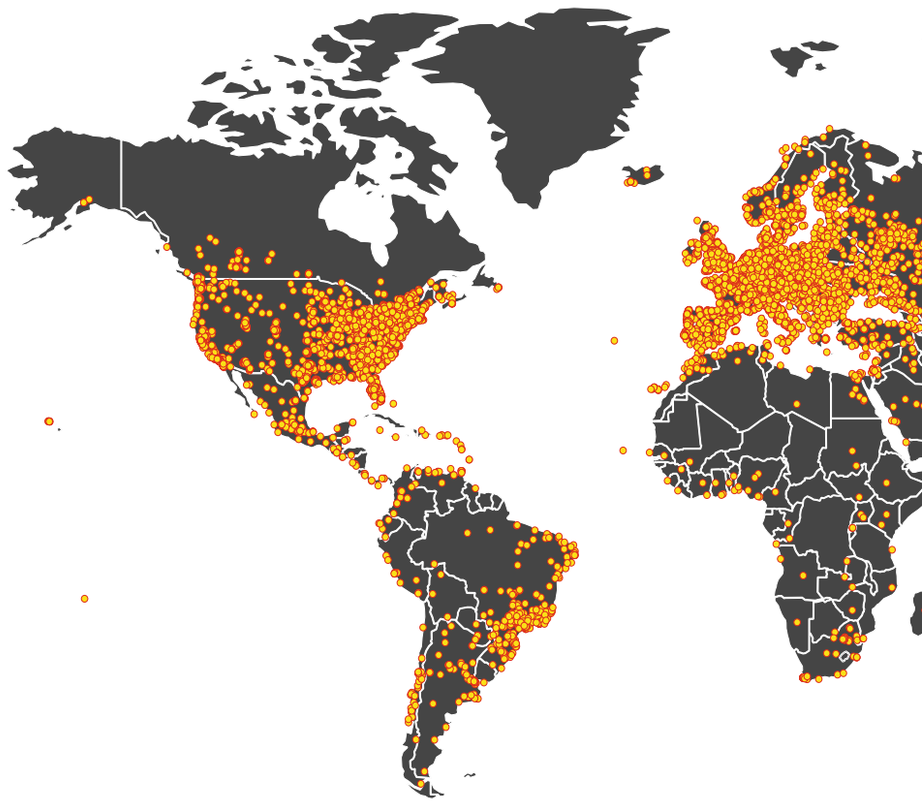
Wie können die Daten wieder beschafft werden?
Wenn ein Computer geknackt wird und die Daten verschlüsselt werden, ist es im besten Fall möglich, den Computer aus einem Back-up wiederherzustellen. Unternehmen sollten regelmässig ihre Daten sichern und diese als Offline-Back-up auf separaten Laufwerken ablegen. Zudem sollten die Gesellschaften sicherstellen, dass Updates auch tatsächlich installiert werden.

Welche Länder sind tangiert?
Gegen wen sich die Attacke richtet, ist bis jetzt völlig unklar. Laut Daten der Sicherheitsfirma Kapersky vom Freitag ist vor allem Russland (20% der Angriffe) betroffen. Der Grund dafür ist, dass in Russland noch sehr viele inoffizielle Versionen von Windows XP laufen. Daneben sind vor allem die Ukraine, Indien, Taiwan und Tadschikistan tangiert. In der Schweiz sind keine grösseren Störungen bekannt.

Warum bringen Unternehmen ihre Software nicht auf den neusten Stand?
Neue Software ist nicht nur teuer, sondern es kann auch sein, dass Eigenentwicklungen oder externe Programme nicht auf neuen Systemen laufen. Das würde bedeuten, dass man beispielsweise Datenbanken neu programmieren muss, was viel mehr kostet als ein neues Betriebssystem. Auch Computer von Aussendienstmitarbeitern können ein Sicherheitsrisiko darstellen, weil sie durchgehend mit dem System der Firma verbunden sind.

Ein globaler Angriff

Orte mit Computern, die in den vergangenen 24 Stunden infiziert worden sind (Stand: Montag, 15.30 Uhr)



QUELLE: MALWARETECH

Digitaler Bandwurm befällt

Bei der jüngsten Cyberattacke war erstmals ein Erpressungstrojaner im Umlauf, der

Im Gegensatz zum Ausland hat der Erpressungstrojaner «Wanna Cry» hierzulande wenig Schaden angerichtet. Trotzdem kommen teilweise haarsträubende Unterlassungen zum Vorschein.

GIORGIO V. MÜLLER

Ein einziger Sensibilisierungstag hat nicht gereicht: Vor fast genau einem Jahr, am 19. Mai 2016, wurde in der Schweiz der erste Awareness-Tag zum Thema Ransomware durchgeführt. Zusammen mit Partnern machte die Melde- und Analysestelle Informationssicherung (Melani) des Bundes die Öffentlichkeit auf die spezifischen Gefahren von Erpressungsversuchen via Verschlüsselungstrojaner (Ransomware) aufmerksam; sie zeigte, wie man sich dagegen schützen und was im schlimmsten Fall getan werden kann. Angesichts der laut Experten bisher nur etwa 200 in der Schweiz durch «Wanna Cry» Infizierten – weltweit ist die Rede von rund 200 000 Fällen – zeigt die Aufklärungsarbeit offenbar Wirkung. Betroffen seien nur einige wenige Privatpersonen und KMU gewesen, aber keine Grossunternehmen, lässt Max Klaus, der stellvertretende Leiter von Melani, schriftlich wissen.

Diese geringe Anzahl dürfte die tatsächliche Situation jedoch stark beschönigen, sagt Sonja Meindl, die Geschäftsführerin für die Schweiz und Österreich des IT-Sicherheits-Spezialisten Check Point Software. Im Gegensatz zu anderen Ländern müssen hier solche Attacken den Behörden nicht gemeldet werden. Deshalb geht auch Klaus davon aus, dass es nur die Spitze des Eisbergs sei, den Melani jeweils sehe. Diese Situation ändert sich in einem Jahr, weil dann die neue EU-Datenschutz-Grundverordnung in Kraft tritt, an die sich auch Schweizer Firmen halten müssen, die ausserhalb der Landesgrenze geschäften. Konkret habe Check Point Software, die laufend auf ihrer Website über die neusten Entwicklungen berichtet, am Freitag einen betroffenen Schweizer Kunden unterstützt, der jedoch anonym bleiben wollte. Ihre Sicherheitslösungen hätten «Wanna Cry» bisher erfolgreich abgewehrt, sagt Meindl. Die Erfahrung habe aber gezeigt, dass oft Attacken mit leicht abgeänderten Versionen wiederholt würden.

Trojaner, mit denen Computer mit einem Virus infiziert werden und für deren Entschlüsselung ein Lösegeld verlangt wird, sind kein neues Phänomen. Laut dem Kaspersky Lab hat sich die Menge von Ransomware allein von Frühling 2015 bis Frühling 2016 verfünffacht. Bei der zweiten Version von «Wanna Cry», die in diesen Tagen ihr Unwesen rund um den Globus treibt und eine Sicherheitslücke in alten Windows-Betriebssystemen nutzt, sind laut Meindl vor allem die Verbreitung und die Geschwindigkeit bemerkenswert. Grossfirmen wie Telefónica wiesen ihre Mitarbeiter an, sich mit ihren Geräten ja nicht einzuloggen; die Gefahr bestehe, dass infizierte Geräte das ganze Netzwerk ansteckten. Denn dem Trojaner ist noch ein Wurm angehängt, der sich von Rechner zu Rechner fortsetzen kann.

Bitcoin wird dem dubiosen Ruf gerecht

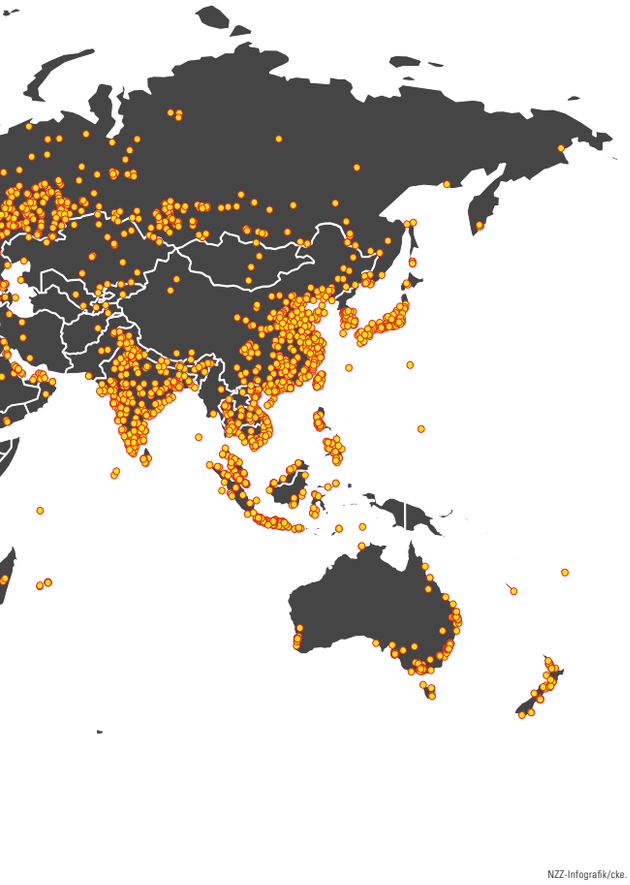
«Ablasszahlungen» von gerade einmal 55 000 Franken

cri. · Der jüngste Ärger mit der Schadsoftware «Wanna Cry» hat auch Bitcoin zurück in die Schlagzeilen gebracht. Tatsächlich wollen die Erpresser in Einheiten dieser Kryptowährung im Gegenwert von 300 $ bezahlt werden, bevor sie auf «gekaperten» Rechnern gezielt verschlüsselte Daten wieder freigeben. Sie setzen offensichtlich auf die scheinbare Anonymität des «kostengünstigen und dezentralen Netzwerks für die sichere, Übermittlung digitaler Werte», das hinter der Währung stehen soll. Schliesslich lohnt sich eine Erpressung für die Täter nur, wenn sie nicht erwischt werden. So gesehen bestätigt das Vorgehen die Kritiker, die Bitcoin regelmässig in Verbindung mit illegalen Geschäften bringen – etwa solchen im so genannten Darknet. Erstaunlich ist, dass die Erpresser bis Montagabend nur Bitcoins im Wert von etwa 55 000 Fr. erhalten haben, obwohl sie sehr viele Rechner infiziert haben. Das mag daran liegen, dass sie nicht mehr völlig anonym sind, sobald sie die erhaltenen Bitcoins bewegen. Zudem waren viele Opfer nicht an den Umgang mit Bitcoins gewöhnt und hätten praktisch nicht zahlen können, selbst wenn sie gewollt hätten. Bitcoins gelten in libertären Kreisen als virtueller Ersatz für etablierte Währungen, der unabhängig von einer Notenbank auf Basis kryptografischer Verfahren in begrenzter Menge geschaffen, dezentral verwaltet und wertstabil bleiben sollte. Davon kann aber keine Rede sein – denn was würde wohl passieren, wenn der Frankenkurs um 700% zulegte wie Bitcoin in den vergangenen zwei Jahren?

Feuerversicherung des 21. Jahrhunderts

Werner Enz · Cyber-Versicherungen finden in Europa erst allmählich Verbreitung, in Amerika dagegen sind sie schon fest verankert. Im vergangenen Jahr erreichte der US-Cyber-Markt ein Volumen von 3 Mrd. $, in Deutschland waren es erst 30 Mio. €. AIG Europe hat im Zeitraum 2013 bis 2016 eine enorme Zunahme der Schadenmeldungen registriert, wobei – wie im vorliegenden Fall – Cyber-Erpresser mit Verschlüsselungs-Ransomware mit 16% aller Fälle an der Spitze lagen. Datenschutzverletzungen durch Hacker und Schäden wegen unberechtigter Zugriffe folgen auf den nächsten Rängen. Der deutsche Broker Funk sieht Cyber-Risiken als Chefsache. Zum Risikomanagement gehöre, Systeme von Firmen mit simulierten Hackerangriffen auf das schwächstes Glied im ganzen Abwehrdispositiv zu testen.

Manche bezeichnen Cyber-Versicherungen als Feuerversicherung des 21. Jahrhunderts, weil Schäden wie Betriebsunterbruch oder Zerstörung von Infrastruktur ähnlich sind. Feuer sind (meist) zufallsbedingt, wogegen Cyber-Schäden gezielt durch Kriminelle herbeigeführt werden. Aus versicherungstechnischer Sicht bildet Letzteres eine hohe Hürde.



NZZ-Infografik/cke.

die Welt

sich von Rechner zu Rechner fortsetzt

Das habe es bisher noch nie gegeben, sagt Martin Lee, der technische Leiter des Cisco-Talos-Teams, das sich mit Sicherheitsthemen befasst. In einigen Fällen sei das Ausmass «katastrophal» gewesen, meint er.

Perfider Kombitrojaner

Der Schaden ist nicht nur finanzieller Natur. Auch in der Schweiz gibt es noch viele zum Internet offene Netzwerkdienste (Server-Message-Blocks), über die von aussen zugegriffen werden kann. Dies zu vermeiden gehöre wie die Aktualisierung der Software zur Grundhygiene jedes guten IT-Systems, sagt Matthias Bossardt, der bei KPMG den Bereich Cyber Security leitet. Dass die seit dem 14. März verfügbare Software-Aktualisierung von Microsoft – seit Samstag sogar für alte Systeme wie XP, für die es seit längerem keine Aktualisierungen mehr gibt – noch immer nicht von allen heruntergeladen wurde, ist deshalb schwierig zu verstehen.

Die angesichts der grossen und schnellen Verbreitung geringe Summe, die bisher erpresst werden konnte – die Rede ist von 55 000 Fr. – erklärt sich Meindl von Check Point Software dadurch, dass via Blogs und Meldestellen rasch bekanntwurde, dass die gesperrten Daten auch nach einer Lösegeldzahlung nicht wieder verfügbar sind. Das deutet auf eine wenig professionelle Täterschaft hin. Dieser Ansicht ist auch der in Grossbritannien domizilierte Cisco-Experte Lee. Ausgeklügelte Angreifer würden ihr Unwesen so lange wie möglich im Geheimen treiben. Lee rechnet damit, dass die medial prominent dokumentierte Attacke Nachahmer findet.

Wer konkret dahintersteckt, ist bis jetzt nicht bekannt. Offenbar erfolgten die ersten Angriffe aus Asien; Russland und Spanien waren am stärksten davon betroffen, weil dort noch viele Computer mit veralteter Betriebssoftware im Einsatz stehen. Weshalb britische Spitäler besonders stark tangiert sind, dafür hat auch Lee keine Antwort. Vor gut einem Jahr habe es aber schon einmal eine Ransomware-Attacke gegeben, die speziell amerikanische Spitäler im Visier hatte. Als Einfallstor dienten die elektronischen Patientendossiers – kein gutes Omen für die Schweiz, die sich erst aufmacht, elektronische Patientendossiers einzuführen.

Prävention wäre einfach

Vor allem in Schweizer KMU gebe es noch viele potenzielle Sicherheitslücken, die indes mit wenig Aufwand schliessbar seien, meint Meindl. Erfahrungsgemäss werde es auch nach den Attacken noch viele ungeschützte Geräte geben. Das erklärt sie sich damit, dass es in vielen Unternehmen nur wenige Wartungsfenster gebe, die für grossflächige Software-Aktualisierungen genutzt werden können. Sie kenne Firmen, die lediglich zwei Mal pro Jahr solche Gelegenheiten wahrnähmen, weil jede Änderung die Gefahr neuer Fehler mit sich bringe. In der Regel kommt es auf die Risikoabschätzung jeder einzelnen Firma an, als wie akut und gefährlich eine Attacke für das eigene Unternehmen eingestuft wird.

Das Geschäft mit Sicherheitslücken

IT-Firmen, Nachrichtendienste und Kriminelle konkurrieren um Schwachstellen

MARIE-ASTRID LANGER

Der Chef von Microsoft, Brad Smith, hat Stellung dazu bezogen, dass eine Sicherheitslücke im hauseigenen Betriebssystem Windows den bisher grössten Cyberangriff ausgelöst hat, und dabei den Nachrichtendiensten eine Mitschuld gegeben. In einem Blog-Eintrag von Sonntag kritisiert Smith das Horten von Sicherheitslücken, wie es viele Geheimdienste praktizieren. Sie müssten sich den Preis vergegenwärtigen, den die Gesellschaft für dieses Verhalten zahle. «Regierungen weltweit sollten den Vorfall als Weckruf betrachten», schreibt Smith.

Fehler im Code unvermeidbar

Die Problematik, die Smith beschreibt, ist altbekannt und zugleich topaktuell. Für ihre Spionagearbeit haben Nachrichtendienste ein ureigenes Interesse daran, Sicherheitslücken in Software zu finden – vor allem in solcher, die wie das Betriebssystem Windows weltweit verbreitet ist. Derartige Schwachstellen gibt es in jedem Programm, vor allem in komplexen Anwendungen, deren Quellcode oft aus Millionen von Zeilen besteht.

Für Nachrichtendienste sind diese Lücken interessant, weil sie ihnen idealerweise den Zugriff auf Computersysteme weltweit ermöglichen; gleichzeitig haben sie ein Interesse daran, dass die Schwachstellen nicht entdeckt und behoben werden. Problematisch wird es jedoch, wenn die Nachrichtendienste selbst gehackt werden, wie wohl im aktuellen Fall geschehen.

Die Enthüllungen von Edward Snowden 2013 zur Arbeit der amerikanischen NSA oder auch die jüngsten Veröffentlichungen von Wikileaks zur CIA zeigen, dass vor allem die amerikanischen Nachrichtendienste sehr aktiv solche Sicherheitslücken suchen und horten. Die Snowden-Enthüllungen offenbarten auch, dass Computerfirmen in den USA mit Geheimdiensten zusammengearbeitet und für sie Hintertüren («backdoors») in die Systeme eingebaut haben. Eine derartige Kooperation streiten viele Firmen vehement ab, doch allein der Verdacht schadet ihrem Ruf – vor allem, wenn es sich um IT-Sicherheitsfirmen wie RSA handelt. Der Chef der IT-Firma Cisco etwa beschwerte sich 2014 in einem Brief an Barack Obama, dass man «so nicht arbeiten könne»; andere Unternehmen haben sich dem angeschlossen. Entsprechend bemühen sich die Unternehmen nun, zumindest nach aussen eine Distanz zur Regierung zu wahren.

Die Technologiefirmen haben ihrerseits ein Interesse daran, Schwachstellen in ihren Systemen möglichst schnell zu finden und zu korrigieren. Mit sogenannten «Bug-Bounty-Programmen» bieten sie ein «Kopfgeld» für aufgespürte Sicherheitslücken. Microsoft etwa zahlt laut eigenen Angaben zwischen 15 000 $ und 10 000 $ für die Entdeckung solcher Schwachstellen; Apple hat erst im vergangenen Sommer ein «Bounty-Programm» eingeführt und zahlt nun bis zu 200 000 $.

Deutlich mehr Geld lässt sich mit solchen Lücken aber auf dem freien Markt erwirtschaften: Die Firma Exodus etwa, deren Geschäftsmodell auf dem An- und Verkauf solcher Lücken fusst, bietet bis zu 500 000 $ für Apple-Lücken. Für eine Schwachstelle im gängigen Browser Google Chrome zahlt Exodus 50 % mehr als der Entwickler selbst, nämlich 150 000 $. Auf dem Schwarzmarkt sind die Preise bisweilen noch höher.

«Digitale Genfer Konvention»

Auch die Nachrichtendienste machen bei dem Bieterwettbewerb fleissig mit. Das FBI etwa hat Anfang 2016 im Streit mit Apple um ein verschlüsseltes iPhone Hacker damit beauftragt, das Gerät zu knacken – und dafür 900 000 $ gezahlt.

Beharren die Nachrichtendienste auch künftig auf dem Horten von Sicherheitslücken, bleibt es wohl immer nur eine Frage der Zeit, bis Cyber-Kriminelle diese Lücken ihrerseits stehlen und ausnutzen – wie im aktuellen Fall geschehen.

Microsoft-Chef Smith forderte denn auch zu einer Zusammenarbeit zwischen Technologiesektor, Regierungen und Privatpersonen auf und erneuerte seinen Ruf nach einer «Digitalen Genfer Konvention» mit Verhaltensregeln für den Cyberspace.

Schweizer Nachrichtendienst zieht nach

ase. · Ab dem 1. September kann der Schweizer Nachrichtendienst ebenfalls Sicherheitslücken in Computerprogrammen ausnutzen, wie sie am Anfang von «Wanna Cry» standen. Das neue Nachrichtendienstgesetz (NDG) erlaubt ihm das Eindringen in Computersysteme und Computernetzwerke und damit den Einsatz von Schadsoftware. Die Verwendung von Staatstrojanern war einer der umstrittenen Punkte der Vorlage, wurde jedoch nach intensiven Diskussionen vom Parlament und vom Volk mit klarer Mehrheit bewilligt.

Die Forderung nach einer Korrektur des Gesetzes, wie sie der grüne Nationalrat Balthasar Glättli nun aufgestellt hat, ist chancenlos. Diese Frage stelle sich nicht, sagt SVP-Nationalrat Franz Grüter, der als einer von wenigen bürgerlichen Politikern dem NDG lange kritisch gegenüberstand. «Die Politik ist klar der Meinung, dass der Staat dieses Instrument haben muss, um den wachsenden Gefahren, beispielsweise durch Terroristen, begegnen zu können», erklärt der IT-Unternehmer. Die Gefahr bestehe, dass solche Sicherheitslücken von den falschen Leuten ausgenutzt würden. Das müsse möglichst verhindert werden. Denn letztlich überwiege der Sicherheitsgewinn.

Deutschland rüstet auf

Unternehmen schliessen sich im Kampf gegen Cyberangriffe zusammen

CHRISTOPH EISENRING, BERLIN

Die Anzeigetafeln in einigen Bahnhöfen sind noch dunkel, einzelne Billettautomaten funktionieren nicht. Aber so schlimm wie letzten November hat es Deutschland nicht getroffen. Damals hatte es einen Cyberangriff auf 900 000 Router von Kunden der Deutschen Telekom gegeben. Immerhin wurde damals der Schaden rasch behoben. Im Februar wurde sogar ein mutmasslicher Drahtzieher in London verhaftet. Der Chef des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm, sagte am Montag, Deutschland sei bei dem jüngsten Angriff mit einem blauen Auge davongekommen. Gleichzeitig bleibe aber die Bedrohung hoch.

Immer mehr Schadsoftware

Dazu genügt der Blick in den BSI-Lagebericht vom letzten November. Demnach werden täglich 380 000 neue Schadprogramme gesichtet, die oft durch E-Mail-Anhänge weiterverbreitet werden. Die Anzahl von Spam-Nachrichten mit Schadsoftware im Anhang hat sich im ersten Halbjahr 2016 gegenüber dem Vorjahr verdreizehnfacht. Das BSI mahnt in dem Bericht ausdrücklich, dass sich die Bedrohung durch Ransomware – bei welcher der Kunde auf seine Daten nur wieder Zugriff hat, wenn er Lösegeld zahlt – gegenüber Ende 2015 deutlich verschärft habe. Schönbohm ist deshalb über den jüngsten Erpressung-Trojaner «Wanna Cry» nicht überrascht. Täglich würden von Fachleuten bis zu 39 000 Infektionen deutscher Systeme registriert – immerhin gibt es hier einen Rückgang gegenüber dem Vorjahr mit 60 000 «Ansteckungen».

Deutschland rüstet denn auch in der Abwehr gegen Cyberangriffe auf – und dies im Wortsinne. Verteidigungsministerin Ursula von der Leyen investiert 100 Mio. € in ein «Zentrum für Cyber-Sicherheit der Bundeswehr». Aus derzeit 200 Angestellten sollen alsbald 600 werden. Gerechtfertigt wird dies etwa damit, dass es allein im Januar und Februar 284 000 Angriffe auf das Netz der Bundeswehr gegeben habe.

Auch das BSI will im laufenden Jahr seinen Personalbestand um 30% oder 180 Stellen aufstocken. Beim BSI angesiedelt ist ein Abwehrzentrum, das im Ernstfall zum Einsatz kommt, um Behörden oder Betreibern von Versorgungsnetzen wie Energie, Wasser und Telekommunikation zu helfen. Das BSI baut dazu eine mobile Eingreifgruppe auf. Den Parlamentariern selbst war der Schrecken vor zwei Jahren in die Glieder gefahren, als Hacker in das Computersystem des deutschen Parlaments eingedrungen waren. Es war ein Schock, dass vertrauliche Informationen einer so wichtigen Institution nicht sicher sind.

«I_Love_You»
. . . «WannaCry»

Kommentar auf Seite 11

Doch das Aufstocken von staatlichen Ressourcen ist nur eine Massnahme. Entscheidend ist, dass sich die Wirtschaft selbst vor solchen Angriffen schützt. Oft sind Firmen hier Einzelkämpfer und verbergen, wenn sie Opfer von Cyberattacken geworden sind. Die Deutsche Cyber-Sicherheitsorganisation (DCSO), eine Gesellschaft, der sich 14 DAX-Firmen und weitere grosse Unternehmen angeschlossen haben, versucht das zu ändern. Dem Fachbeirat gehören auch das Innenministerium und Forschungsinstitute an. Die DCSO sitzt in Berlin und hat 60 Mitarbeiter. Auch am Wochenende kam sie zum Einsatz, beurteilte die Situation und gab Empfehlungen an die Mitgliedfirmen ab.

Die Wirtschaft engagiert sich

DCSO-Technologiechef Andreas Rohr erklärt, dass man den Angreifern das Leben schwerer mache, wenn sich Cyber-Opfer austauschten. Die Hacker müssten dann ihre Strategie variieren, was die Attacken kostspieliger mache. Muss sich eine Firma Vorwürfe machen, wenn sie ihre Software nicht immer sofort à jour bringt? So war ein Update, um einen Befall mit dem Trojaner zu verhindern, seit zwei Monaten verfügbar. Das sei bei Konzernen etwas anders als bei einem privaten PC-Nutzer, erklärt Rohr. Firmen testeten zunächst, ob ein Update den normalen Betrieb tangiere. Ein strukturierter Test könne ein paar Wochen dauern, wenn das Update nicht absolut dringend sei.

Bei den Mitgliedfirmen von DCSO wurden nur zwei kleinere Fälle einer Infektion entdeckt und die Trojaner unschädlich gemacht. Zugleich sieht Rohr im Erpressungs-Trojaner «Wanna Cry» aber eine neue Bedrohung: Dieser hat sich nämlich automatisch von Gerät zu Gerät verbreitet. Bisher musste man etwa einen E-Mail-Anhang öffnen oder einen «bösartigen» Link anklicken, damit es zur «Ansteckung» mit Ransomware kam. Ein rasches Software-Update ist deshalb zentral, um nicht Opfer einer nächsten Angriffswelle zu werden.