Spiegel-Online, 13. Mai 2017

Es gibt zwei Arten, die derzeitige Situation nach dem globalen Ransomware-Angriff mit der Malware WannaCry zu beschreiben. Die Kurzform lautet, pardon: Die Kacke ist mächtig am Dampfen.

Die etwas längere, diplomatischere Formulierung kommt von Microsoft, sie steht in diesem bemerkenswerten Blogpost: Es sei "schmerzhaft" gewesen, von so vielen betroffenen Unternehmen und Einzelpersonen zu erfahren. Microsoft ergreife nun eine "höchst ungewöhnliche Maßnahme": Es verteilt ein Notfall-Update auch für jene Betriebssystemversionen, die es eigentlich schon lange nicht mehr unterstützt. In erster Linie ist das Windows XP.

Natürlich hätte Microsoft ebenso gut sagen können: Wir hatten euch vor der Zeitbombe gewarnt. Und zwar schon vor mehr als vier Jahren. Damals drängte das Unternehmen die vielen XP-Nutzer in aller Welt zum Umstieg auf eine neuere Windows-Version. "Windows XP basiert auf einer Sicherheitsarchitektur, die nicht mehr den heutigen Anforderungen entspricht", sagte zum Beispiel der damalige Chef der deutschen Windows-Sparte, Oliver Gürtler.

> **Malware** ist ein allgemeiner Begriff, der Software bezeichnet, die schädlich ist.
> **Ransomware** ist ein Typ von Malware, der in erster Linie Computer übernimmt und deren Nutzer daran hindert, an Daten zu gelangen, bis dieser dafür zahlt.
> Der Name ist vom englischen *ransom* abgeleitet, was **"Lösegeld"** bedeutet.

Anfang 2013 war XP weltweit immer noch auf vier von zehn Desktop-Rechnern installiert. Heute läuft das 2001 eingeführte System dieser Messung zufolge auf sieben Prozent aller stationären Computer – was immer noch viel ist.
In gewisser Weise ist Microsoft Opfer seines eigenen Erfolgs geworden. XP war ein Hit. Nicht nur für Privatanwender, sondern auch für Unternehmen und andere Institutionen. Selbst militärische Einrichtungen haben es eingesetzt.

Um mal ein besonders eindrückliches Beispiel zu geben: Selbst auf den mit Atomsprengköpfen ausgerüsteten U-Booten der britischen Marine war bis mindestens 2016 eine Variante von XP installiert, wahrscheinlich hat sich daran seither nichts geändert.

Nun hängt so ein U-Boot nicht am Internet, was die Infektion mit einer Malware schon extrem viel unwahrscheinlicher macht. Aber das Beispiel veranschaulicht etwas anderes: Viele Institutionen haben lange keinen zwingenden Anlass gesehen, die Mühen eines Systemwechsels auf sich zu nehmen.

Updates kosten Zeit und Geld

Systemadministratoren können mehrere Gründe aufzählen, warum Unternehmen und Organisationen so zögerlich waren und sind. Der XP-Nachfolger Vista etwa galt als unausgereift und wurde zum Flop, er war also nie eine echte Option. Peripherie-Geräte wie Drucker, von industriellen oder medizinischen Spezialgeräten und -programmen ganz zu schweigen, müssen auf das jeweilige System angepasst werden und dabei mitunter bestimmte rechtliche Vorgaben erfüllen – niemand baut so ein ganzes Ökosystem gerne um. Es gilt: *"**Never change a running system**"*.

Mit beträchtlichen Kosten, vielleicht auch Produktionsausfällen, wäre es ohnehin verbunden, was sich zum Beispiel Krankenhäuser oder Mittelständler nicht immer leisten können oder wollen. Das gilt auch für den Support, den Microsoft noch immer für XP anbietet. Solang alles funktionierte, durften sich XP-Nutzer bestätigt fühlen. Wer hätte sich vor vier Jahren schon eine Ransomware-Attacke wie die jetzige vorstellen können?
Vorerst ist die gestoppt. Die Erpresser-Software verbreitet sich momentan nicht mehr weiter, weil Sicherheitsforscher – eher zufällig – den *Kill Switch* gefunden haben. Vorbei ist die Gefahr aber nicht. IT-Sicherheitsexperten sagen bereits, dass die Täter vom Freitag eher amateurhaft vorgegangen seien. Der nächste Angriff könne viel bösartiger ausfallen, die Anleitung – sprich: der Code – stehe schließlich offen im Netz.

Das Mindeste, was Nutzer von XP und anderen alten Windows-Systemen nun tun müssen, ist das Notfall-Update von Microsoft einzuspielen. Doch ähnlich wie bei einem Systemwechsel kann auch ein reines Update dazu führen, dass in einem komplexen Netzwerk plötzlich Dinge nicht mehr funktionieren. Es ist deshalb zu befürchten, dass manche Anwender es deshalb darauf ankommen lassen werden und einfach hoffen, dass sie auch dem nächsten Angriff irgendwie entgehen.

Ransomware

Alles, was schief gehen konnte

Der weltweite Ransomware-Angriff auf Firmen, Organisationen und sogar Krankenhäuser ist das Ergebnis eines perfekten Sturms. Mitschuldig sind die NSA und träge Anwender.

Von **Patrick Beuth**

13. Mai 2017, 1:10 Uhr / 271 Kommentare

Das Drehbuch für diesen denkwürdigen Freitag, an dem innerhalb von Stunden 45.000 Computer in aller Welt lahmgelegt wurden, entstand am 15. April. Es beinhaltet Aussagen wie: "Dies ist ein Ein-Knopf-Hack. Du drückst den Knopf und der Server gehört dir. Alles, was du willst. Es ist superböse. Verrückt böse." Oder auch: "Du hast keine Ahnung, wie schlimm das ist, wenn du nicht in der IT eines Unternehmens arbeitest. Diese Sicherheitslücke wird zehn Jahre lang bestehen, oder länger."

Geschrieben hat das alles die Person, die sich auf Twitter @SwiftOnSecurity nennt. Wer dahinter steckt, ist unbekannt.

Aber der einstige Satire-Account mit seiner schrägen Mischung aus Taylor-Swift-Songzeilen und Tipps zur IT- und Informationssicherheit wird in der Fachwelt längst ernst genommen. Denn wer auch immer dahinter steckt, hat offensichtlich eine Menge Ahnung vom Thema.

Den weltweiten Angriff mit der Ransomware WannaCry (auch WannaCrypt, WanaCrypt0r, Wcrypt oder WCRY genannt), die verschiedenste Dateien verschlüsselt und löschen kann, wenn das Opfer kein Lösegeld zahlt, hat SwiftOnSecurity zumindest auf einer Ebene vorhergesehen: Er war offenbar möglich, weil er auf einer schweren Sicherheitslücke in fast allen Windows-Versionen basiert, die nicht von jedem Nutzer geschlossen werden kann.

Ein "worst case scenario" nach dem nächsten

Doch der Hintergrund zu dem so globalen wie katastrophalen Angriff, von dem Firmen, Krankenhäuser, Universitäten und auch die Deutsche Bahn betroffen sind, hat mehrere Ebenen, zusammen ergeben sie den perfekten Sturm.

So war es allem Anschein nach die NSA, die diese Sicherheitslücke entdeckt hat. Entdeckt, aber nicht veröffentlicht, sondern für eigene, offensive Einsatzzwecke geheim gehalten.

Patrick Beuth *Redakteur im Ressort Digital, ZEIT ONLINE*

Dann trat ein erstes *worst case scenario* ein: Die NSA verlor die Kontrolle über ihre Werkzeuge. Im August 2016 fing jemand (oder eine Gruppe) an, Methoden, Anleitungen und Angriffscode des US-Geheimdienstes im Internet zu veröffentlichen. Shadow Brokers nannten sich die Täter. Es sah anfangs nach einem extrem aufwendigen Scherz aus, doch die Kostproben wirkten überzeugend. Im April 2017, nach mehreren weiteren Veröffentlichungen, kündigten die Shadow Brokers ihren Rückzug an. Doch ein letztes Paket mit NSA-Tools stellten sie am 14. April noch offen ins Netz – und das hatte es in sich. Belege für Hacks der NSA gegen Banken und das Swift-System waren darunter, aber auch öffentlich unbekannte, schwere Sicherheitslücken in Windows. Und jeder konnte sie sich nun zunutze machen.

Noch am 14. April versuchte Microsoft zu beruhigen: Das Unternehmen habe die Schwachstellen behoben, schrieb es in diesem Blogpost. Und zwar bereits im März, wie aus den Details hervorgeht. Das Unternehmen wusste also davon, bevor die Shadow Brokers damit an die Öffentlichkeit gingen. Was bedeuten könnte, dass die NSA Microsoft gewarnt hat.

Dennoch trat erneut der schlimmstmögliche Fall ein: Die Sicherheitspatches wurden von Microsoft nicht an die große Glocke gehängt und viele Institutionen rund um den Globus brachten ihre Systeme nicht auf den neuesten Stand. Sei es aus Unwissen oder aus Bequemlichkeit. Oder weil sie immer noch das ebenfalls betroffene Windows XP verwenden, dessen Support Microsoft 2014 eingestellt hat – verbunden mit einer Warnung und dem dringenden Rat, ein neueres, sichereres System zu installieren. Wer keinen individuellen, sehr teuren Supportvertrag mit Microsoft hat, kann die Lücke gar nicht mehr schließen.

IT-Sicherheit und Patientensicherheit hängen eng zusammen

Genau das haben sich die Täter nun bei ihrer Ransomware-Kampagne zunutze gemacht. Die Lücke ist das Einfallstor in die veralteten Systeme und sorgt dafür, dass sich die Erpressungssoftware installiert.

Der nächste Bestandteil des perfekten Sturms wird daran erkennbar, dass zu den besonders Betroffenen auch mehrere Krankenhäuser in Großbritannien gehören. Wie *Motherboard* im vergangenen Jahr herausgefunden hat, ist XP dort noch immer weit verbreitet. Oftmals ohne Supportvertrag.

Ransomware-Angriffe auf Krankenhäuser gab es in der Vergangenheit schon mehrfach, auch in Deutschland. Die Träger müssten also längst gewarnt sein. Trotzdem stehen moderne, vergleichsweise sichere IT-Systeme offensichtlich nicht besonders weit oben auf ihren Prioritäten- und Investitionslisten.

Warum zu einer neuen, teureren Windows-Version wechseln, wenn die alte doch noch läuft, dürften sich viele Verantwortliche sagen – und ihr oft knappes Budget lieber in andere Bereiche stecken, die näher am Patienten sind. Wie eng IT-Sicherheit und Patientensicherheit zusammenhängen, wird nun wahrscheinlich auch der Letzte verstanden haben. Jetzt, da es erst einmal zu spät ist.

Wirklich perfekt – im übertragenen Sinne natürlich – wird dieser Sturm dann, wenn sich herausstellen sollte, dass kaum ein betroffenes Unternehmen, kaum eine Organisation eine aktuelle Sicherungskopie ihrer Daten hat.


ZEIT ONLINE

Such

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Arbeit Entdecken Sport ZEITmagazin mehr ▾

WannaCry

Großer Schaden für 31.000 Dollar

Finanziell hat sich der Angriff der WannaCry-Erpresser bisher kaum gelohnt. Der Schaden aber ist enorm. Es zeigt sich, was passiert, wenn Geheimdienste Lücken nutzen.

Von **Kai Biermann**

14. Mai 2017, 11:19 Uhr / Aktualisiert am 14. Mai 2017, 14:35 Uhr / 207 Kommentare

Sie haben weltweit für Ärger und Verwirrung gesorgt, viel Geld aber haben sie bisher nicht eingenommen: Am Freitag starteten Kriminelle den sogenannten WCry, WannaCry oder Wanna-Decryptor-Angriff, um von Betroffenen Geld zu erpressen, indem sie die Daten auf den befallenen Rechnern verschlüsselten. Weltweit wurden dabei wohl mehr als 75.000 Rechner in rund 100 Ländern angegriffen. Bislang sind aber offenbar nur wenige Betroffene bereit, das geforderte Lösegeld zu zahlen. Bis Sonntagvormittag wurden knapp 31.000 Dollar an die Kriminellen gezahlt.

Die Einnahmen der Angreifer sind in Echtzeit sichtbar, weil die Täter die Zahlung in Bitcoin fordern. Hat der Erpressungswurm einen Computer infiziert, sucht er dort nach allen möglichen Dateiformaten und beginnt, die Daten zu verschlüsseln. Anschließend wird der Nutzer aufgefordert, innerhalb von drei Tagen Bitcoin im Wert von 300 Dollar zu zahlen, sonst verdoppele sich der Preis. Wer bis zum 19. Mai nicht gezahlt habe, verliere seine Daten endgültig.

In den Schadprogrammen sind dazu drei unterschiedliche Bitcoin-Adressen fest programmiert – sogenannte Wallets, Brieftaschen –, an die das Geld überwiesen werden soll. Eine davon steht beispielsweise in den Erpressungsnachrichten, die bei der Deutschen Bahn auf Bildschirmen erschien.

Alle Transaktionen, die mit Bitcoins erfolgen, werden in Form einer sogenannten Blockchain in einer Datenbank abgelegt. Diese Datenbank ist dezentral auf Tausenden Rechnern verteilt. Ihre Einträge können von jedem nachvollzogen werden. Und so kann auch jeder die Einnahmen verfolgen, die die Kriminellen erzielen. Ein Reporter des Onlinemagazins *Quartz* hat dazu einen Twitterbot aufgesetzt, der die drei Bitcoin-Wallets der Kriminellen beobachtet und jedes Mal einen Tweet absetzt, wenn eine Zahlung eingeht. Derzeit registriert der Bot zwei bis drei Einzahlungen pro Stunde. Außerdem weist er von Zeit zu Zeit das Gesamtergebnis aus: Am Sonntagvormittag waren es demnach 30.706 Dollar. Es soll aber noch eine vierte Bitcoin-Adresse der Kriminellen geben, weswegen die Einnahmen möglicherweise höher sind.

Die Bitcoin-Datenbank speichert nicht nur Zahlungseingänge. Sollten die Kriminellen versuchen, das Geld aus ihren Wallets abzuheben, ist das ebenfalls sichtbar. Wenn sie dabei Fehler machen, könnte das zu ihrer Identifizierung führen. Zwar bieten verschiedene Dienste an, Bitcoins unterschiedlicher Nutzer miteinander zu vermischen oder das Nachverfolgen des Geldes durch komplexe Transaktionen zu erschweren. Gleichzeitig gibt es aber auch Werkzeuge, die genau solche Umwege aufdecken können.

Unternehmen und Organisationen weltweit betroffen

Das Bundeskriminalamt ermittelt bereits gegen die Täter. Und die europäische Polizeibehörde Europol fordert eine internationale Untersuchung, da es sich um eine Attacke in einem bisher noch nie dagewesenen Ausmaß gehandelt habe. Die *New York Times* hat eine Karte erstellt, die zeigt, wie sich der Erpressungswurm weltweit verbreitet hat.

Die Attacke traf neben vielen privaten Nutzern unter anderem britische Krankenhäuser, ein Werk des japanischen Autoherstellers Nissan im englischen Sunderland, die Produktion in mehreren französischen Werken von Renault in Frankreich sowie Fahrplananzeigen, Ticketautomaten und Überwachungskameras der Deutschen Bahn. Auch russische Banken, chinesische Geldautomaten und Schulen sowie der amerikanische Lieferdienst FedEx sind betroffen.

Der Schaden, den der Angriff verursachte, dürfte daher weitaus größer sein als die Einnahmen der Kriminellen. Dabei halten IT-Sicherheitsexperten die Täter nicht unbedingt für Genies. Dass das Schadprogramm sich so rasant verbreitet hat, lag wohl vor allem an der ausgezeichneten Vorarbeit des US-Geheimdienstes NSA. Die hatte die Lücke in dem Microsoft-Code entdeckt.

Zwar warnte der Geheimdienst das Unternehmen, programmierte aber gleichzeitig wohl auch das Werkzeug (mit dem NSA-Codenamen Eternalblue), das die Lücke ausnutzt. Die NSA wollte es offenbar für ihre Zwecke einsetzen. Eine Hackergruppe namens Shadow Brokers veröffentlichte es dann vor Kurzem zusammen mit vielen anderen IT-Werkzeugen der NSA, um vor den Gefahren dieser Politik zu warnen, Kriminelle nutzten es nun für ihre Zwecke.

Die NSA ist daher zumindest mitverantwortlich, auch wenn das eigentliche Problem die vielen Rechnersysteme sind, die nicht auf einem aktuellen Stand gehalten werden, um Geld zu sparen. Kritiker wie der Grüne Bundestagsabgeordnete Konstantin von Notz fordern daher, dass Geheimdienste solche Lücken nicht ausnutzen dürften, da die gesellschaftlichen Kosten höher seien als der Informationsgewinn der Dienste.

Trojaner wurde womöglich aktualisiert

Update: Die erste Welle des Trojaners enthielt einen sogenannten *kill switch*, eine Abschaltautomatik. Ein IT-Sicherheitsforscher hatte diesen Schalter unabsichtlich aktiviert, als er eine Website registrierte, deren Adresse im Schadcode enthalten war. Daraufhin kontaktierten die Schadprogramme diese Website und verbreiteten sich nicht weiter.

Inzwischen aber scheinen Varianten des Trojaners im Umlauf zu sein, die diesen Aus-Schalter nicht mehr enthalten, wie mehrere Medien das IT-Sicherheitsunternehmen Kaspersky zitieren. Der Rat, den alle Sicherheitsexperten übereinstimmend geben, gilt daher weiter: Windows-Systeme sollten unbedingt mit dem Sicherheitsupdate von Microsoft aktualisiert werden.


ZEIT ONLINE

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Arbeit Entdecken Sport ZEITmagazin

Schadsoftware

Bezwinger von WannaCry in den USA festgenommen

Das FBI wirft Marcus Hutchins vor, einen Banking-Trojaner entwickelt zu haben. Bekannt geworden war der Brite, als er die Abschaltfunktion der Ransomware WannaCry fand.

4. August 2017, 7:26 Uhr / Quelle: ZEIT ONLINE, AP, dpa, jp, pb / 49 Kommentare

Das FBI hat den britischen IT-Experten Marcus Hutchins festgenommen. Ihm wird vorgeworfen, Schadsoftware für die Sammlung von Onlinebanking-Zugängen programmiert und verbreitet zu haben. Dem FBI zufolge wurde er in Gewahrsam genommen, als er auf dem Heimweg von den Hackerkonferenzen Black Hat und Def Con in Las Vegas war.

Hutchins war an der Abwehr der globalen WannaCry-Attacke im Mai beteiligt. Er war es, der die Ausbreitung der Ransomware stoppte, als er eine Webadresse in deren Quellcode fand, für die es aber keine Website gab. Als er die Domain für 10,69 US-Dollar registrieren ließ, betätigte er damit unwissentlich den *kill switch* von WannaCry. Möglicherweise war die Domain ein eingebauter Testmechanismus, mit dem die Malware überprüfte, ob sie bereits IT-forensisch untersucht wird – solange die Domain nicht registriert war und auf die regelmäßigen Kontaktversuche von WannaCry dementsprechend auch nicht reagieren konnte, blieb WannaCry aktiv.

Für seinen Fund wurde der damals 22-jährige Hutchins, der für die Firma Kryptos Logic arbeitet und sich bis dahin öffentlich nur unter dem Pseudonym MalwereTech geäußert hatte, zum unfreiwilligen Helden erklärt. Britische Medien veröffentlichten seinen vollen Namen.

Die Entwicklung von Malware ist nicht zwingend illegal

WannaCry hatte am 12. April weltweit Computerdaten verschlüsselt und Lösegeld gefordert. Die Schadsoftware nutzte dafür eine Sicherheitslücke von Microsoft. In Deutschland war beispielsweise die Deutsche Bahn betroffen, die Regierungsnetze nach ersten Angaben aber nicht. Es war die bis dato weitreichendste Ransomware-Attacke.

Nun aber wird ihrem Bezwinger Hutchins vorgeworfen, zusammen mit einem weiteren Angeklagten zwischen Sommer 2014 und Sommer 2015 den Bank-Trojaner Kronos geschaffen und zum Verkauf angeboten zu haben, unter anderem auf der mittlerweile geschlossenen Darknetplattform AlphaBay. Das Programm fängt über täuschend echt nachgemachte Websites von Banken die Benutzernamen und Passwörter von Kunden ab. Das geht aus der Anklageschrift hervor, die aber keine Beweise enthält, sondern nur die Vorwürfe. Der Name des zweiten Verdächtigen ist in dem Dokument geschwärzt.

Entscheidend für eine Anklage ist nach Einschätzung des Rechtsprofessors Orin Kerr, ob Hutchins und dem zweiten Verdächtigen nachgewiesen werden kann, dass sie Kronos verkaufen wollten, damit andere damit etwas Illegales tun. Denn weder die Entwicklung noch der Verkauf von Malware ist zwingend rechtswidrig – andernfalls gäbe es keine kommerzielle Überwachungssoftware für Strafverfolger.

Laut Anklageschrift wird Hutchins und der zweiten Person eine "Verschwörung" zur Verletzung des Computer Fraud and Abuse Act vorgeworfen, die Verletzung eines US-Gesetzes zum Verkauf und Bewerben von Abhörtechnik, das Abhören selbst sowie die Beihilfe zum Computerhacking.

Sicherheitsforscher von IBM hatten 2014 Werbung für Kronos in einem russischen Onlineforum entdeckt. Dort schrieben die Anbieter unter anderem, die 7.000 Dollar teure Malware sei besonders für "erfolgreiche Banking-Aktionen" gemacht. Das US-Justizministerium teilte mit, Kronos sei noch immer eine Bedrohung für die Sicherheit und die Privatsphäre von Internetnutzern.