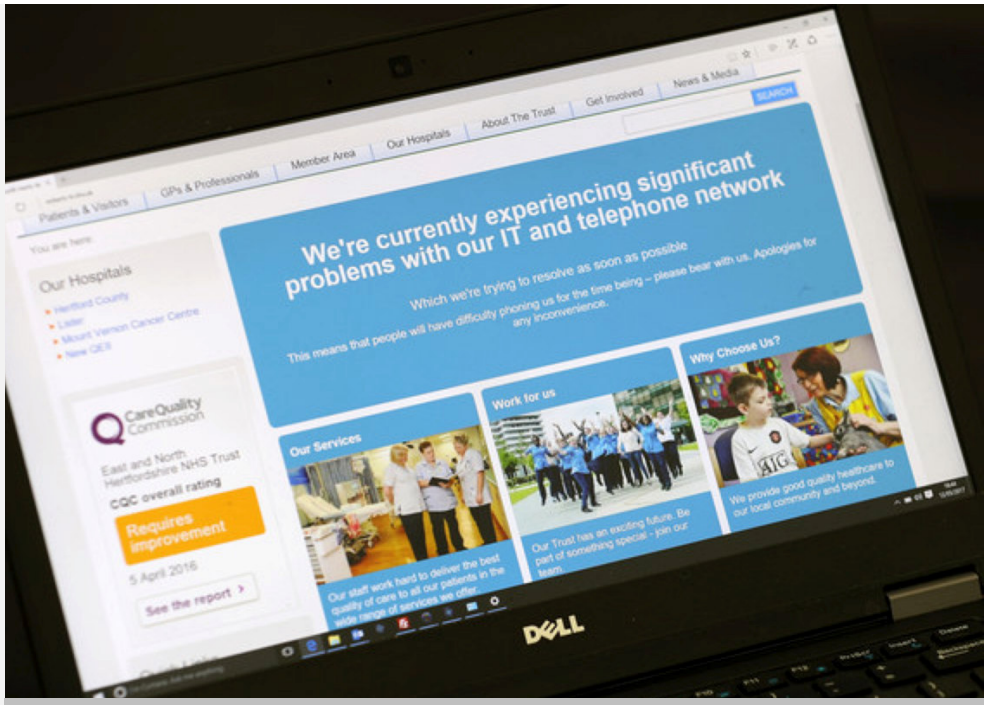
Im Dickicht der Cybersecurity

Experte

Dr. Frank Umbach

Region:

Nordamerika



12. Mai 2017: Der Erpressungs-Trojaner WannaCry setzte ein Drittel des IT-Netzwerks des britischen Nationalen Gesundheitdienstes (NHS) außer Betrieb und verzögert so viele Abläufe (Foto: dpa)

Ein weltweiter Anstieg der ausgeklügelten Cyberattacken auf industrielle Kontrollzentren hat Unternehmen, Regierungen und Cybersecurity-Experten gleichermaßen alarmiert. Solange es schwierig bleibt, die Quellen von Cyberattacken zu identifizieren, während offensive Cyber-Tools immer alltäglicher und leichter zugänglich für Schurkenstaaten, Dschihadisten und Cyber-Kriminelle auf der ganzen Welt werden, darf man erwarten, dass derartige Angriffe auf Informations- und Kontrollsysteme (ICS) zunehmen. Zerstörerische Angriffe auf kritische Infrastrukturen haben längst die „roten Linien" früherer Prognosen überschritten. Trotzdem können wir den Umfang der künftigen Bedrohungen der Cybersicherheit gar nicht unterschätzen.

Der Erpressungs-Trojaner „WannaCry" verschlüsselte im Mai 2017 weltweit auf Festplatten gespeicherte Daten und er forderte von den Opfern eine Zahlung in Höhe von 300 Dollar in Bitcoin, damit diese den Entschlüsselungscode erhielten.

Es war der jüngste Weckruf für die hochindustrialisierten Nationen, vor allem die Vereinigten Staaten und Europa, die sich bisher nicht ausreichend genug vorbereitet haben, um umfassende Cyberattacken abzuwehren. Durch die Ausnutzung von Sicherheitslücken in den größten Organisationen und Unternehmen hat WannaCry unterstrichen, wie stark die globale digitale Wirtschaft mittlerweile untereinander vernetzt ist – mit gemeinsamen kritischen Infrastrukturen (CIs), die in vielen Ländern das Rückgrat von Handel, Wohlstand und Sicherheit bilden.

Die bösartige Software, von der Hunderttausende Computer in mehr als 150 Ländern befallen waren, wurde als eine der bisher virulentesten und weitreichendsten Cyberattacken bezeichnet. Ihre deutlich sichtbaren Auswirkungen auf den britischen Nationalen Gesundheitsdienst (NHS), wo ein Drittel des IT-Netzwerks ausfiel, zeigten die potenziell verheerende Wirkung auf kritische Infrastrukturen wie Krankenhäuser. WannaCry infizierte einige der weltweit größten Konzerne, darunter den spanischen Mobilfunk-Riesen Telefonica, die Deutsch Bahn, den französischen Automobilhersteller Renault und den US-amerikanischen Logistikgiganten FedEx. Er verbreitete sich auch nach Russland und zwang dort das Innenministerium, mehr als 1.000 seiner Computer offline zu nehmen. In China waren fast 30.000 Institutionen betroffen.

Ein markantes Merkmal der WannaCry-Cyberattacke war ihre wahllose Natur. Es wurden keine spezifischen Institutionen ins Visier genommen, doch die britischen Krankenhäuser waren gezwungen, Operationen und andere Behandlungen von Patienten zu verzögern oder abzubrechen. Auch der Mangel an Vorbereitung war offensichtlich. Cybersecurity-Experten nannten die NHS-Informationssysteme einen Sicherheits-Alptraum, der enorme Investitionen erfordert, um sie auf den neuesten Standard zu bringen.

Kurz nach der Veröffentlichung leistungsstarker Hacking-Tools, die angeblich von der National Security Agency (NSA) gestohlen worden waren, zeigte der Wannacry-Ausbruch das Ausmaß, in dem Regierungen und Unternehmen durch konstante und zunehmend anspruchsvolle Cyberattacken aus rivalisierenden Nationalstaaten und von deren Geheimdiensten, von Terroristengruppen, Hackern und Cyberkriminellen

ins Visier genommen werden. Aktuelle Einschätzungen über dieses Ausmaß der Bedrohung stehen hier in dieser Faktbox:

Faktbox: Einschätzung der Bedrohung

• Die wirtschaftlichen Verluste aus der Cyberkriminalität übersteigen den weltweiten Gewinn aus dem Drogenhandel (Quelle: Europol)

• Über 70% der Unternehmen, die durch Erpressungs-Malware angegriffen wurden, bezahlten Lösegeld, oft in der anonymen digitalen Währung Bitcoin (IBM Research)

• Cyberattacken auf Informations- und Kontrollsysteme (ICS) stiegen im Jahr 2016 um 110% (IBM Research)

• Die Cyberkriminalität in Deutschland verdoppelte sich im Jahr 2016 im Vergleich zum Vorjahr auf 82.000 Fälle, was zu einem Schaden von über 51 Millionen Euro führte (diese Zahlen beruhen auf den gemeldeten Angriffen und könnten nur die Spitze des Eisbergs sein) (Deutsches Bundeskriminalamt)

• Mehr als 67% der Institutionen bemerken gar nicht, dass sie Ziel einer Cyberattacke geworden sind, bis sie eine dritte Partei darauf aufmerksam macht (FireEye)

• Die Institutionen und Unternehmen in den USA benötigen durchschnittlich 99 Tage, um eine Attacke zu bemerken; in Europa kann das bis zu 200 Tage dauern (FireEye)

• Für ein Drittel der 1.552 bekannten ICS-Schwachstellen gab es zum Zeitpunkt ihrer Offenlegung noch keine Reparaturmöglichkeit (FireEye)

• Zwischen 17% und 93% der Software von großen Anbietern weisen Schwachstellen auf, für die es noch keine Lösung gibt (Kaspersky)

• Eine Umfrage unter 70 professionellen Hackern ergab, dass 88% glauben, dass sie innerhalb von 12 Stunden die Cybersecurity-Firewalls anvisierter Systeme durchbrechen können (Nuix)

• Bis 2020 werden die US-Unternehmen jährlich 101,6 Milliarden Dollar ausgeben, um sich gegen Hacker zu schützen (zum Vergleich: 2016 waren es noch 73,7 Milliarden Dollar) (International Data Corp.)

• Die weltweiten Kosten aus der Internetkriminalität verdoppeln sich bis 2021 auf 6 Billionen US-Dollar von 3 Billionen US-Dollar im Jahr 2015. Diese Kosten beinhalten die Schädigung und Zerstörung von Daten, verlorene Produktivität, den Diebstahl von geistigem Eigentum und personenbezogenen Daten, Betrug, Unterschlagung, Betriebsstörungen, die Löschung und Wiederherstellung gehackter Systeme und

Reputationsschäden (Cybersecurity Ventures)

• Kreditkartenbetrug wird voraussichtlich von 4 Milliarden Dollar im Jahr 2016 auf 20 Milliarden Dollar im Jahr 2020 steigen (CNBC)

• Der weltweite Cyber-Versicherungsmarkt könnte bis 2022 14 Milliarden Dollar an Prämien generieren und damit eine jährliche Wachstumsrate von fast 28% aufweisen (Allied Market Research)

Die meisten Cyberattacken werden von den betroffenen Unternehmen, insbesondere im Finanzsektor, nicht gemeldet, weil sie Reputationsschäden und den Verlust von Kunden gegenüber Wettbewerbern befürchten. Viele Firmen und Betreiber von kritischen Infrastrukturen sehen keine Alternative zum Lösegeld, da der Verlust von tagesaktuellen Daten zu schwerwiegend ist und sogar zu Todesfällen führen kann (z. B. bei der Patientenüberwachung oder Operationen in Krankenhäusern).

Silberstreif am Horizont

Der positive Aspekt der Verbreitung von Cyberattacken ist, dass sie das internationale Bewusstsein und die Zusammenarbeit bei der Bewältigung des Problems erhöht haben. Die westlichen Länder teilen sich aktiv Fachwissen und Informationen – mit konkreten Ergebnissen.

Im Jahr 2016 z.B. haben Forscher aus mehr als 40 Ländern, darunter auch die USA, zusammengearbeitet, um das globale Avalanche-Phishing-Netzwerk zu zerstören, das seit mindestens 2009 betrieben wurde. Phishing ist ein Versuch, sensible Informationen wie Benutzernamen, Passwörter oder Kreditkartenangaben durch elektronische Kommunikation zu erhalten, indem man vorgibt, eine vertrauenswürdige Quelle darzustellen. Avalanche bestand aus einem verstreuten Cloud-Hosting-Netzwerk von bis zu 600 Servern und 500.000 infizierten Computern, die von Cyberkriminellen gemietet wurden, um weltweite Phishing- und Malware-Angriffe zu starten.

Trotz dieser Fortschritte konnten jedoch die Vorbereitungs- und Verteidigungskapazitäten nicht mit den offensiven Fähigkeiten transnationaler krimineller Organisationen und staatlich unterstützter Hackergruppen Schritt halten.

Stillschweigen oder offenlegen

Die WannaCry-Schadsoftware unterstrich auch die konkurrierenden Sicherheitsinteressen zwischen privaten Akteuren und Regierungsinstitutionen – vor allem den Strafverfolgungs- und Sicherheitsbehörden, die selbst offensive Cyberwaffen entwickeln und einsetzen. Fehler und Schlupflöcher in weit verbreiteter kommerzieller Software werden von Militär- und Sicherheitsorganisationen genutzt, um den Terrorismus und die internationale Kriminalität zu bekämpfen sowie für nachrichtendienstliche und Anti-Terror-Operationen.

Im Fall von WannaCry wurde der Ausbruch nur möglich gemacht, weil ein anspruchsvolles Cyberspying-Tool – EternalBlue, das eine Sicherheitsanfälligkeit in File-Sharing-Protokollen der Microsoft Windows-Software ausnutzt – angeblich im vergangenen Jahr von der NSA gestohlen wurde, der Behörde, die die US-Signalaufklärung kontrolliert. Der wahrscheinlich Schuldige war eine Cybercrime-Gruppe, die als die „Shadow Brokers“ bekannt ist, und die im Verdacht steht, ein Verbündeter der russischen Geheimdienste zu sein. EternalBlue wurde dann zur schnelleren Verbreitung an andere Cyber-Akteure im „Darknet“ – dem Online-Marktplatz der globalen Unterwelt – weiterverkauft.

Das NSA-Tool ermöglicht es Hackern, sich durch verschiedene Netzwerke und zwischen Organisationen zu bewegen, indem sie legitime File-Sharing-Protokolle erstellen. Cyber-Experten hatten jahrelang vor solchen Schlupflöchern gewarnt, welche die US-Geheimdienste entweder für sich selbst geschaffen haben oder für die sie ihr Fachwissen nutzten, um sie zu verwenden. Microsoft äußerte sich sehr kritisch über die US-Regierung, die ihre Informationen über diese Schwachstellen nicht herausgab, was es ihr erlaubt, Cyber-Waffen „zu lagern“. Der Rechtsberater des Unternehmens, Brad Smith, sagte, dass diese Praxis das Äquivalent dazu wäre, als würde man zulassen, dass Kriminelle Tomahawk-Raketen stehlen. „Wiederholt sind die von der Regierung entdeckten Schwachstellen in die Öffentlichkeit gelangt und haben weit verbreitete Schäden verursacht“, sagte er in einem Blog vom 14. Mai.

Da Europa seine eigenen offensiven Cyber-Kapazitäten entwickelt, müssen seine Geheimdienste und Strafverfolgungsbehörden sorgfältig abwägen, ob sie Software-

Schwachstellen für sich behalten oder offen legen müssen. Dieses Kosten-Nutzen-Kalkül, das im Fachjargon als „Vulnerability Equities Process“ (VEP) bezeichnet wird, würde feststellen, ob Sicherheitsfehler, die Netzwerk- und Softwareanbietern unbekannt sind (Zero-Day-Schwachstellen), offengelegt oder zur Bekämpfung der Internetkriminalität und der Vereitlung von Angriffen genutzt werden sollen. Während alle westlichen Länder offiziell eine Politik der Offenlegung fördern, haben sie in der Praxis oft dafür gesorgt, sich Hintertüren und andere Mechanismen offenzuhalten, um auf verschlüsselte Kommunikationen zugreifen zu können.

Verbraucherkalkül

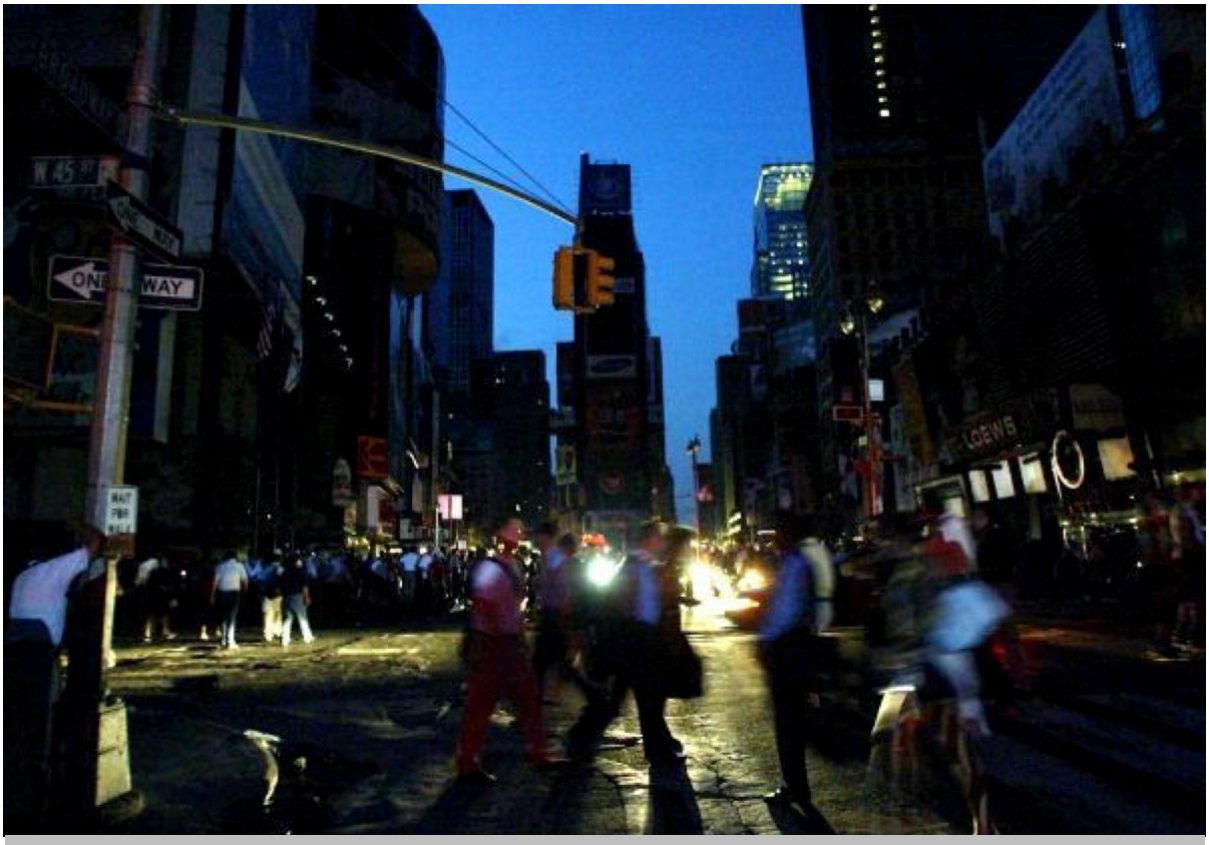
Die neue Welle der Informationstechnologie ist das „Internet der Dinge“ (Internet of Things – IoT). Es ist zu hoffen, dass diese Netzwerke aus Smart-Sensor-fähigen Geräten, die über das Internet kommunizieren und miteinander kooperieren, neue Unternehmen schaffen, „intelligente Städte“ verwalten und sogar medizinische Ferndienste verbreiten. McKinsey hat die jährlichen wirtschaftlichen Folgen des IoT bis 2025 auf weltweit 3,9 Billionen Dollar bis 11,1 Billionen Dollar geschätzt.

Da diese internetgebundenen Geräte weit verbreitet sind, könnten Verbrecher ihre Schwachstellen für Diebstahl und Datenverfälschung ausnutzen oder Zombie-Computernetze („Botnetze“) zur Verbreitung von Malware oder zur Beschädigung von Websites durch die Bombardierung mit Informationsanfragen erstellen.

Die IoT-Sicherheit wird gleich an mehreren Fronten zu einer Herausforderung. Erstens gibt es keinen übergreifenden Industriestandard, was die Entwicklung von End-to-End-Sicherheitslösungen behindert. Stattdessen haben wir inkompatible Technologien und mehrere Schwachstellen. Zweitens führt die Massenproduktion von IoT-Geräten eine Vielzahl neuer Angriffsvektoren ein. Da viele dieser Produkte sehr kurze Ersatzzyklen haben, wird es noch schwieriger, maßgeschneiderte Sicherheitstechnologien zu entwerfen.

Auch die Ökonomie der persönlichen Elektronik- und der Haushaltsgeräte spielt eine Rolle. Während sowohl die Kunden als auch die Produzenten die Sicherheit als wichtig ansehen, werden IoT-Geräte vor allem als Massengüter wahrgenommen, die

beim Preis konkurrieren. Kostensenkungen arbeiten gegen die Notwendigkeit, Systeme zu entwerfen, die Verstöße gegen private oder kommerzielle Daten verhindern. Bisher sind die Kunden meistens nicht bereit gewesen, mehr zu bezahlen – wie bei den Halbleiterunternehmen zu sehen ist, die darum kämpfen müssen, dass sie ihre Sicherheitsinvestitionen wieder erwirtschaften können. Die Produzenten müssen noch daran arbeiten, die Endnutzer zu überzeugen, dass es sich lohnt, für Sicherheit zu bezahlen.



Das Albtraum-Szenario ist eine Cyberattacke, die kritische Infrastrukturen lahmlegt. Im August 2003 saßen 45 Millionen Menschen im Nordosten der USA ohne Strom da, nachdem ein Softwarefehler im Netzalarmsystem eine Kaskadenreaktion bewirkt hatte (Foto: dpa)

Und schließlich werden die Unternehmen mit innovativen IoT-Anwendungen für kommerzielle Zwecke („Industrie 4.0“) mit speziellen Problemen konfrontiert, vor allem, weil sich viele Unternehmen und Hersteller auf veraltete Computersysteme und Software verlassen. Das Verbinden älterer Systeme mit dem Internet untergräbt die End-to-End-Sicherheit und setzt bisher stabile Fertigungsprozesse der Gefahr einer Attacke aus.

Staaten als Auftraggeber

Für Regierungen, die ihre kritischen Infrastrukturen und Industrien vor anspruchsvollen Cyberattacken und Spionage verteidigen müssen, stellen staatlich geförderte Bedrohungen (Advanced Persistent Threats, APTs) die größte Sicherheitsherausforderung dar. APTs sind in der Regel mit ausländischen Geheimdiensten oder nicht-staatlichen Hacker-Gruppen verbunden.

China, Russland, der Iran, Nordkorea und einige andere Länder wurden von westlichen Geheimdiensten beschuldigt, symbiotische und gegenseitig vorteilhafte Beziehungen zu kriminellen Gruppen aufzubauen. Diese Beziehungen basieren auf einer einfachen kommerziellen Logik. Da die Sicherheits- und Strafverfolgungsbehörden in diesen Ländern nur selten die privatwirtschaftlichen Gehaltsforderungen von Cyber-Experten erfüllen können, müssen sie weitere Anreize bieten. Dazu gehören die strafrechtliche Immunität und der Zugang zu Daten und Tools für ihre Cybercrime-Aktivitäten.

Russland hat seit Jahren Cyberattacken gegen seine internen Kritiker eingesetzt, deren E-Mails gestohlen und manipuliert oder deren elektronische Dokumente verfälscht werden. Die Techniken, die in diesen Operationen verfeinert wurden, wurden dann in anspruchsvolleren und innovativeren Cyberattacken auf kritische Infrastrukturen und ICS in den USA und Europa eingesetzt. Zu den bekanntesten Zielen dieser massiven und gut organisierten Operationen gehörten die Präsidentschaftswahlkampagnen der USA (2016) und Frankreich (2017), die von der Gruppierung „Fancy Bear“ (auch als APT28 Group bekannt) gehackt wurden und die mit dem russischen Militärgeheimdienst GRU verbunden ist.

Diese Aktivitäten sind Teil einer breiteren, nicht deklarierten Kampagne des asymmetrischen Hybridkriegs, von dem man annimmt, dass der Kreml ihn gegen die westlichen Demokratien führt. Diese Bemühungen umfassen Fake News und andere Formen der Desinformation, die dazu entworfen wurden, um Zweifel und Ungewissheit zu säen, während sie neue Narrative für die öffentliche Meinung formulieren. Das deutsche Bundesamt für Verfassungsschutz (BfV) und sein Bundesamt für Sicherheit in der Informationstechnik (BSI) haben Russland

beschuldigt, im Mai 2015 mittels einer Cyberattacke große Mengen persönlicher und politischer Daten der Abgeordneten des Deutschen Bundestags gestohlen zu haben. Das BfV hat behauptet, „immer mehr Beweise für Versuche zur Beeinflussung der Bundestagswahl“ im Herbst 2017 gefunden zu haben und forderte deshalb nach Gesetzesänderungen, die die Zerstörung gefährlicher Server von Hackern erlauben sollen.

Fallstudie: Das Energienetz der Ukraine

Da alle kritischen Infrastrukturen, die direkt oder indirekt mit dem Internet verbunden sind, auf eine stabile Stromversorgung angewiesen sind, gelten nationale Stromnetze als Achillesferse hochindustrialisierter Gesellschaften. Erfolgreiche Cyberattacken in diesen Netzwerken würden die Volkswirtschaften und politischen Systeme dieser Länder sofort destabilisieren.

Ein landesweiter Stromausfall gilt gemeinhin als eine der gefährlichsten Konsequenzen einer Cyberattacke. Experten haben seit Jahren gewarnt, dass die automatisierten industriellen Systeme, die CIs kontrollieren, wie Kraftwerke und Stromnetze, extrem anfällig sind. Die hypothetischen Szenarien eines „Cyber Pearl Harbours“ fanden eine Bestätigung in der Realität, als das Stromnetz der Ukraine im Dezember 2015 von einer gut koordinierten externen Cyberattacke getroffen wurde. Es war der weltweit erste bekannte digitale Angriff dieses Ausmaßes und dieser Cyber-Einbruch verursachte weit verbreitete Energieausfälle, die bis zu sechs Stunden andauerten.

Kriminaltechnische Untersuchungen durch ukrainische und westliche Geheimdienste sowie durch unabhängige Informations- und Kommunikationstechnologiker gelangten zu dem Schluss, dass der Angriff von einer russischen Hackergruppe namens „Sandworm“ durchgeführt worden war, die zuvor Energieunternehmen in den USA und Europa attackiert hatte. Der Trojaner BlackEnergy wurde verwendet, um Fernzugriff auf die Überwachungs- und Datenerfassungs-Systeme (SCADA) der anvisierten Unternehmen zu erhalten. Sobald die Sicherheitsbarrieren durchdrungen waren, zerstörte eine Malware namens KillDisk Dateien, was das SCADA-System inoperabel machte und die Reparatur erheblich erschwerte.

Gleichzeitig wurden die Call-Center der ukrainischen Energieunternehmen einer koordinierten Cyberattacke unterzogen. Diese blockierte die Berichte der Kunden über die Stromausfälle und verlängerte so den Blackout. Das Endergebnis war die Störung der Stromversorgung von etwa 230.000 Menschen, so dass 103 Gemeinden völlig im Dunkeln saßen und weitere 186 teilweise der Energie beraubt waren.

Der Angriff von 2015 auf das Stromnetz der Ukraine war Teil einer langjährigen russischen Kampagne, die im Mai 2014 begann, als eine Aufklärungssonde Spear-Phishing-E-Mails nutzte, die gegen ein ukrainisches Energieunternehmen eingesetzt wurden. Das gleiche Unternehmen wurde im Dezember 2015 erfolgreich angegriffen. Ähnliche Cyberattacken wurden gegen alle sechs staatlichen ukrainischen Eisenbahnbetreiber, die Fernsehsender, die Stromverteiler in der Westukraine, die Staatsarchive und die Bergbauunternehmen gestartet. Die Angriffe haben sich in den folgenden Jahren fortgesetzt.

Im Gegensatz zu den hochindustrialisierten westlichen Ländern konnte die Ukraine innerhalb von drei bis sechs Stunden ihre Dienstleistungen wiederherstellen, indem sie auf einen manuellen Code umstellte. Die moderneren westlichen Stromversorgungssysteme könnten weniger anfällig für Hackerangriffe sein, aber es wäre auch schwieriger, sie wieder in Betrieb zu nehmen, da sie weitaus stärker von automatisierten Steuerungssystemen abhängig sind. Für diese Betreiber ist das Umschalten auf einen manuellen Code viel komplizierter oder könnte sogar unmöglich sein.

Die ukrainischen Erfahrungen zeigten auch, dass Fernzugriffsfunktionalität und insbesondere Modems unsicher sind und so weit wie möglich eingegrenzt werden sollten. Betreiber in den Niederlanden haben sich zum Beispiel für ein Smart-Metering ohne Fernabschaltungs-Option entschieden. Mit der Einführung von Smart Grids und Smart Metern in den Privathaushalten und in der Industrie wird die zukünftige Stromversorgung viel stärker den Cyber-Bedrohungen ausgesetzt sein, zum Teil weil sie Millionen neuer Einstiegspunkte in das Stromnetz schaffen. Weder Staaten noch Gesellschaften sind wirklich bereit für die kaskadierenden Auswirkungen einer Cyberattacke auf diese Systeme oder für die Reparaturarbeiten,

die nötig sein werden, um die Energie schnell wiederherzustellen, um katastrophale Schäden zu vermeiden.

Ausblick

Die WannaCry-Infektion hat erneut die Notwendigkeit einer stärkeren Regulierung hervorgehoben, um die Unternehmen und die Eigentümer kritischer Infrastrukturen dazu zu zwingen, an die Öffentlichkeit zu gehen, wenn sie Opfer einer Cyberattacke geworden sind. Die Sicherheitsrisiken für Informations- und Kontrollsysteme sind nicht auf ihre spezifischen Schwachstellen beschränkt, sondern sie sind systemischer Natur. Die Einführung neuer Technologien kann die Anfälligkeit der Gesellschaft gegenüber Cyberattacken nur noch weiter erhöhen.

Die endgültigen finanziellen Kosten von WannaCry waren nicht so schlimm, aber das nächste Mal könnte die Welt nicht so viel Glück haben. Innerhalb der nächsten zwei oder drei Jahre werden weitere 2 bis 3 Milliarden Menschen online gehen. Diese beispiellose Expansion erhöht den Spielraum für massive und synchronisierte Cyberattacken, die gleichzeitig auf Stromversorger, Gesundheitsnetzwerke, Chemieanlagen, Flugzeugsysteme, Finanzdienstleistungen, Telekommunikationsnetze und sogar nukleare Anlagen abzielen könnten.

Nach jüngsten Studien darf die Lahmlegung landesweiter kritischer Infrastrukturen für einen Zeitraum von Stunden, Tagen oder sogar Wochen nicht mehr länger als „Schwarzer Schwan“ – also als unvorhersehbares Ereignis – betrachtet werden. Es ist jetzt das Basisszenario geworden. Die einzige Frage ist, wann und wo es eintrifft.