KULTUR NEU ENTDECKEN

SWR2

Blackout um 0.00 Uhr

Die Ukraine als Testgelände für den Cyberkrieg

Von Inga Lizengevic

Sendung: Mittwoch, 8. Januar 2020
Redaktion: Wolfgang Schiller
Regie: Inga Lizengevic
Produktion: Dlf/SWR 2019

Musik

01 O-Ton Oleksii Yasinsky
Sprecher 1
Wir haben gerade den «Snowden»-Film gesehen. Da ging das Licht aus. Ich habe auf die Uhr geschaut. Es war Punkt Null Uhr.

Autorin
Kyiv, die Nacht vom 16. auf den 17. Dezember 2016

02 O-Ton Oleksii Yasinsky
Sprecher 1
Es kommt schon vor, dass das Netz im Winter durch elektrische Heizungen überlastet wird. Besonders, wenn es kalt ist. Aber dann brennt nur in einem Stockwerk die Sicherung durch. Das hier war anders. Meine Frau lachte: Das sind die Hacker. Jetzt sind sie zu uns nach Hause gekommen. Ich habe das gleiche gedacht ... auch, weil es Punkt Null Uhr geschah. Und man muss bedenken, unser Land ist im Krieg. Auf den Stromausfall hätte ein Bodenangriff folgen können.

Autorin
Auch ohne Bodentruppen hätte die Situation schnell eskalieren können.

03 O-Ton Oleksii Yasinsky
Sprecher 1
Vier Stunden. Vier Stunden hätten gereicht, damit das Wasser in den Rohren einfriert. Damals gab es kaum Schnee. Minus dreißig Grad, die Erde war durchgefroren. Das Eis hätte die Rohre zerrissen, auch die Pumpen. Wir waren nah an einer Katstrophe

Autorin
Es ist der zweite Angriff dieser Art. Fast genau ein Jahr zuvor, haben Hacker schon einmal die Stromversorgung der Ukraine attackiert.

Ansage
«Blackout um null Uhr. Die Ukraine als Testgelände für den Cyberkrieg».
Ein Feature von Inga Lizengevic

Atmo Zugfahrt

04 O-Ton Marina Krotofil
Sprecherin 1
Es ist ein Angriff auf die kritische Infrastruktur, die Zivilisten versorgt. Denken Sie an medizinische Geräte, die nicht ohne Strom funktionieren. Solche Angriffe gefährden das Leben von Zivilisten.

Autorin
Marina Krotofil ist angesehene Cybersicherheitsexpertin. Sie fährt zu einer Konferenz in den Niederlanden, um über die Vorfälle in der Ukraine zu sprechen.

05 O-Ton Marina Krotofil
Sprecherin 1
Doch weder der erste noch der zweite Angriff wurden jemals von irgendeiner Regierung verurteilt. Das ist besorgniserregend, weil die rote Linie weiter nach hinten verschoben wurde. Früher hätte man gesagt, hey, das ist nicht akzeptabel. Das ist ein Angriff auf die Zivilbevölkerung. Doch plötzlich ist es Normalität – in so einer Normalität möchte doch keiner leben.

Autorin
Spezialgebiet der gebürtigen Ukrainerin: Cybersicherheit von kritischer Infrastruktur. Als externe Beraterin unterstützte sie 2015 und 2016 die forensische Untersuchung der Hackerangriffe auf den ukrainischen Energie-Sektor.

06 O-Ton Marin Krotofil
Sprecherin 1
Diese Angriffe sind, abgesehen von Stuxnet, die ersten öffentlich bekannten Cyberangriffe, die einen physischen Schaden verursacht haben. Also sehen wir erstens, die Angreifer haben einen physischen Schaden verursacht, indem sie den Strom abgeschaltet haben. Zweitens, die Angreifer haben die entsprechenden Fertigkeiten und werden nicht aufgehalten. Und drittens stellt sich die Frage von Cyberkrieg und Ethik. Insbesondere, weil der Angriff auf Stromnetze ein Angriff auf Zivilisten ist.

Atmo Freizeichen Telefon

07 O-Ton Frauenstimme im Hörer
Stadtwerke Ettlingen.

08 O-Ton Andreas Salm
Ja, schönen guten Tag. Mein Name ist Andreas Wellner, schönen guten Tag.

Autorin
Das Dachgeschoss eines Bürogebäudes - die Firma HiSolutions, Berlin Treptow. Teil Eins eines sogenannten Pentrationstests. Andreas Salm versucht, eine Mitarbeiterin der Stadtwerke Ettlingen zu übertölpeln.

10 O-Ton Andreas Salm
OK. Lassen Sie mich Ihnen einen Kontext geben. Ich bin von einer Organisation, die Tischtennis-Firmenmeisterschaften oder Turniere deutschlandweit ausrichtet...

Autorin
Salm hat die Eckdaten seiner erfundenen Identität auf ein Whiteboard geschrieben. Name, Adresse, Geburtsdatum... er möchte Vertrauen gewinnen, um die Dame in Ettlingen später zu einem Klick zu bewegen. Er möchte, das sie Warnhinweise ignoriert, und einen speziell präparierten Email-Anhang öffnet.

11 O-Ton Andreas Salm
Also ich würde das aber trotzdem nicht kampflos aufgeben wollen. Ich wollte versuchen Ihnen die Unterlagen zuzusenden. Vielleicht kann ich ja doch Ihr Interesse für die Veranstaltung wecken. Und wenn da Interesse besteht, dann würde ich mich

einfach über den Rückruf oder Antwort auf meine Nachricht freuen. Und dann können wir uns vielleicht auch gerne mal zusammensetzen.

Autorin
Penetrationstests ermöglichen Unternehmen, den Zustand ihrer IT-Sicherheit einzuschätzen und Sicherheitslücken zu schließen. Die Firma HiSolutions und die Stadtwerke Ettlingen haben sich bereit erklärt, für den Deutschlandfunk einen solchen Penetrationstest durchzuführen, und beobachten zu lassen.

13 O-Ton Andreas Salm
OK, gut dann würde ich Ihnen das jetzt direkt dahin zusenden. Und dann freue ich mich auf eine Rückmeldung von ihnen. Ja, danke. Wiederhören... gut, OK. Aber jetzt haben wir einen Vorwand und können da grad eine Mail schicken. Das sollten wir jetzt auch gleich machen, weil sie muss ja gleich weg.

Autorin
Salm fasst das Telefongespräch in einer E-Mail zusammen und fügt einen Link zum Download hinzu. Die Mitarbeiterin der Stadtwerke soll ein Dokument herunterladen und öffnen. Um das Dokument zu öffnen, muss sie einen Warnhinweis wegklicken. Echte Angreifer könnten sich dann im System der Stadtwerke ausbreiten. Um die Erfolgschancen zu erhöhen, werden parallel ähnliche Attacken auf andere Mitarbeiter der Stadtwerke gestartet. Auch die Hackerangriffe in der Ukraine begannen im Frühjahr 2015 ein halbes Jahr vor dem ersten Blackout mit einer E-Mail.

Musik

17 O-Ton Oleksii Yasinsky
Sprecher 1
Die Mail war an einen Juristen addressiert und enthielt als Anlage eine Excel-Tabelle und ein PDF mit einem Gerichtsbeschluss. In der Mail befand sich auch ein Bild, das nicht automatisch geladen wurde. Stattdessen gab es die Aufforderung, zu klicken, um das Bild zu laden. Der Server mit dem das Bild verbunden war, befand sich in der Türkei im Tor-Netz.

Autorin
Ein kleiner Konferenzraum mit einem großen Bildschirm. Oleksii Yasinsky, Leiter des ISSP Labs & Research Center, hat im Auftrag der Energieversorger die Angriffe in den Jahren 2015 und 2016 untersucht. Er zeigt mir einen Screenshot der Email. Betreff, Absender, Inhalt – alles stimmte mit den Erwartungen des Empfängers überein. Weder das Antivirenprogramm noch die Firewall lösten Alarm aus. Der Empfänger öffnete die Mail.

18 O-Ton Oleksii Yasinsky
Sprecher 1
Im Anhang war ein Virus. Es war auf eine einfache, jedoch elegante Art versteckt. Mail und Anhang haben die Spam- und Virenprüfung bestanden. Das Virus war mit gewöhnlichen Macros geschrieben, mit denen in Excel Prozesse automatisiert werden. Wenn man das Virus extrahiert, zeigt sich, dass es eine Backdoor namens BlackEnergy ist.

Autorin
BlackEnergy ist eine modular aufgebaute Schadware, die bereits 2007 auf dem russischen Schwarzmarkt auftauchte. Der erste prominente Einsatz fand 2008 in Geogrien statt. 2015 in der Ukraine war die dritte Generation der Schadware aktiv. BlackEnergy baut eine Hintertür in die Netzwerke des Opfers ein. Durch diese sogenannte Backdoor werden über Monate einzelne Teile der Schadware nachgeladen. Sobald alle Teile beisammen sind, können die Angreifer die Kontrolle über das System übernehmen.

19 O-Ton Oleksii Yasinsky
Sprecher 1
Der Täter kann dadurch zum Beispiel aus der Ferne einen Keylogger einschalten. Er kann einen Scanner einschalten und alle Hosts in der befallenen Infrastruktur abscannen. Man kann ihm den Befehl geben, sich zu verstecken, sich ruhig zu stellen und die Backdoor Nachts zu einem bestimmten Zeitpunkt zu öffnen. BlackEnergy besteht aus einzelnen Modulen mit einer Vielzahl von Optionen. Zum Zeitpunkt des Angriffs gab es 17 Module, inzwischen sind es weit mehr.

Atmo Koffer öffnen

Autorin
Vier Männer in schneeweißen Businesshemden, schwarze Anzüge, schicke Schuhe. Nur bei einem blitzen rote Socken auf - das einzige Indiz, dass sie keine gewöhnlichen Berater sind. Die vier erscheinen morgens um acht bei den Stadtwerken Ettlingen.

Atmo Auspacken

20a O-Ton Andreas Salm
Vielen Dank, das wir heute hier sein dürfen.

20b O-Ton Eberhard Oehler
Ja, sehr gerne.

20c O-Ton Andreas Salm
Das das so reibungslos geklappt hat.

Autorin
Eberhard Oehler, Leiter der Stadtwerke, begrüßt die vier. In den nächsten zwei Tagen werden sie die IT-Sicherheit seiner Firma auf die Probe stellen.

21 O-Ton Eberhard Oehler
Dann arbeitet Mal ...

Autorin
Der Test läuft bereits - begonnen hat er mit den präparierten Emails aus Berlin. Andreas Salm prüft, ob seine Mail von gestern geklickt wurde.

22 O-Ton Andreas Salm
Wir haben insgesammt vier Szenarien, die wir angeschrieben haben, in zwei haben wir einen Klick erreicht, und einmal eine Mal eine Dokumentenausführung mit dem integrierten Macro.

Autorin
Vor sechs Jahren wurden die Stadtwerke schon einmal gehackt. Auch damals war es nur ein Test. Eberhard Oehler hat damals öffentlich zugegeben, dass seine Firma angreifbar war. Seitdem versucht er, die Branche auf das Problem aufmerksam zu machen. Regelmässig hält Oehler Vorträge. Heute spricht er vor Studenten des Karlsruher Instituts für Technologie.

23 O-Ton Vortrag Eberhard Oehler
Am ersten Tag, nach 26 Minuten hatte er das Passwort unseres IT-Lieferanten gehackt, weil unser IT-Lieferant eines der Top-Hundert-Passwörter verwendet hat.

Autorin
Ein Hacker namens Felix Lindner führte den Penetrationstest in den Stadtwerken Ettlingen damals durch.

24 O-Ton Vortrag Eberhard Oehler
Ich bin gefragt worden, was passiert wäre, wenn er auf die Enter-Taste gedrückt hätte, und er hatte das 20kV-Schema mit beiden Übergabestationen scharf geschaltet. Hätte Felix auf die Entertaste gedrückt, wären 40 Tausend Menschen in Ettlingen ohne Energie gewesen.

Autorin
Das Bewusstsein, dass daraus entstand, hatte weitreichende Folgen. Die IT-Sicherheit der Stadtwerke wurde komplett überarbeitet.

25 O-Ton Vortrag Eberhard Oehler
Felix hat in einen unserer zentralen Drucker zwischen dem Netzwerkanschluss und der Netzwerksteckdose des Druckers eine mobile Festplatte mit Datenfernübertragung gesteckt.

Autorin
Damals war der Zugang zum Gebäude der Stadtwerke ohne Weiteres möglich. Heute müssen sich die Besucher anmelden. Sie bekommen Besucherausweise und werden von Kameras überwacht.

26 O-Ton Vortrag Eberhard Oehler
Er hat da den Datenverkehr mitgeschrieben, hat diesen Datenverkehr analysiert und aus der Analyse des Datenverkehrs war es ihm möglich, das Passwort unseres IT-Administrators zu hacken, und damit war er in unserer IT.

Autorin
Seitdem erscheint Ettlingen regelmässig in der Presse - als einziges öffentlich bekanntes Beispiel eines erfolgreichen Penetrationstests in Deutschland.

27 O-Ton Vortrag Eberhard Oehler
Allerdings muss man sagen, die Software, die wir einsetzen und dessen Passwort der Felix nach 26 Minuten gehackt hatte, diese Software setzen auch etwa 270 weitere Stadtwerke in Deutschland ein. Und jetzt stellt ihr euch Mal vor, der hackt nicht nur Ettlingen, sondern Bretten, Bruchsal, Baden-Baden, Raststadt, Karlsruhe lassen wir mal außen vor, die haben eine andere Software, und schaltet all diese Kraftwerke mit einem Druck auf die Entertaste ab. Dann passiert eines, dass die Netzfrequenz, und das habe ich hier jetzt mal mit der, mit so einer Waage dargestellt, die Netztfrequenz ist nicht mehr stabil. Beim Abschalten von mehreren Stadtwerken in Nordbaden kommt die Netzwaage ins Ungleichgewicht.

Autorin
Zwischen Juni 2018 und Juni 2019 wurden dem Bundesamt für Sicherheit in der Informationstechnik 252 Angriffe auf kritische Infrastrukturen gemeldet, 29 davon auf den Energiesektor. Das, was Eberhard Oehler im Rahmen eines Tests erlebte, wurde für die ukrainischen Energiekonzerne 2015 einen Tag vor Weihnachten Wirklichkeit.

Musik
Atmo Telefone klingeln.

28 O-Ton Ihor Korolyshin
Sprecher 1
Der Cursor bewegte sich und klickte die Schalter aus. Wir haben es gleichzeitig auf allen Bildschirmen gesehen. Es war surreal.

Autorin
Ein großer Raum, drei Schreibtische vor einer riesigen Wand mit Kacheln. Wir sind in der Dispatcherzentrale des Energiekonzerns «Prykarpattyaoblenergo» in der Westukrainischen Stadt Ivano-Frankivsk. Dispatcher Ihor Korolyshin hat den ersten großen Hackerangriff auf die Energieversorgung der Ukraine am 23. Dezember 2015 miterlebt. Die Hacker knipsten die Schalter der Umspannwerke einen nach dem anderen aus. Es was ein orchestrierter Angriff auf den Energiesektor der Ukraine.

29 O-Ton Ihor Korolyshin
Sprecher 1
Stellen Sie sich vor, man hat die Maus in der Hand, der Cursor gehorcht aber nicht. Er bewegt sich, wie er will, jemand anderer kontrolliert den Cursor.

Atmo Telefone klingeln.

Autorin
Alleine im Gebiet von Iwano-Frankiwsk blieb damals eine viertel Million Menschen am Tag vor Weihnachten über Stunden ohne Strom.

30 O-Ton Ihor Korolyshin
Sprecher 1
Die Dipatcher aus den Bezirken rufen an. Auch ihre Cursor haben sich verselbständigt.

Autorin
Zur gleichen Zeit fanden auch in den Regionen Kyiv und Chernovtsy identische Attacken statt. Auch hier wurden die Computer von Hackern aus der Ferne kontrolliert.

Musik aus

31 O-Ton Volodymir Fedyk
Sprecher 2
Die Dispatcher des zentralen Büros riefen an. Sie sagten, dass massenhaft Verbraucher abgeschaltet würden. Hunderttausende, es war wie eine Lavine.

Autorin
Volodymir Fedyk leitet die IT-Abteilung von Prykarpattyaoblenergo. Die Angreifer waren tief in die Steuerungssoftware der Umspannwerke eingedrungen, und sie kannten sich mit der Software gut aus. Die Dispatcher konnten das auf ihren Bildschirmen beobachten. Dispatcher Korolyshin:

32 O-Ton Ihor Korolyshin
Sprecher 1
Zuletzt haben unsere IT-Menschen den Server abgeschaltet. Die weiteren Klicks hatten dann keine Folgen. Die Angreifer haben das bemerkt, und sind verschwunden. Danach konnten wir die Cursor wieder selbst bewegen. Wir haben angefangen, alle Bezirke manuell einzuspeisen. Die Notdienstbrigaden sind losgefahren und haben alle Schalter per Hand wieder eingeschaltet.

Autorin
Am nächsten Tag gab es dann das Nachspiel. Beim Hochfahren der Rechner zeigte sich, dass viele Festplatten endgültig gelöscht, Domain Controller und Server beschädigt waren.

33 O-Ton Volodymir Fedyk
Sprecher 2
Wir haben nicht sofort verstanden, was passiert. Später haben wir die Technik vom Internet getrennt. So konnten wir einen Teil retten. ... Wie wir erfahren haben, enthielt BlackEnergy ein Modul namens KillDisc. Dieses Modul überschrieb die Daten, und so wurden viele Informationen restlos vernichtet.

Autorin
KillDisc war offensichtlich mit einem Timer versehen. Obwohl die Internetverbindung unterbrochen und die Fernsteuerung deaktiviert worden war, zerstörte KillDisc beim nächsten Hochfahren die Festplatten der Rechner.

34 O-Ton Volodymir Fedyk
Sprecher 2
Wir haben versucht nachzuvollziehen, warum bestimmte Rechner beschädigt wurden, und andere nicht. Rechner mit wichtig klingenden Namen wurden angegriffen. Die Rechner «Boss», «VIP», oder «Buch» waren interessant. Sie wurden vernichtet. Rechner mit weniger wichtigen Namen blieben verschont. Die Angreifer konnten wohl die Strukur des Netzes und die Workstations im Netz sehen.

Da sie Rechner mit «bedeutsamen» Namen ausgesucht haben, war es wohl kein automatisierter Vorgang. Sie haben gezielt nach bedeutsamen Namen gesucht.

Autorin
Die meisten Informationen konnten zwar aus Backups wiederhergestellt werden, aber die Untersuchung wurde durch das Ausradieren der Logfiles massiv erschwert...

Atmo Zug
«Morgen, jemand hier einen Kaffee?» – «Gern» – «Milch, Zucker? Was brauchen Sie dafür?»

Autorin
BlackEnergy bestand 2015 bereits aus 17 einzelnen Modulen. So etwas in seiner Freizeit zu programmieren, gilt als unmöglich. Unter Experten ist es Konsens, dass solche Angriffe von staatlichen Stellen in Auftrag gegeben werden. Staatlich finanzierte Hackergruppen werden Advanced Persistent Threat Groups – kurz APT genannt.

35 O-Ton Marina Krotofil
Sprecherin 1
Typischerweise kann man eine staatlich finanzierte APT-Gruppe daran erkennen, dass die Arbeitszeiten den Bürozeiten ähneln: 9:00 bis 18:00 Uhr. Also wird die Arbeit gegen 8 oder 9 Uhr aufgenommen, und die Aktivitäten fallen nach 17 oder 18 Uhr signifikant ab.

Autorin
Zwar ist es meist unmöglich einzelne APT-Gruppen bestimmten Staaten eindeutig zuzuordnen - trotzdem haben diese Gruppen oft erkennbare Handschriften, oder hinterlassen sogar Hinweise auf ihre Urheberschaft.

36 O-Ton Marina Krotofil
Sprecherin 1
Man kann sich eine APT-Gruppe als ein Projekt vorstellen. Sie haben einen Projektmanager. Finanziert werden sie von einer staatlichen Stelle. Also haben sie ein Management, ein Budget, Bedürfnisse... sie können sich die notwendigen Werkzeuge beschaffen. In verschiedenen Ländern gibt es unterschiedliche Herangehensweisen. In Nordkorea z. B. sind APT-Mitglieder angehalten, ihre Aktivitäten selbst zu finanzieren. Sie übernehmen eine Aufgabe vom Staat, aber sie werden für die Entwicklung der Exploits nicht entlohnt, sondern müssen ihr Geld selbst verdienen. Z. B. in dem sie eine Bank ausrauben und dadurch ihre Operationen finanzieren.

Autorin
Natürlich dürften nur ausländische Banken gehackt werden. Andere Cybersicherheitsexperten erzählen mir, dass auch in anderen totalitären Staaten die Symbiose von Staatssicherheit und Hackern so oder so ähnlich funktioniert.

Atmo Ansage im Zug, niederländisch / Black Hat Sessions, Stimmengewirr

Autorin
Black Hat Sessions, eine Cybersecurity Konferenz in der Nähe von Uttrecht. Das Thema: «Cybersicherheit in den kritischen Infrastrukturen». Der große Vortragsaal ist voll. Das Foyer glänzt in der pink und lila Neonbeleuchtung. Schwarze Wände, von der hohen Decke hängen lila Leuchtkugeln. Marina Krotofil treffe ich nach ihrem Vortrag wieder.

37 O-Ton Marina Krotofil
Internationale Sicherheitsexperten sind sich einig, dass die Ukraine als Übungsgelände für Cyberangriffe diente. Das ist nichts Neues. Im Augenblick macht China das gleiche in Thailand. Genauso, wie Soldaten zu Übungszwecken in echte bewaffnete Konflikte geschickt werden. Auch Cyberkriminelle probieren ihre neueste Schadware zuerst in Firmen oder Ländern mit niedrigeren Sicherheitsstandards aus. Am Ende verwenden alle die gleichen Antivirenprogramme und Firewalls, und so kann man die Schadware verfeinern, ohne entdeckt zu werden. Läuft das Programm zuverlässig, bewegt man sich in die westlichen Länder. Dieses Vorgehen erfüllt mehrere Zwecke: Testen, verfeinern und gleichzeitig die politische Lage destabilisieren.

Autorin
Für die These von der Ukraine als Übungsgelände sprechen die Details des zweiten Angriffs auf den Energiesektor im Jahr 2016.

Musik
Atmo Ortswechsel

38 O-Ton Oleh Zaichenko
Sprecher 2
Nachdem ich die Funktion des Umspannwerks überprüft und den Bericht übermittelt hatte, fing es plötzlich an. Die Schalter begannen völlig planlos, sich abzuschalten. Auch der Eigenbedarf im Umspannwerk ist ausgegangen, also das Licht. Auch bei uns im Umspannwerk ist der Strom ausgegangen.

Autorin
Oleh Zaichenko war in der Nacht auf den 17. Dezember 2016 diensthabender Dispatcher im kyiver Umspannwerk Nord.

39 O-Ton Oleh Zaichenko
Sprecher 2
Die Transit-Leitungen sind durch Relais-Mikroprozessoren geschützt. Ich habe sie überprüft, und festgestellt, dass es keine Notabschaltungen waren. Es konnten nur nicht autorisierte Abschaltungen gewesen sein.

Autorin
Zaichenko rannte raus. Stille. Das typische Knarzen des Magnetfelds fehlte. Es gab tatsächlich keine Spannung.

40 O-Ton Oleh Zaichenko
Sprecher 2
Das war vom System nicht vorgesehen. Ich konnte mechanische Ursachen ausschliessen. Da wurde mir klar, das muss ein Hacker-Angriff sein.

Autorin
Die Hacker haben sich seit dem ersten Angriff vor einem Jahr weiter entwickelt. 2015 bestand der Angriff hauptsächlich darin, in das System des Netzbetreibers einzubrechen und die Kontrolle über die Leitstelle zu übernehmen. Der Angriff 2016 war deutlich ausgefeilter, und verlief komplett automatisiert mit einer Schadware namens «Industroyer». Sie ist die erste bekannte Schadware, die speziell für den Angriff auf Strometze entwickelt wurde. «Industroyer» begann, Leistungsschalter in rascher Folge an und aus zu schalten. Die Techniker vor Ort konnten die Systeme nur retten, indem sie sie vom Netz trennten. Ohne Ingenieurkenntnisse der Leitsystemtechnik wäre die Progammierung von «Industroyer» nicht möglich gewesen. Die Schadware gilt als leicht übertragbar auf Stromnetze in Europa, im Mittleren Osten und in Asien. Mit einer einfachen Erweiterung könnte sie auch in den USA angewendet werden. Auch in diesem Fall begann der Angriff vermutlich mit einem Virus in einer E-Mail.

41 O-Ton Valentin Kaplun
Sprecher 1
Es sah nach einem Hackerangriff aus. Das Monitoring zeigte, dass die technischen Mittel des Umspannwerks «Nord» nicht erreichbar waren. Auf den Rechnern war der blaue Bildschirm eines abgestürzten Windows zu sehen.

Autorin
Der IT-Leiter Valentin Kaplun war fassungslos. Informationen über das neue computergesteuerte Leitsystem von UkrEnergo hatten die Hacker wohl im Internet gefunden. Dass das alte analoge System parallel noch existierte, war nicht öffentlich bekannt. Und zum Glück funktionierte es auch noch. Möglicherweise hat das die Bewohner von Kyiv vor einer Katastrophe bewahrt.

Atmo Ortswechsel

42 O-Ton Manuel Atug
Was sind eigentlich kritische Infrastrukturen? Eine Gesellschaft, die funktioniert nicht ohne Strom, Trinkwasser, Ernährung... Ja auch mit Banken, ohne geht's nicht. Und das ist eben definiert worden als Kritis, als kritische Infrastruktur. Und diese kritischen Infrastrukturen sind eben das Herzstück einer Gesellschaft... Das Problem ist nur - und deswegen greife ich vor - warum defensiv statt offensiv: diese kritischen Infrastrukturen benutzen in der Regel dieselben SCADA Komponenten, dieselben PLC Leitrechner, die haben dieselben Steuersysteme am Start.

Autorin
August 2019. Mildenberg, Brandenburg. Es glänzt, blinkt und blitzt. Hier Techno, da Drum and Base, dort Karaoke. Chaos Communication Camp - CCC Camp. Mehr als 5000 Hacker und Hacksen haben sich versammelt. Frauen wie Männer sind als Einhörner, Katzen oder Eichhörnchen verkleidet. Auf manchen T-Shirts steht «Früher war mehr Hack». Manuel Atug bildet Prüfer aus, die die Betreiber kritischer Infrastrukturen zertifizieren. Beim Chaos Computer Club ist er seit über dreiundzwanzig Jahren aktives Mitglied. Sein Vortrag heißt «Defensive statt Offensive am Beispiel von Kritis»

43 O-Ton Manuel Atug
Es gibt bekannte Hersteller und die werden eben weltweit eingesetzt. Heißt: diese Dinger vernetzen sich immer mehr mit dem Internetz und wollen quatschen, also miteinander dann kommen irgendwelche Sales rum und sagen, mach das übers Internet dran, und dann ist das schick. Und so haben wir eben die ein oder andere Situationen, dass immer mehr von dem Zeug angeschlossen ist, oder eben nicht sauber getrennt ist, anhand von: Office Netzwerk – separat, OT-Produktionsnetzwerk separat. Und dann hast du eben nicht so einen dämlichen Ransomwaretrojaner über eine E-Mail dich da irgendwie angreift.

Autorin
Nach dem Vortrag kommt Manuel Atug von der Bühne. Groß, stämmig, gemächlich. Sogleich bildet sich ein Kreis um ihn. Es wird über die Vorzüge des Preppens und über die Cybersicherheit in kritischen Infrastrukturen diskutiert.

44 O-Ton Manuel Atug
Habe ich genug Wasser, habe ich genug Essen? Es bringt dir nichts, zum Beispiel trockenen Reis zu haben. Den kannst du ja dann nicht aufkochen und essen. Was dir aber was bringt, ist haltbarere Dinge, die du nutzen kannst. Zwei Kilo Zucker, Mehl bringt dir jetzt zum Beispiel auch nicht viel...

45 O-Ton Hacker 1
Kekse...

46 O-Ton Manuel Atug
Ja, du kannst Kekse horten.

Autorin
Manuel Atug erklärt, warum es aus seiner Sicht kaum möglich ist, kritische Infrastrukturen vor Hackern zu sichern.

47 O-Ton Manuel Atug
Kritische Infrastruktur hat halt historische Produkte im Einsatz. Es sind Produktionsstätten, die seit Jahrzehnten im Einsatz sind, noch Jahrzehnte laufen werden. Aus der Definition heraus dieser Produktionsstätten sind sie einfach schon beim Betrieb veraltet. Auch in der IT, und insofern brauchen wir uns da nichts vormachen. Das ist nun Mal unsicher. Es wird mit Maßnahmen drumherum abgeschützt, oder versucht diesen Schutz entsprechen aufzubauen. Aber es ist genauso angreifbar wie alles andere, was IT ist. Pustet man feste dagegen, kann es umkippen. Und das passiert regelmäßig.

Autorin
Die eigene IT ernsthaft zu prüfen und vorhandene Sicherheitslücken zu schliessen, sei teuer. Viele Unternehmen würden daher darauf verzichten. Schliesslich funktioniere ja bislang alles soweit. Andere Hacker plaudern aus dem Nähkästchen.

47a O-Ton Hacker 2
Da wird ja ausdrücklich gesagt, das Gerät nicht scannen, weil, wenn das kaputt ist, dann doof.

48 O-Ton Hacker 3
Wir führen auch Pentests durch, nur wir können uns diese Scheinsicherheit und dieses «können wir nicht die Hälfte der Infrastruktur sicher machen? Weil dann können wir das Projekt kleiner machen.» nicht mehr leisten. Es ist eine Aussage, die ich letzte Woche erhalten habe.

49 O-Ton Manuel Atug
Die haben dann nur die eine Hälfte der IT gesichert und über die andere Hälfte ist die Hoffnung, dass kein Angreifer kommt, ja?

50 O-Ton Hacker 2
Ja genau, die haben halt nur Windows-Domaine gescannt. Der Rest war dann zu kompliziert und zu teuer. Super.

Autorin
Haltet ihr solche Angriffe, wie sie sich in der Ukraine ereigneten auch in Deutschland für möglich?

51 O-Ton Manuel Atug
Also die Steuersysteme, die in der Ukraine betrieben wurden, und im Einsatz sind, sind die selben, die man in den USA, in Frankreich, in Deutschland, oder sonstwo im Einsatz hat. Insofern sind sie durch so einen Angriff genauso angreifbar. Da macht die Schadsoftware nicht Halt an der Grenze. Insofern kann das komplett so realisiert werden, in Deutschland.

Atmo Kyiv

Autorin
Staatliches Zentrum für Cyberverteidigung der Ukraine. Ein großes Gebäude mit getönten Fensterscheiben, von einem schwarzen Gitter umzäunt. Der geräumige Eingangsbereich ist mit zwei Schranken rechts und links gesichert. An den Schranken Soldaten hinter Glasscheiben. Uniformierte laufen vorbei. Pass und Presseausweis werden akribisch kontrolliert. Zwei Männer und eine Frau begleiten mich zu einem kleinen Konferenzraum. Ein großer sportlicher Mann mit dichtem angegrautem Haar kommt dazu. Mykola Khudyntsev, Chef des Zentrums.

52 O-Ton Mykola Khudyntsev
Sprecher 2
Das ist eine militärische Struktur, aber ich bin ein Zivilist. Wir haben auch andere zivile Mitarbeiter, aber die meisten sind Soldaten. Wir sind in erster Linie IT- und Telekommunikationsfachleute, aber die militärische Disziplin hilft uns, unsere Aufgaben zu lösen.

Autorin
Das Zentrum für Cyberverteidigung existiert seit 2015. Es ist als Reaktion auf die sich häufenden Cyberangriffe auf die Ukraine entstanden. Nach dem Sieg des Maidan ging es los. 2014 wurde die Krim von Russland annektiert. Im Osten des Landes begann der Krieg. Gleichzeitig wurde die Infrastruktur der Ukraine mit Cyberangriffen überzogen. Der Energiesekor, Medienunternehmen, der Kyiver Flughafen, der Rentenfond, das Finanzministerium, die Bahn und das Ministerium für Infrastruktur wurden gehackt.

53 O-Ton Mykola Khudyntsev
Sprecher 2
Nach der Analyse der Schadcodes kann man sagen, dass hinter den Cyberangriffen der Jahre 2014, 2015 und 2016 die gleichen Gruppen stehen. Das stimmt auch mit den Einschätzungen unserer Staatssicherheit überein. Die Handschrift der Codes deutet daraufhin. Zweifelsohne steht hinter diesen Angriffen unser nördlicher Nachbar, der heute leider unser Gegner ist. Auch wenn man das alles nicht beweisen kann... so wie wir nicht Mal die Anwesenheit des russischen Militärs im Donbass vollständig beweisen können... es ist augenscheinlich, aber juristisch beweisen können wir es nicht. Es gibt nur indirekte Beweise.

Atmo Berlin

Autorin
Die Angreifer verwenden fremde Infrastruktur, sie können ihre Spuren im Netz weitgehend verschleiern, oder sogar falsche Spuren auslegen. Die Zuordnung einer Attacke, die sogenannte Attribution, wird dadurch sehr schwer.

54 O-Ton Sven Herpig
Eine der besten Attributionen kann ich natürlich vornehmen, wenn ich in den Netzwerken der Gegner schon drin bin, und dort live nachverfolgen kann, wie ein Angriff stattfindet.

Autorin
Sven Herpig ist Projektleiter für Internationale Cyber-Sicherheitspolitik bei der Stiftung Neue Verantwortung.

55 O-Ton Sven Herpig
Das war z.B., sagt man so, bei russischen Aktivitäten gegen die USA, wo die niederländischen Geheimdienste bereits drinnen waren. Oder beim Angriff auf Sony Pictures Entertainment aus Nordkorea, wo es heißt, dass die amerikanischen Geheimdienste bereits in den nordkoreanischen Netzwerken waren, und diesen Angriff dann auch mitverfolgen konnten, und sich deswegen so sicher waren.

Autorin
In fremde Netze einzudringen, und sie zu unterwandern - das wäre auch die Voraussetzung für einen gezielten Gegenschlag. Nach dem Cyberangriff auf den Bundestag 2015 und dem Cyberangriff auf das Auswärtige Amt 2018 wird auch in Deutschland darüber diskutiert. Bundesinnenminister Horst Seehofer Mitte Mai 2019.

56 O-Ton Horst Seehofer
Unsere Sicherheitsbehörden müssen die rechtlichen und technischen Instrumente haben, um politisch motivierte Kriminalität wirkungsvoll zu bekämpfen. Auch im Bereich der Cybersicherheit, wo wir noch zwei große Projekte als Bundesregierung und Parlament zu stemmen haben: die aktive Cyberabwehr und das Internetsicherheitsgesetz 2.0.

Autorin
"Aktive Cyberabwehr" ist der Begriff der Regierung. Kritiker sprechen vom "Hackback". Wobei das Innenministerium bestreitet, Angriffe auf kritische Infrastruktur anderer Länder zu planen. Es gehe immer nur um Gefahrenabwehr.

57 O-Ton Sven Herpig
Deutschland hält sich bisher im Cyberraum weitaus defensiver - soweit wir wissen - als andere Länder, wie z. B. Beispiel die Vereinigten Staaten, Israel, die Britten, aber auch China oder Russland. Das hat bisher auch die Gründe, dass wir zwar eine rechtliche Grundlage haben, nämlich die rechtliche Grundlage aus dem generellen Einsatz des Militärs auch weiterhin vorliegt. Das heißt im Verteidigungsfall und im Spannungsfall, so wie bei mandatierten Auslandsmissionen, und beim Schutz der eigenen IT Systeme darf die Bundeswehr eben aktiv werden. In anderen Fällen nicht, lässt sich das auch so in den Cyberraum übersetzen, glaube ich. Von daher haben wir bisher eine relativ defensive Position gefahren, mit der wir auch meines Erachtens auch sehr gut gefahren sind.

Atmo Ortswechsel Bonn

58 O-Ton Brigadegeneral Peter Richert
Ich glaube, die Situation heute ist gekennzeichnet durch die hybriden Szenarien in denen Cyber, wie gesagt, bloß nur einen Aspekt darstellt. Daneben kommen diese ganzen Maßnahmen im Informationsumfeld, Fake News, Propaganda etc., und das ist auch der Grund warum vor zwei Jahren dieser Organisationsbereich Cyber- und Informationsraum gegründet wurde um diese ganzen Elemente unter einem Dach zusammenzufahren, um gegenseitige Abhängigkeiten zu erkennen, und um möglicherweise Anomalien zu erkennen, um frühzeitig auch ein Lagebild, ein umfassendes Lagebild zu diesem Thema zu erarbeiten.

Autorin
Ein großer weißer Gebäudekomplex, Glasfassade, schwarze Gitter. Das Kommando Cyber- und Informationsraum mit Sitz in Bonn wurde am 1. April 2017 gegründet. Das Kommando besteht aus 24 Dienststellen. Die Abteilung Einsatz wird von Brigadegeneral Richert geleitet. Er empfängt mich in seinem Büro. Ein ausladender Arbeitstisch mit Computer, ein runder Tisch, fünf Stühle. Wasser, Kaffee und Kekse.

59 O-Ton General Brigadegeneral Peter Richert
Das Kommando Cyber- und Informationsraum verfügt natürlich auch über offensive Wirkmöglichkein. Offensive Wirkmittel sind im Prinzip Softwarewerkzeuge, mit denen ich in der Lage bin, eine militärische Wirkung zu erzeugen, indem ich gegnerische IT-Systeme beeinträchtige und in ihrer Funktionsfähigkeit vermindere. Der große Vorteil dieser Cyberwirkmittel ist nach unserer Bewertung der, dass ich damit herkömmliche kinetische Wirkmittel, also das was durch Heer, Luftwaffe, Marine kinetisch gemacht werden kann, entsprechend subsituieren kann. Offensive Maßnahmen, wie sie es nannten «hacken», unterliegen immer einer Einzelfallentscheidung im Rahmen eines politischen Mandates und können dann entsprechend detailliert betrachtet werden.

Autorin
Doch wie würde die Bundeswehr reagieren, sollten die deutschen Stromnetze von anderen Staaten aus angegriffen werden? In welchen Fällen könnten die offensiven Wirkmittel tatsächlich eingesetzt werden?

60 O-Ton General Brigadegeneral Peter Richert
Der Einsatz offensiver Cyberwirkmittel unterliegt den gleichen Bestimmungen, die es für jedes Wirkmittel in den Streikräften gilt: Heer, Luftwaffe und Marine. Das heißt, es ist klar zu prüfen, wo ein entsprechender Angreifer ist, und nur wenn ein Ziel eindeutig identifiziert ist, darf es auch entsprechend angegriffen werden. Im Bezug auf die Attribution im Cyberraum ist das mit Sicherheit ein etwas schwieriges Unternehmen. Gleichwohl gibt es Möglichkeiten, mit einer entsprechenden Aufklärung und dem entsprechenden Zeiteinsatz auch hier Rückschlüsse ziehen zu können. Und nur wenn ein Ziel eindeutig feststeht, nur dann sind auch entsprechende Wirkmittel erlaubt einzusetzen.

Autorin
Genau hier setzen die Kritiker der offensiven Maßnahmen an. Man muss die fremden Netze bereits im Vorfeld infiltriert haben und den Angriff tatsächlich «life» miterleben, um den Angreifer eindeutig identifizieren zu können. Im Nachhinein ist das nahezu unmöglich. In Deutschland soll die Infiltration fremder Netze künftig offenbar in den Aufgabenbereich der Nachrichtendienste fallen, insbesondere des Bundesnachrichtendienstes.

61 O-Ton Sven Herpig
Wir wissen, dass unser Bundesnachrichtendienst ein Programm hat, was Strategic Cyber Defence in ausländischen Netzen macht. Das heißt, die haben ich glaub 250 Millionen irgendwann bekommen, dafür, dass sie in ausländischen Netzen die IT Sicherheit für Deutschland herstellen, was auch immer das heißen mag.

Autorin
Dass der BND die Zuständigkeit gerne hätte, wird mir hinter vorgehaltener Hand von mehreren Seiten bestätigt. Offiziell äußert sich der BND dazu nicht.

Atmo Ortswechsel

Autorin
Betritt man das Gebäude der Stadtwerke Ettlingen, steht man in einer tropischen Welt. Grüne Landschaft, Kois im Teich. Linker Hand geht es zu den Büros. Das Hackerteam hat einen Blick auf den Teich und die immergrünen Bäume.

62 O-Ton Andreas Salm
Wir waren bis jetzt auf der Suche nach direkten Zugriffsmöglichkeiten aus der Business-IT in die SCADA-Umgebung. Es hat sich jetzt nach weiteren Analysen gezeigt, dass es nur eine überschaubare Anzahl von Schnittstellen gibt. Und diese Schnittstellen haben wir uns jetzt natürlich näher angesehen und überprüft, ob es da nicht Schwachpunkte gibt, die uns den Zugang ermöglichen.

Autorin
Im eigentlichen Pen-Test geht es also nun darum, den Schritt von der Officeumgebung der Verwaltung, die mit dem Internet verbundenen ist, in die nicht direkt von außen erreichbare technische Leitstelle des Stromnetzes zu machen – die sogenannte SCADA-Umgebung. Andreas Salm und seine Kollegen prüfen nicht nur Schwachstellen im Netzwerk und in der Software, sie schauen sich auch im Gebäude um. Und davor.

63 O-Ton Andreas Salm
Man kommt hier aufs Gelände, dahinten ist die Türe offen. Hier kommt man direkt rein. Selbst wenn vorne jemand säße und die Türe wäre zu, diese ist ja offen... Ich würde jetzt gerne im Lagerbereich gucken, ob man nicht eine Netzdose findet. Einen Wlan Access Point oder irgendwas in der Art. Netzwerkkabel. Das ist wahrscheinlich hier unten für die Büros die Verkabelung? Das heißt hier, wenn man sich zwischen schalten würde... Also hier könnte man reinkommen. Das ist also kritisch, wenn man hier rankommen kann, und wenn die Verbindung nicht verschlüsselt ist, was sie wahrscheinlich nicht ist, weil internes Netztwerk, wäre man also in dem Fall direkt im Netzwerk... also da hinten habe ich auch schon ein Kabel gesehen...

Autorin
Wir laufen weiter durch die Gänge der Stadtwerke und landen irgendwann neben einem Drucker. Andreas Salm sucht nach ungesicherten Netzwerkdosen. Alle Dosen sind deaktiviert, bis auf die eine, an die der Multifunktionsdrucker angeschlossen ist. Salm zieht das Lankabel aus der Netzwerkdose und schließt seinen Laptop daran.

65 O-Ton Andreas Salm
Wir sehen eine Status-LED, wir haben einen Netzwerkzugang. Das gibt mir natürlich Einblick in das Netzwerk. Ich sehe hier natürlich sofort, welche IP-Adressen werden verwendet, und könnte jetzt auch direkt mir so eine IP-Adresse nehmen und in das Netzwerk eingreifen. Jetzt sieht man aber auch, dass keine weiteren Pakete mehr kommen.

Autorin
Nach knapp 20 Sekunden hat das System erkannt, dass der Nutzer, der sich anstelle des Druckers eingeklinkt hat, nicht autorisiert ist. Der Nutzer wird ausgesperrt. Doch diese 20 Sekunden können eintscheidend sein.

66 O-Ton Andreas Salm
Wenn hier ein Virus drauf wäre, der automatisch sich weiter verbreiten kann, kann das unter Umständen schon reichen, das der in das Netzwerk rein kommt. Muss nicht. Könnte.

Musik

Autorin
Man kann sich das Internet als Straße vorstellen. Man kann durch die Straße laufen und an Fenstern und Türen rütteln. Manche Türen sind verschlossen, andere stehen offen. Offene Türen laden zum Diebstahl ein. Es kommt auch vor, das eine Tür falsch montiert wurde. Entdeckt man so einen Fehler, ist es eine Schwachstelle. Findet man einen Weg, den Montagefehler zum Öffnen der Tür zu nutzen, so wird das als Exploit bezeichnet. Wird der Bauherr über den Fehler informiert, und entwickelt daraufhin eine Abdichtung, wäre das ein Patch. Wird das Wissen über den Fehler weder dem Hausbewohner, noch dem Bauherrn mitgeteilt, hat man eine Zero-Day-Schwachstelle. "Zero Day" - "null Tage", weil der Bauherr "null Tage" Zeit hat, um sich gegen einen Einbruch zu wehren, indem er den Fehler behebt - er weiss ja nichts davon. Und was, wenn ganz viele Türen offen oder fehlerhaft montiert sind? Und was, wenn der Entdecker des Fehlers weder den Bauherrn noch den Besitzer informiert, sondern sein Wissen an Einbrecher verkauft? Oder an einen Staat, der

seine Bürger kontrollieren will, und nun einfach unbemerkt vorbeischauen kann? Genauso sieht es auf dem Markt der Schwachstellen aus. Es gibt Researcher, die danach suchen. Sie entscheiden, ob sie diese Schwachstellen an die Hersteller melden, oder sie für gutes Geld verkaufen - auf speziell dafür geschaffenen Plattformen.

77 O-Ton Manuel Atug
Die Abnehmer sind staatliche Akteure, aber auch Militär oder Geheimdienste, Nachrichtendienste oder sogar kriminelle Banden, die eben sagen, ich möchte mit einer Ramsomeware beliebige Leute erpressen, weil ich deren Systeme verschlüssele, und sie müssen mir per Bitcoin auszahlen. Die können das genauso kaufen, wie jeder andere.

Autorin
Doch oft ist es nicht einmal nötig, neue Schwachstellen und Exploits zu verwenden, um in fremde Systeme einzudringen. Denn häufig werden bereits bekannte Schwachstellen einfach nicht gepacht, oder die Nutzer spielen Updates zu spät auf, z. B. weil es lästig ist, und die Systeme ja auch ohne Update funktionieren. Manuel Atug weiß aus Erfahrung: Viele Produktionssysteme werden über Jahrzehnte gar nicht upgedatet.

78 O-Ton Manuel Atug
Hat man ja auch selber schon zu Hause gesehen, ob ich Linux, einen Windows oder einen Mac, oder was auch immer habe, ein Handy. Jedes Update ist... ich hoffe dass er danach noch läuft, so. Und diese Hoffnung ist ja nicht nur bei uns zu Hause. Diese Hoffnung haben auch kritische Infrastruktur-Betreiber. Aber wenn ich eine kritische Infrastruktur betreibe, dann sage ich nicht, naja, dann mache ich halt ein Update, und wenn 's kaputt ist, dann tausche ich es aus. Also wenn ich halt ein Kraftwerk habe, kann ich nicht einfach sagen, ja dann mache ich ein Update an den kritischen Komponenten und wenn es kaputt ist, dann fahren wir kurz das Kraftwerk, runter tauschen das Bauteil aus und dann fahren wir es wieder hoch. Also so funktioniert das in der dauerverfügbaren Versorgungsleistung nicht. Und dann überlegen die natürlich dreimal, ob die das Updaten. Und dann geht das so über 10, 15, 20 Jahre. Und dann hat man eine sehr obskure Historie, die dazu führt dass viele Altlasten betrieben werden, die halt nicht mehr up-to-date sind. Aber, dann kommt im Gegenzug: ist das noch sicher betreibbar? Und dann wird's kompliziert.

Autorin
Eine Lösung, die Cybersicherheit langfristig zu erhöhen, wäre das "sichere Programmieren". Doch das steht weder in Deutschland noch weltweit auf den Stundenplänen der Programmierer.

79 O-Ton Manuel Atug
Also wenn ich ein Auto fahren will, mache ich den Führerschein. Dann lerne ich auch viel über Safety. Wenn ich programmieren will, brauche ich noch nicht mal ein Studium. Ich kann einfach einen Quellcode schreiben, und der ist da. Da gibt's keine Zulassungsvoraussetzungen.

Autorin
Solche Voraussetzungen wären ein erster Schritt in Richtung Cybersicherheit.

80 O-Ton Manuel Atug
Alle müssen Richtung sichere Entwicklung von Software gehen. Und alle müssen diese Schwelle einfach höher setzen. Wenn man es nicht beigebracht bekommt, entwickelt man ja auf Funktion hinaus, nicht auf sichere Funktion hinaus. Also man entwickelt eine Funktion, man testet die und die klappt. Und dann sagt man, ja, Super! War ja das erwartete Ergebnis. Das jemand das anders verwendet und das dann vielleicht irgendwie kaputt geht, oder Fehlverhalten erzeugt, wird ja nicht gegengeprüft. Dieser umgekehrte Test: funktioniert auch nur das Gewünschte und nichts anderes? Der bleibt oft aus. Das ist aber der Security-Test, den man sozusagen machen muss. Und dieses vom Entwickeln her und von Testen her wird das oft nicht gemacht. Weil es einfach nicht klar ist, oder nicht geschult wurde.

Atmo Ortswechsel

81 O-Ton Frau
Hallo...

82 O-Ton Andreas Salm
Wir haben telefoniert. Sie erinnern sich? Ich habe die Mail gesendet. Das war keine ernsthafte Anfrage, sondern es war der Versuch ihnen ein Dokument unterzujubeln, in der Hoffnung, dass sie das öffnen würden. Genau.

83 O-Ton Frau
Sauber.

84 O-Ton Andreas Salm
Wir wollten einfach Mal gucken, wie es denn aussieht, wenn man von außen käme und ein Dokument präparieren würde, ein Szenario gestalten würde...

85 O-Ton Frau
Drum habe ich das Ding gar nicht aufmachen können...

86 O-Ton Andreas Salm
... dass irgendjemand dazu bewegt das Dokument dann zu öffnen... Da ist kein Schadprogramm drin, keine Sorge. Aber da wäre eine Rückmeldung gekommen: Das Dokument wurde geöffnet. Das hätte auch ein Virus sein können und es hätte in die Systemumgebung kommen können.

Autorin
Vor zwei Tagen hatte Andreas Salm die Test-E-Mail verschickt. Und jetzt ist er vor Ort, um sich für die Unannehmlichkeiten zu entschuldigen und über das Täuschungsmanöver aufzuklären.

87 O-Ton Frau
Wir sind ja insgesamt sowieso sehr vorsichtig. Ich versichere mich oft zurück, dass wenn da ein Absender ist, den ich nicht erkennen kann, noch mal nachzufragen in der IT-Sicherheit. Das mache ich eigentlich immer. Aber jetzt bei dem Anruf und dem, dass mir jemand was schickt und es eigentlich ja verabredet war, dass ich was bekomme, bin ich jetzt nicht davon ausgegangen, und mich macht es jetzt schon etwas sprachlos, dass ich jetzt reingelegt worden bin.

88 O-Tom Andreas Salm
Aber es zeigt halt auch wie leicht man doch, auch wenn man sicherheitsbewusst ist und die Risiken kennt, dann doch reingelegt werden kann. Und mit dem muss man halt einfach immer rechnen.

Autorin
Was man auf keinen Fall machen sollte, ist Warnhinweise einfach wegzuklicken, wenn man Anlagen öffnet oder Dateien lädt - selbst wenn die E-Mail von einem bekannten Kontakt stammt.

Atmo Ortswechsel

Autorin
Die Männer in den schneeweißen Hemden packen Ihre Sachen. In den zwei Tagen in Ettlingen konnten sie nachweisen, dass es Wege gibt, sich unbefugt im Firmennetz einzunisten. Sie haben einen Katalog mit Schwachstellen zusammengestellt. Der Sprung aus der Office-IT in die Leitstelle der Stadtwerke ist ihnen jedoch nicht gelungen. Eberhard Oehler:

89 O-Ton Eberhard Oehler
Ich habe noch kein endgültiges Ergebnis, was ich allerdings jetzt aus den ersten Gesprächen mit den Leuten von HiSolutions erfahren habe, gibt mir Hinweise, dass es deutlich schwieriger geworden ist, im Vergleich zu dem Angriff aus dem Jahr 2013. Das ist zum einen ein Hinweis, dass wir bei den Stadtwerken Ettlingen was Cybersicherheit anbelangt auf dem richtigen Weg sind, zeigt aber auch, weil gleichwohl haben sie Erfolg, zumindest partiellen Erfolg, dass wir keinen Grund haben, locker zu lassen.

Musik

Autorin
Nicht immer bleiben Angriffe auf ein Unternehmen oder ein System beschränkt. Der bislang größte Cyberangriff in der Geschichte war "Notpetya". Er heißt so, weil die verwendete Schadware erst einmal aussah wie eine bekannte Ransomware namens "Petya", mit der Hacker Festplatten verschlüsseln und gegen Lösegeld wieder freigeben. Bei "Notpetya" gab es keinen Schlüssel, die Festplatten wurden zerstört. Der Troyaner traf internationale Konzerne wie die Reederei Maersk, den Lebensmittelhersteller Mondelez, den Pharmakonzern Merck, den Logistik-Dienstleister Fedex, den Haushaltswarenhersteller Reckitt Benckiser und viele andere. Der Schaden wird auf 10 Milliarden Euro geschätzt. Und auch dieser Cyberangriff richtete sich zunächst gegen ukrainische Unternehmen.

Atmo Ortswechsel

90 O-Ton Olessia Linnik
Sprecherin 2
Bevor ich ins Flugzeug stieg, wurde mir mitgeteilt, dass wir attakiert werden. Die Computer im Büro verschlüsselten sich einer nach dem anderen. Und nicht nur bei uns. In der ganzen Ukraine herrschte Panik und Hysterie. Ich musste dann einsteigen und das Handy ausschalten.

Autorin
Olessia Linnik ist Geschäftsfrau. Ihre Firma vertreibt die Buchhaltungssoftware M.E.Doc zu deutsch «Honig». Am 27. Juni 2017 ist sie auf dem Heimweg von einer Dienstreise. Der Flug dauert eine Stunde und vierzig Minuten. In dieser Zeit entwickelt sich die Situation in der Ukraine zu einem Desaster. Computer im ganzen Land fallen nach und nach aus.

91 O-Ton Olessia Linnik
Sprecherin 2
Die Bankautomaten funktionieren nicht mehr, Menschen können nicht mehr mit der Karte zahlen – im Laden oder an der Tankstelle. Ein Kollaps. Ich rufe im Büro an. Wir überlegen, was wir tun können, wie wir unsere Arbeit wieder aufnehmen können. Ob wir versuchen können, die Rechner neu zu installieren.

Autorin
Ministerien, Banken, Anzeigetafeln von den Flughäfen, die U-Bahn, die Telekom, die Post und die Bahn sind betroffen. Das Strahlungsmonitoringsystem des Atomkraftwerks Tschernobyl kann nur noch manuell gefahren werden. Auf dem Weg ins Büro liest Olessia Linnik, dass ihre Firma für die Verbreitung der Schadware verantwortlich gemacht wird, die den Kollaps ausgelöst hat.

92 O-Ton Olessia Linnik
Sprecherin 2
Mein erster Gedanke war: das könnte die Konkurrenz sein. Oder eine Kampagne gegen unser Produkt.

Autorin
Doch ihre Software wurde von Hackern missbraucht, um eine Attacke auf die Wirtschaft des Landes zu starten. Die Buchhaltungssoftware war als Wirt für das Virus bestens geeignet - sie war im ganzen Land verbreitet. Für die ukrainische Cyberpolizei aber sah es zunächst so aus, als würde der Angriff von den Entwicklern der Buchhaltungssoftware ausgehen.

93 O-Ton Olessia Linnik
Sprecherin 2
Am Tag des Angriffs um zwölf Uhr Mittags versuchten Cyberkriminelle, von litauischen IP-Adressen aus in unsere Website einzudringen. Dann schalteten sie eine Umleitung auf französische Server. Diese Umleitung blieb zwei Stunden aktiv, dann wurde sie wieder abgeschaltet. Unsere Website arbeitete wieder ganz normal.

Autorin
In der Zwischenzeit haben die Angreifer ihr Virus über ein reguläres Update der Buchhaltungssoftware im ganzen Land verbreitet. Alle Rechner, die das Update bekommen haben, sind befallen. Auch die Niederlassungen internationaler Firmen sind betroffen. So kann sich die Attacke über deren Netzwerke weit über die Grenzen der Ukraine hinaus verbreiten. Der IT-Sicherheitsexperte Oleksii Yasinsky:

94 O-Ton Oleksii Yasinsky
Sprecher 1
Die Ukraine ist in diesem Fall nicht nur ein Testgelände, sondern womöglich auch eine Backdoor geworden. Es gibt viele Niederlassungen in der Ukraine, die mit ihren

Mutterkonzernen eine Verbindung haben. Deswegen hatte diese Attacke womöglich das Ziel, einen Zugang zu anderen Organisationen zu bekommen.

Musik

Autorin
Bis heute ist unklar, ob die weltweite Ausbreitung gezielt geplant, oder ein Unfall war. NotPetya hat fast alle Spuren durch das Löschen der Festplatten verwischt. Untersuchungen der Attacke deuten darauf hin, dass dieselbe ATP-Gruppe am Werk war, wie bei den Angriffen auf die Stromversorgung der Ukraine. Gerichtsfest beweisen lässt sich das nicht. Oder doch? Anfang 2019 hat der Mondelez-Konzern, eines der Opfer der NotPetya-Attacke, die Zurich-Versicherung in den USA verklagt. Die Versicherung betrachtet den Angriff als Kollateralschaden einer kriegsähnlichen Handlung, und weigert sich deshalb den Schaden zu ersetzen. Im Gerichtssaal in Chicago wollen Zurichs Anwälte beweisen, dass tatsächlich Russlands Staatshacker hinter NotPetya stecken.

Sprecher 2
Absage
Blackout um 0:00 Uhr - Die Ukraine als Testgelände für den Cyberkrieg.
Ein Feature von Inga Lizengevic.
Es sprachen: Nagmeh Alaei, Lisa Bihl, Kerstin Fischer, Andreas Potulski und Bruno Winzen.
Ton und Technik: Wolfgang Rixius und Roman Weingardt
Regie: die Autorin
Redaktion: Wolfgang Schiller
Eine Produktion des Deutschlandfunks mit dem Südwestrundfunk 2019