Deutschlandradio Kultur

Manuskript

Kultur und Gesellschaft

Kostenträger :	P 62100
Organisationseinheit:	46
Reihe :	**Forschung und Gesellschaft**
Titel :	**Cyberwar** Computernetze als Schlachtfelder der Zukunft?
Autor/in :	Philip Banse
Redakteur/in :	Jana Wuttke
Sendung :	20.01.2011
Regie :	Beate Ziegs
Ton:	Martin Eichberg
Besetzung :	Ilka Teichmüller, Gerd Grasse

Funkhaus Berlin
Hans-Rosenthal-Platz
10825 Berlin
Telefon (030) 8503-0

ATMO
(NATO-Film über Estland) Wind, Musik, Cyberklänge

OTON (Englisch)
Die Menschen in Estland empfanden das als Bedrohung der nationalen Sicherheit, als Bedrohung für alle. Die Spannung war groß, die Leute wollten mehr wissen, gingen online, wollten Nachrichten-Sites aufrufen – aber das ging nicht. Dann wollten sie Online-Banking machen, aber auch das Bankensystem war down. Es gab eine ziemlich emotionale Reaktion. Die Leute dachten, da stimmt was nicht, einige fürchteten, die Regierung sei abgesetzt.

Sprecherin
Jaak Aviksoo, Estnischer Verteidigungsminister, in einem offiziellen Film der NATO über den angeblich bis dahin größten Cyberangriff.

Autor
Tallin am Morgen des 27. April 2007. Die estnische Regierung plant, ein Ehrenmal aus dem Zentrum der Hauptstadt Tallin entfernen zu lassen, das Denkmal erinnert an russische Soldaten. Estnische Russen protestieren, es kommt zu gewalttätigen Ausschreitungen in der estnischen Hauptstadt. Die Proteste werden begleitet von Angriffen über das Internet. Webseiten estnischer Banken sind nicht mehr abrufbar; auch die Netzauftritte von Polizei und Regierung gehen offline. Die landesweite Notrufnummer funktioniert nicht mehr.

Sprecherin
In dem NATO-Film erklärt Ian West, Direktor von NATOS Computer Incident Response Capability Technical Center:

OTON
Unsere Versorgungssysteme wie Gas, Wasser und Strom, unsere Flugsysteme, die Verteidigungssysteme und natürlich die Geldwirtschaft – sie alle sind abhängig von Computernetzwerken. Schaltet man diese Netzwerke ab, kann der der Effekt verheerend sein.

Autor
Das Internet ist zu einem Teil unseres Lebens geworden. Wir lesen in ihm, reden, chatten, kaufen, beichten, lernen und arbeiten im Internet. Immer mehr Menschen, aber auch

Maschinen werden mit Datenleitungen vernetzt: Mobiltelefone, Fernseher, Stromgeneratoren, Panzer, Einspritzdüsen in Chemiewerken. Die Vernetzung birgt Chancen. Und Risiken.

Autor
Das Internet wurde für illegale Aktionen genutzt, solange es existiert: Karl Koch brach Mitte der Achtziger Jahre in Rechner des US-Militärs ein und verkaufte die Daten an den KGB; Kreditkarten werden geklaut, geheime Wirtschaftsdaten entwendet. Die Zahl der Angriffe ist schwer zu messen, vieles deutet darauf hin, dass es mehr werden. US-Militärs warnen seit Jahren vor einem „elektronischen Pearl Harbor" oder einem "digitalen 11. September". Deutschland will ein Cyberabwehrzentrum errichten, ein gemeinsamer Spähposten mit Polizei und Geheimdiensten. Denn die Zahl der Attacken auf deutsche Regierungsnetze habe ich im vergangenen Jahr verdoppelt, sagt ein Sprecher des Innenministeriums.

15 OTON
Es geht bei solchen Angriffen um das Abziehen von Know How, von regierungsinternem Wissen, es geht um das Abgreifen von Wirtschaftswissen, von Strukturkenntnissen: Wie ist Deutschland auf bestimmte Situationen vorbereitet? Das ist ein ziemlich bunter Strauß. Das Interesse ist sehr groß und sehr mannigfaltig – was die Zahlen ja auch belegen.

OTON
(Collage aus TV-Tönen) Nun gibt es eine Art Cyberwar / Cyberkrieg ist kein Thema mehr für Science Fiction Filme allein / The cyber war threat has been grossly exagurated … *(darauf)*

Sprecherin
Nicht jeder Angriff über das Internet ist ein Cyberwar, ein Krieg, warnt der Autor, Programmierer und Experte für Computersicherheit Bruce Schneier in der CBS-Show Intelligence Squared:

OTON (Englisch)
Metaphern sind wichtig. Wenn wir über „Krieg“ sprechen, dann ruft man das Militär und wir bekommen militärische Lösungen: Sie haben einen Feind, der muss besiegt werden. Wenn man über diese Bedrohungen als Kriminalität, bekommen wir polizeiliche Lösungen. Wie wir über das Thema reden, wie die Schlagzeilen aussehen, bestimmen, welche Lösungen wir bekommen.

OTON
Wir reden über Cyber Crime, Cyber Warfare, Cyber Espionage und am Ende präventiv Cyber Security.

Sprecher
Udo Helmbrecht, Direktor der ENISA, der Europäischen Agentur für Netzwerk- und Informationssicherheit, einer EU-Einrichtung, die sich vor allem um die Sicherheit des europäischen Internets kümmert. Kriminalität, Krieg, Spionage und Sicherheit - welcher Angriff aber in welche Kategorie gehört, sei aber nicht immer einfach fest zu stellen:

OTON
Wir haben heute die Herausforderung, dass wir, wenn wir Angriffe haben, die gleich Technologie sehen und nicht auf den ersten Blick wissen, ist das nun ein Krimineller, der damit Geld verdienen will, ist das Spionage oder ist das im Sinne asymmetrischer Kriegsführung ein Angriff. Und nur mit Sicherheitsbehörden und Geheimdiensten kann man letztlich herausfinden, wo der Angriff herkommt in solchen Fällen.

Autor
Und wenn die Urheber vergangener Cyberangriffe ausgemacht werden konnten – dass Staaten dahinter steckten, konnte selten bewiesen werden.

OTON
We can´t tell foreign invaders from bored Kids.

Autor
„Wir können ausländische Invasoren nicht mehr unterscheiden von gelangweilten Kindern“, sagt der Hacker Bruce Schneier. So war es beim angeblich ersten Cyberwar in Estland. Die Regierung beschuldigte Russland, die Netzattacke initiiert zu haben, Russland stritt ab. Beschuldigt wurde letztlich ein 22jähriger Russe aus Tallin, der für ein Mahnmal protestierte.

Sprecherin
Ein ähnliches Bild in Georgien, Sommer 2008.

ATMO

(Krieg in Georgien)

Autor

Russland und Georgien führen Krieg um Südossetien. Angreifer legen über das Internet die Server der georgischen Regierung lahm, Webseiten des Präsidenten werden gehackt und verändert. Die US Cyber Consequences Unit, ein nach eigenen Angaben unabhängiges Institut zur Erforschung von Cyberattacken, untersuchte den Fall und kam zu dem Schluss:

Sprecherin

"Die Angreifer und ihre Aktionen sind allem Anschein nach zivilen Ursprungs."

Autor

Zivile Angreifer steckten auch hinter den Attacken auf die Webseiten von Paypal, Mastercard und Visa im Herbst letzten Jahres.

OTON (Englisch)

Anonymus hat Seiten angegriffen, die nicht mehr mit Wikileaks zusammen arbeiten wollen.

Sprecherin

Sagt ein 22jähriger Mann namens Coldblood der BBC. Er sei ein Sprecher von Anonymus, so der junge Mann, einer schwer zu fassenden Spaß-Guerilla im Netz.

OTON (Englisch)

Anonymus verfolgt keine konventionellen Ziele. Ideen wabern umher. Ist eine gut, wird sie umgesetzt.

Autor

Estland, Georgien, Anonymus – diese und ungezählte weitere Angriffe bedienten sich der gleichen simpeln Technik: Distributed Denial of Service Attacken, kurz DDos. Tausende Computer rufen gleichzeitig eine Webseite auf, mehrmals in der Sekunde. Der Server ist dafür nicht ausgelegt und bricht zusammen. Die Angriffsrechner wurden oft mit einem Virus infiziert und sind nun fernsteuerbar. Die Besitzer wissen nicht, dass Ihr Rechner für einen Angriff missbraucht wird und auf Befehle aus der Ferne wartet, um Webseiten anzugreifen.

OTON (Englisch)
Das sind sehr effektive, aber auch sehr primitive Angriffe. Solche DDos-Attacken sind die die Speere des Internet-Zeitalters.

Sprecherin
Toomas Hendrik Ilves, Staatspräsident von Estland.

OTON (Englisch)
Die wahren Bedrohungen sind weitaus komplexer und erfordern ganz neue Verteidigungsstrategien.

Autor
Im Sommer 2010 lernte die Welt eine ganz neue Art Cyberwaffe kenn, die mit den grobschlächtigen Netzattacken der Vergangenheit nichts mehr zu tun hat.

OTON
Trailer-Musik von ZDF heute

OTON
(Moderation) Die Computer-Attacke auf Industrieanlagen im Iran ließ an Wochenende aufhorchen. Der Computerwurm Stuxnet hatte zehntausende Geräte gefallen – auch die im Atomkraftwerk Busher, das demnächst ja ans Netz gehen soll.

05a OTON
Stuxnet ist interessant, weil es eine ganze Reihe von Hypothesen beweist, die wir schon länger hatten über die Gestalt von Cyberwar, eben, dass es sehr hoch entwickelte Angriffe gegeben wird, dass es vor allem auch Sabotage-Angriffe geben wird. Das waren alles Sachen, die nur hypothetisch waren und nicht richtig bewiesen. Und das hat Stuxnet jetzt sehr eindrücklich beweisen.

Autor

Sandro Gayken forscht zu Computersicherheit an der Freien Universität Berlin und hat ein Buch geschrieben mit dem Titel „Cyberwar“. Der Wurm Stuxnet wurde im Sommer 2010 erstmals entdeckt. Forscher und Konzerne brauchten Monate, ihn zu verstehen.

06 OTON
Wir haben jetzt den ersten echten Cyberwar-Angriff der Geschichte gesehen, nämlich einen Angriff, der tatsächlich physisch auch die Zielobjekte zerstört hat.

Sprecherin
Ralph Langner aus Hamburg, ein Sicherheitsberater für Computersysteme, der den Computerwurm Stuxnet früh untersucht hat.

07 OTON
Hier wurde tatsächlich physisch etwas zerstört bei militärischen Zielen und das zu einem sehr, sehr günstigen Preis, wenn man es mal in militärischen Kategorien rechnet. Also das werden wir wohl häufiger sehen.

Sprecher
Stuxnet ist aus zwei Gründen die bisher schärfste Cyberwaffe, sagt Gabi Dreo Rodosek, Professorin für Kommunikationssysteme und Internet-Dienste an der Universität der Bundeswehr München.

08 OTON
Stuxnet ist extrem genial programmiert und hat ein ganz bestimmtes Ziel, nämlich Industriekomplexe lahm legen.

Autor
Stuxnet infiziert Computer über einen USB-Stick, überwindet allerlei Sicherheitshürden, verbreitet sich über das Netzwerk und treibt sehr viel Aufwand, um nicht entdeckt zu werden. Für ihr informationstechnisches Meisterstück nutzten Stuxnets Programmierer gleich vier bisher unbekannte Sicherheitslücken in Microsofts Betriebssystem Windows. Solche unbekannten Lücken werden auf dem Schwarzmarkt gehandelt und kosten viel Geld, sagt der Programmierer Felix von Leitner, Inhaber der der Beratungsfirma Code Blue:

08a OTON

Die Schätzungen gehen alle aus von siebenstellig in Euro. Das ist eine Menge Geld, das haben normale Leute nicht, deswegen gehen viele davon aus, dass eine Regierung dahinter steckt.

Autor

Anders als herkömmliche Schadsoftware will Stuxnet nicht wahllos Rechner befallen. Ziel waren allein Industrieanlagen, die mit einer Siemens-Software gesteuert werden. Stuxnet ist keine Streubombe, sondern ein Lenkwaffe. Die Siemenssoftware steuert viele Industrieanlagen: Klärwerke, Raffinerien, Chemiewerke, Atomkraftwerke. Wie diese Industriesteueranlagen, auch SCADA-Systeme genannt, funktionieren, erklärt der Sicherheitsberater Felix von Leitner.

07a OTON

Wenn man so ein Atomkraftwerk hat oder überhaupt eine Anlage, dann hat man Steuerrechner und man hat lauter kleine verteilte Sensoren. Also da hinten ist jetzt zum Beispiel irgendeine Turbine von einem Kühlungssystem. Und die möchte man monitoren, man möchte sehen, ob die für Kühlung sorgt oder ob die gerade ausgefallen ist. Das heißt, man hat ein dezentrales System aus Sensoren, kleinen Rechnern, die hat man vernetzt über so eine Art Ethernet. Und dann hat man eine Schaltzentrale, wo die ganzen Sachen zusammenlaufen und da läuft dann so eine Siemens-Software, die die ganzen Meldungen rein bekommt und grafisch darstellt. Und das nennt sich dann Industriesteuerung.

09 OTON

Man muss auch sagen, dass der Aufwand, mit dem Stuxnet entwickelt wurde, enorm ist, da für die Entwicklung sowohl nicht bekannte Schwachstellen von Windows nötig waren, aber auch detaillierte Kenntnisse über den anzugreifen Industriekomplex.

Sprecherin

Gabi Dreo Rodosek von der Universität der Bundeswehr München:

10 O-Ton

Wenn man so ein Siemens-Industriesteuerungs-System aufbaut, dann ist das bei jeder Installation anders. Es wird halt von Leuten aufgebaut vor Ort, um den Anforderungen zu genügen, aber keine zwei Systeme sehen genau gleich aus.

Sprecherin
Felix von Leitner

11 OTON
Und das zeigt auch, dass der, der das programmiert hat, Zugriff auf so eine Anlage gehabt haben muss. Das ist wieder ein Indiz dafür, dass die echt Aufwand getrieben haben. Das ist keine Sache, die ich hier mal programmiere und dann läuft die dahinten. Das muss man schon testen.

Autor
Denn Stuxnet ist zwar auf Tausenden solcher Steuerungen rund um den Globus gesichtet worden. In den meisten Industrie-Anlagen macht Stuxnet gar nichts, sondern versucht nur, nicht entdeckt zu werden. Aktiv wird der Wurm nur in Industrieanlagen, in denen er ganz bestimmte Wechselrichter vorfindet, spezielle Geräte, die aus Gleichspannung eine bestimmte Wechselspannung erzeugen, etwa für Motoren, sagt Lars Kroll vom Viren-Spezialisten Symantec. Diese Wechselrichter programmiere Stuxnet um:

07b OTON
Und aus der Frequenz, die dort vorgegeben wird durch diesen Code, wissen wir, dass dort Motoren am Ende angeschlossen waren, die einfach speziell sind von ihrer Art – und zum Beispiel für Zentrifugen eingesetzt werden können.

Sprecherin
Mit diesen extrem feinfühligen Zentrifugen wird Uran geschleudert und so angereichert, damit es als Brennstoff taugt für Atomkraftwerke.

07c OTON
Technisch ist es so, dass diese Motoren mit einer speziellen Frequenz zu betreiben sind. Das heißt, diese Motoren für diese - offenbar - Zentrifugen, sollten zwischen einer Frequenz von 807 und 1210 Hz betrieben werden. Und Stuxnet ändert diese Frequenz, baut Frequenzsprünge ein, so dass diese Motoren beziehungsweise die Produktionsanlagen nicht das gewünschte Ergebnis produzieren – aber nicht so, dass nichts funktioniert, sondern, dass

sich der Motor dreht, die Zentrifuge sich dreht, aber am Ende kommt nicht das raus, was raus kommen sollte.

Autor
Ziel von Stuxnet war demnach, die Brennstoffproduktion für Atomkraftwerke zu sabotieren. Aber wo? Welches Land wurde angegriffen? Vieles deutet auf den Iran und seinen geplanten Atomreaktor in Busher:

07d OTON
Wir wissen ja, dass im Iran von den IAEA-Inspektoren inzwischen festgestellt wurde, dass Zentrifugenanlagen zerstört wurden. Wir alle wissen, dass Busher immer noch nicht in Betrieb gegangen ist, obwohl es Ende August in Betrieb gehen sollte. Also da kann man sich dann auch eins und eins zusammen zählen.

Sprecher
Sagt der Hamburger Stuxnet-Analyst Ralph Langner. In keinem Land habe Stuxnet zudem so viele Anlagen befallen wie im Iran.

12 OTON
Eins ist ganz klar: Wir reden hier über mehrere Nationalstaaten, die zusammen daran gearbeitet haben müssen.

13 OTON
Und die Verdächtigen, die man sich ausdenken kann, sind nicht besonders zahlreich. Sprich Israel hat ein extremes vitales Interesse daran, dieses Atomprogramm zu stören oder zu stoppen; auch die USA können sich das nicht leisten, hier zuzuschauen.

Autor
Aber bewiesen ist nichts.

14 OTON
(Collage aus TV-Tönen) Nun gibt es eine Art Cyberwar / Cyberkrieg ist kein Thema mehr für Science Fiction Filme allein /

15 OTON
Wenn sie das so durchgehen, dann sind bekannt: 2007 Estland, wir hatten im Georgienkrieg den Fall, wo Webserver einfach gekillt wurden, dass die nicht mehr verfügbar waren; wir haben jetzt Stuxnet als einen besonderen Angriff auf SCADA-Systeme.

Sprecher
ENISA-Direktor Udo Helmbrecht:

16 OTON
Wenn sie das aber auf die zeitliche Achse nehmen, sind das aber ja einzelne Ereignisse, die zeitliche noch beherrschbar sind. Und wenn sie über Cyber Warfare reden, muss ja immer jemand hingehen und sagen: Ich mache etwas im Sinne asymmetrischer Kriegsführung. Und das sehen wir heute noch nicht.

17 OTON (Englisch)
Es ist kein Cyberkrieg. Aber meine These ist: Es droht ein Cyberkrieg.

OTON
Michael McConnell, ehemaliger Leiter des mächtigen US-Abhörgeheimdienstes NSA, auf CBS.

17 OTON (Englisch)
Wir reden über die potentielle Bedrohung durch Cyberwar. Ich sage: Selbst wenn es einen gewöhnlichen Krieg zwischen Nationalstaaten gibt, wird Cyber ein Teil dieses Krieges sein.

MUSIK
(Rechenzentrum)

Autor
So formiert auch die Bundeswehr Cybertruppen mit offensivem Auftrag: 50-100 dieser Soldaten gehören zur „Gruppe Computernetzwerkoperationen“. Diese staatlich bezahlten Hacker sollen in fremde Netzwerke eindringen, dieses auszukundschaften, gegebenenfalls manipulieren oder zerstören – vermutlich mit Denial of Service Attacken, wie sie auch jene

nutzen, die Rechner der estnischen und georgischen Regierung sowie von Mastercard und VISA angriffen. Es zeichnet sich digitales Wettrüsten ab. Schon wird diskutiert, ob nicht auch die Bundeswehr Botnetze betreiben muss, um genug Feuerkraft zu besitzen.

Sprecherin
Das Problem: Schon die Vorbereitung von Computersabotage steht unter Strafe. Angriffe auf fremde Rechner, schwere Computersabotage sind in Deutschland strafbar und können mit bis zu 10 Jahren Gefängnis bestraft werden.

Autor
Das ist nicht die einzige rechtliche Grauzone von Cyberkonflikten. Wann ist ein Angriff über das Internet nicht mehr kriminell, sondern ein kriegerischer Akt, der Vergeltungsschläge rechtfertigt? Auch die NATO hat darauf bisher keine überzeugende Antwort gefunden. Artikel 5 des NATO-Vertrags legt den Bündnisfall fest: Ein bewaffneter Angriff auf ein NATO-Mitglied gilt als Angriff auf alle Bündnispartner.

Musik
(Rechenzentrum)

Autor
Doch bei einem echten Cyberwar ist der Angreifer meist unbekannt. Selbst wenn man ihn fasst und sein Heimatland kennt, muss immer noch nachgewiesen werden, dass die Regierung den Angriff befohlen hat.

17c OTON Ich gebe Ihnen ein schönes Beispiel, was die Problematik darstellt.

Sprecherin
Der europäische Netzbewacher Udo Helmbrecht.

17c OTON
Als der Angriff 2007 auf Estland war, war ja die Reaktion: Ah, jetzt muss die NATO eingreifen. Aber es hat sich schnell herausgestellt, dass das die falsche Antwort ist, denn es war ja keine kriegerische Attacke auf Estland, also kann man auch nicht als NATO antworten. Und da ist die Frage, wie geht man damit um und da steht man in der Tat erst am Anfang.

Autor

Ob, wie und wann NATO-Länder sich im Falle eines Internetangriffs beistehen müssen, konnte auch auf dem NATO-Gipfel in Lissabon im vergangenen November nicht geklärt werden. General Kurt Herrmann ist Direktor NCSA, einer NATO-Agentur, die NATO-Netze und IT-Systeme absichert.

27 OTON

Ich denke, es ist klar geworden, dass die Bedrohung der Netze eine strategische Dimension eingenommen hat, dass man Vorkehrungen treffen muss. Ob es dann so einfach ist, einen Artikel 5-Fall fest zu stellen, auf diese Frage möchte ich nicht weiter spekulierend eingehen. Aber ich denke, einen Cyberangriff kann heute durchaus die Dimension einnehmen, die man früher nur von energetischen Waffen erwarten konnte. Das heißt, im Prinzip können Häcker Schäden anrichten, die durchaus vergleichbar sind mit Schäden, die man durch Sprengkörper oder durch Waffeneinwirkung erzielen kann.

Sprecherin

Deswegen hat die NATO in Lissabon beschlossen, nicht nur zu Land, Wasser und in der Luft für Sicherheit sorgen wollen, sondern erstmals auch „Cyberspace“.

Autor

Besonders ängstlich Schauen die westlichen Beobachter des Internets auf Datenpakete aus dem Osten, vor allem aus China. Dort sei der Krieg in Datennetzen, der Angriff auf feindliche Computer, seit 20 Jahren fester Bestandteil der Militärdoktrin, sagt der Sicherheitsforscher Sandro Gayken.

OTON

Man redet auch davon – genaue Zahlen gibt es da natürlich nicht – dass die Chinesen Hacker haben, sehr, sehr gute, wissenschaftlich ausgebildete und soldatisch trainierte Hacker in einer Truppenstärke von 100.000 bis 150.000. Das ist natürlich immens. Mit einer Gruppe von 100 richtig guten Hackern kann ich schon ziemlich viel anstellen. Mit 100.000 stehen einem eine ganze Menge Türen offen.

Autor

So wurde im Bundeskanzleramt Spionage-Software gefunden, die Informationen nach China schicken sollte; auch Google beklagt Spionage-Angriffe aus dem aufstrebenden Reich der Mitte. Solch netzgestützter Informations-Diebstahl ist ärgerlich. Doch große Sorgen bereitet allen Cyber War Verantwortlichen etwas anderes: Wirklich verwundbar sind Industriestaaten an ihren kritischen Infrastrukturen: Stromnetze, Telefonnetze, Internet, Wasserversorgung.

19 OTON
Das ist lange Zeit etwas stiefmütterlich behandelt worden, weil man gesagt hat, das wäre automatisch ein Kriegsverbrechen, wenn man diese kritischen Infrastrukturen angreift. Denn das sind dann Angriffe auf zivile Strukturen. Das ist im Kriegsrecht natürlich eindeutig geregelt, dass man das nicht darf. Deswegen hat man gesagt, aus juristischen Gründen würde das keiner machen. Ist man dann aber eines besseren belehrt worden.

Sprecherin
Der Berliner Sicherheitsforscher Sandro Gayken.

19 OTON
Es gab tatsächlich relativ viele Programme, die sagt haben: Naja, es gibt dieses Attributionsproblem, das heißt, man kann den Angreifer sowieso nicht identifizieren und dann kann mir auch keiner mit dem Kriegsrecht kommen. Das heißt, militärisch ist es wieder rational für die Staaten, die rücksichtsloser sind, mit so was auch zu planen. Denn man kann mit Infrastrukturangriffen eine ganze Menge auch machen.

Autor
Selbst Atomkraftwerke ohne Internetanschluss sind vor Cyberangriffen nicht sicher sind, das hat Stuxnet bewiesen. Experten, die ihr Geld mit Sicherheitsberatung verdienen, sagen: Auch die deutsche Industrie sei durch Software wie Stuxnet verwundbar.

20 OTON
Das ist nicht nur denkbar, das ist eine Tatsache. Da muss man gar nicht spekulieren. Wenn sie die deutschen Industrieanlagen kennen, dann wissen Sie, dass das natürlich funktioniert.

Sprecherin
Der Hamburger IT-Berater und Analyst der Schadsoftware Stuxnet, Ralph Langner.

20 OTON
Sie finden die Siemens-Steuerung, die hier als Mittel zum Zwecke verwendet wurde, in jeder Fabrik, egal, ob sie in ein Kraftwerk gehen, bei einem Autobauer ins Werk gehen oder in eine Chemie-Anlage, sie finden diese Steuerung überall. Es ist ein Faktum, leider, muss man sagen, dass unsere Anlagen genauso verletzlich sind für diesen Angriffvektor, den wir hier sehen, wie wir das für den Iran jetzt unterstellen müssen.

21 OTON
Wir und ich persönlich haben mit Stuxnet sehr viel zu tun, weil wir mit vielen großen Kunden derzeit arbeiten, die sich sorgen, dass sie vielleicht Opfer der nächsten Cyberattacke werden könnten.

Sprecherin
Lars Kroll, vom Anti-Viren-Anbieter Symantec.

22 OTON
Wir sind ja in Deutschland ein Autoland. Man stelle sich eine Produktion für Autos und LKW vor. Dort gibt es Industrieroboter, dort herrscht ein sehr hoher Automatisierungsgrad: Roboter, die Autoteile schweißen, die den Motor ins Auto einbauen. All diese Roboter werden von spezialisierten Systemen gesteuert – unter anderem auch von Systemen, die für eine Attacke wie Stuxnet verwundbar sind.

Autor
Wie sicher sind die deutschen Atomkraftwerke gegen Stuxnet? Lassen sich auch ihre Sensoren, Regler und Motoren über das interne Netz umprogrammieren wie offenbar im Iran?

OTON
Ob das geht, das hängt davon ab, in welchem Sicherheitsmodus die fahren.

Sprecherin
Der Programmierer Felix von Leitner:

OTON

Das ist eines der Argumente der deutschen Kraftwerke gewesen: Bei uns wird das in einem Sicherheitsmodus gefahren, dass vor Ort jemand an dem Gerät einen Schlüssel umlegen muss, damit die programmierbar sind über das Netz. Und damit ist die Angreifbarkeit nicht gegeben, behaupten die. Was stimmen mag. Aber es ist immer noch keine Garantie, dass nicht jemand vor Ort einen Spion in dem Kraftwerk hat. Also eine hundertprozentige Garantie gibt es da nicht, aber es ist schon mal eine gute Sache.

Sprecherin
Alle deutschen AKW-Betreiber ließen eine Interview-Anfrage unbeantwortet.

22g OTON
Natürlich kann man sagen: Einen 100%igen Schutz gibt es nicht. Aber dann sollte man sich klar machen, dass der Schutzgrad, den wir in diesem Bereich Kontrollsysteme heute sehen, der ist nicht irgendwo bei 99%, sondern der ist gegenwärtig irgendwo bei 20 Prozent. Das ist das große Problem, was wir haben.

Sprecherin
IT-Berater und Stuxnet-Analyst Ralph Langner.

OTON
Wir haben hier einen riesigen Nachholbedarf. Man kann viel tun, das Problem ist nur, das kostet Zeit und Geld. Aber diese Aufgabe steht jetzt vor uns.

23 OTON
Langfristig muss man gucken, dass man Software entwickelt, dass sie nicht anfällig ist, aber das ist bisher immer gescheitert.

Sprecherin
Sicherheitsberater und Programmierer Felix von Leitner.

23 OTON
Was man tun muss, ist, dass man in der Richtung forscht, dass man Geld dafür ausgibt, das unsere Ingenieure geschult werden mit der Idee, dass Software sicher entwickelt werden soll und dass man da Aufwand für treiben muss. Das ist nichts, was man im Nachhinein machen

kann. So funktioniert im Moment die Industrie, aber eigentlich muss man das während der Software-Entwicklung machen. Ist wie, wenn man eine Fassade wechselt. Das sieht dann gut aus, aber so strukturelle Probleme im Nachhinein zu beseitigen, ist immer sehr schwierig bis geht gar nicht.

OTON
Was man natürlich tun kann, ist dass man sagt: Okay, diesen Ist-Zustand der hohen Vernetzung versuche ich gar nicht erst zu retten, sondern ich baue den einfach wieder zurück.

Autor
Sagt Sicherheitsforscher Sandro Gayken. Diese Idee der „Entnetzung“ meint nicht nur: Wichtige Computer dürfen nicht am Internet hängen. Es bedeutet auch: Wichtige Computer sollten gar nicht vernetzt sein, auch nicht innerhalb einer Fabrik oder Armee.

22a OTON
Damit baue ich meine Abhängigkeiten zurück, meine Verwundbarkeiten zurück. Das ist natürlich mit massiven Effizienzeinbußen verbunden, auch mit hohen Kosten, man muss dann wieder mehr Personal einstellen. Aber zumindest ist so ein partieller Rückbau in sehr sensiblen Bereichen, das einzige was man tun kann.

Sprecherin
Felix von Leitner hält das Gegenteil für richtig:

24 OTON
Die Doktrin, die uns da schützen kann, ist kürzlich von einem amerikanischen Regierungsmenschen formuliert worden. Der meinte: Der beste Schutz gegen so was ist Kodependenz, also wenn wir alle voneinander abhängen. Wenn wir ein gemeinsames Stromnetz haben und auch in Russland der Strom ausfällt, wenn bei uns der Strom ausfällt, dann greift uns Russland nicht mehr an, ganz einfach. Das wird uns schützen.

Autor
Vorerst sind die meisten Industriestaaten jedoch damit beschäftigt, sich zu sammeln und die Lage zu analysieren. Schnell wird klar: Angriffe über das Internet gehen fast immer über nationalstaatliche Grenzen hinweg.

24a OTON

Es gibt noch keine Regulierung des Cyberwars, keine rechtlichen Maßstäbe. Das ist natürlich auch sehr schwer zu entwickeln. Man kann die Angreifer nicht identifizieren, wenn ich die Angreifer nicht identifizieren kann, kann ich ihn nicht rechtlich belangen, wenn er sich falsch verhält. Da muss man sich generell fragen, inwiefern es Sinn macht, irgendwelche Regulierungen zu entwerfen, wenn ich die sowieso nicht forcieren kann.

Sprecherin

Sicherheitsforscher Sandro Gayken.

24b OTON

Ich selber bin involviert in so ein paar Regulierungsansätze für die EU und für Deutschland und mein Ansatz ist, dass man dann nach innen regulieren muss und nicht versuchen darf, den Angreifer zu regulieren. Man muss sich selbst regulieren auf ein sicheres Verhalten und das bedeutet für mich, dass man den Betreibern kritischer Infrastruktur etwa vorschreibt, dass sie hochsichere Netzwerke verwenden müssen, dass sie sich insgesamt kleiner machen müssen, ihre Netzwerke runter fahren müssen, sichere IT verwenden müssen. Denn von selber machen die das nicht, das ist wahnsinnig teuer für die, so dass man da Regulierungsbedarf hat und gesetzlich steuern müsste.

Autor

Wenn der Angreifer nicht zu fassen ist, muss die Verteidigung stehen. Dazu zählen auch neue Institutionen. Oberste Behörde für die Cyber-Abwehr in Deutschland ist das Bundesamt für die Sicherheit in der Informationstechnik, BSI. Die Bonner Techniker sind vor allem zuständig für den Schutz der Regierungsnetze. Ähnliche Einrichtungen gibt es in vielen EU-Staaten.

OTON

Meiner Meinung nach ist das größte Problem, das wir heute haben, dass wir in unserer demokratischen Struktur nicht so aufgestellt sind, dass wir dem wirklich effektiv gegenübertreten können.

Sprecherin

Sagt Udo Helmbrecht, Direktor von ENISIA, dem Institut für Netzsicherheit der Europäischen Union:

OTON

Wir haben immer diese Silo-Organisationen: Wir haben Verteidigungsministerium, wir haben Innenministerium, Wirtschaftsministerien, wir haben verschiedene Behörden, wir haben verschiedene europäische Strukturen, verschiedene zuständige Kommissare. Und die Kriminellen haben leider den Vorteil, dass sie mit Mitteln agieren, wo wir noch nicht - muss man ehrlicher Weise sagen – die richtigen Mittel haben. Solange es sich um Computerkriminalität handelt, können wir damit recht gut umgehen. Aber wenn es wirklich in Richtung Cyber Warfare geht, dann ist da noch einiges zu tun.

Autor

Gemeint sind vor allem: Neue Strukturen und Institutionen. So soll in Deutschland bald ein Cyber-Abwehrzentrum entstehen, ein staatlicher Wachposten im Internet, besetzt mit Polizisten und Geheimdienstlern. Mit solchen Einrichtungen wollen Staaten das Netz im Blick behalten; Stabsstellen für die Cyberkrieger des Militärs, die ihr neues Gefechtsfeld überblicken und analysieren wollen, um Strategien für Angriff und Verteidigung zu erarbeiten. Die USA sind auf diesem Weg schon einen Schritt weiter.

OTON (Englisch)

Was sie jetzt über den Cyberkrieg hören ist Teil einer lange laufenden Kampagne, um die Kontrolle über das Internet weg zu bewegen von seinem derzeitigen Modell zu einem, das den Geheimdiensten und der NSA viel mehr Einfluss darauf sichert, was Leute im Internet dürfen oder nicht dürfen.

Sprecherin

Marc Rotenberg ist Direktor des Electronic Privacy Information Center, einer Datenschutzorganisation aus den USA.

OTON (Englisch)

Ob das Militär eine größere Rolle in Cybersicherheit spielt, ob sich Internetbenutzer ausweisen müssen, ob Regierungsbehörden unsere Kommunikation routinemäßig überwachen dürfen. All diese Konsequenzen stehen hier zur Debatte.

Sprecherin

Der Netzaktivist und Programmierer Bruce Schneider geht noch einen Schritt weiter:

OTON (Englisch)

Die Bedrohung durch Cyberwar ist massiv übertrieben. Sie ist übertrieben durch Regierung und Wirtschaft um sich Macht und Geld zu sichern.