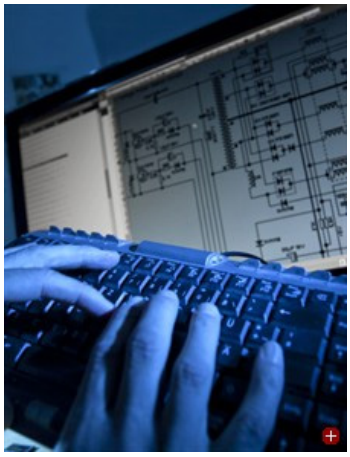
Frankfurter Allgemeine
FAZ.NET

Kurz-Link: http://www.faz.net/-01xy9l

Digitale Attacken

Cyberwar – was ist das?

Die Regierungen der Industriestaaten rüsten sich gegen kriegerische Angriffe aus dem Netz. Aber wie wahrscheinlich sind solche Attacken? Wie würden sie aussehen? Und wie kann man sie verhindern? *Alard von Kittlitz* und *Harald Staun* geben bündige Antworten auf die wichtigsten Fragen.



Der Begriff „Cyberwar" scheint so unwiderstehlich, dass er gerne für alle möglichen Computerattacken verwendet wird.

1. Aktivisten legen Kreditkartenfirmen lahm, Hacker greifen Sony an, ein Computerwurm sabotiert iranische Atomanlagen – was hat das alles miteinander zu tun?

Meistens nicht viel. Der Begriff „Cyberwar" ist so unwiderstehlich, dass er von vielen Medien gerne für alle möglichen Computerattacken verwendet wird, ob es sich um vorübergehende Serverblockaden, kriminellen Passwortdiebstahl oder tatsächlich um ausgefeilte Angriffe staatlicher Sonderkommandos handelt. Nicht jeder Hacker ist ein Cyberkrieger, weshalb man zwar trotzdem über deren Motive streiten kann, es aber hilfreich wäre, Kreditkartenbetrug von Spionage oder Vandalismus von Sabotage zu unterscheiden. Das terminologische Chaos macht es nämlich auch den Analysten nicht einfacher: Wer jeden Windows-Virus mit komplexen Großangriffen in einen Topf schmeißt, warnte Anfang des Jahres eine Studie der OECD, käme zu „grob irreführenden Schlussfolgerungen". Auch Microsofts Sicherheitsexperte Scott Charney hält eine genaue Abgrenzung der verschiedenen Kategorien von Cyberattacken für wichtig. Er empfiehlt, zwischen Computerkriminalität, Militärspionage, Wirtschaftsspionage und Cyberkrieg zu unterscheiden, um adäquat darauf reagieren zu können. Also nicht nur, damit am Ende nicht die Marines das Kinderzimmer eines talentierten Script-Kiddies in Schutt und Asche legen; sondern auch umgekehrt.

2. Was ist denn Cyberwar im engeren Sinn?

Auch darüber streiten die Experten schon ewig. Eine verbindliche völkerrechtliche Definition wäre aber ganz nützlich, weil davon im Zweifelsfall auch die entsprechenden Vergeltungsmaßnahmen abhängen. Streng genommen müsste man den Begriff nur auf nationalstaatliche Konflikte anwenden, die mit digitalen Bomben ausgetragen werden. Das bekannteste Beispiel dafür sind die „Distributed Denial of Service"-Angriffe (DDoS) auf georgische Websites im Kaukasuskrieg 2008, mutmaßlich ausgeführt von russischen Hackern. Brauchbare völkerrechtliche Regeln müssten aber auch das Ausmaß des eingetretenen Schadens berücksichtigen. Im Falle Georgiens war er minimal, nicht nur verglichen mit den Opfern des Militärs, das gleichzeitig in Tiflis einmarschierte. Aber ab wann kann man dann von einem kriegerischen Akt sprechen? Wann tritt der Bündnisfall ein, der nach einem Beschluss der Nato vom Ende vergangenen Jahres auch durch Cyberangriffe ausgelöst werden kann? Wenn Flugzeugpläne vom Server des Verteidigungsministeriums gestohlen werden? Oder erst, wenn ein fremdes Land die Stromversorgung eines Mitgliedstaats ausschaltet?

3. Was wäre denn das Worst-Case-Szenario?

Seit Jahren warnen amerikanische Politiker vor einem „digitalen Pearl Harbor", einem Cyberangriff aus dem Nichts. Auch der nagelneue amerikanische Verteidigungsminister Leon Panetta gehört zu jenen Menschen, die gerne Alarm schlagen: Ein Cyberangriff, der „unsere Energiesysteme, unser Verteilernetz, unsere Sicherheitssysteme, unsere Finanzsysteme und unsere Regierungssysteme lahmlegt", sei „in der heutigen Welt eine reale Möglichkeit", sagte er Anfang des Monats und forderte, „sowohl defensive als auch aggressive Maßnahmen" dagegen zu unternehmen. Noch dramatischer schätzt der ehemalige Antiterrorberater des Weißen Hauses, Richard A. Clarke, die Lage ein. In seinem 2009 erschienenen Buch „Cyberwar" schildert er ein Szenario, das klingt, als hätte er sich vom Drehbuch von „Stirb langsam 4.0" inspirieren lassen: Chinesische Hacker schalten das Pentagon aus, jagen Ölraffinerien in die Luft, lassen Flugzeuge abstürzen und Züge ineinandercrashen – und das alles innerhalb von 15 Minuten.

4. Und warum sollte so etwas nicht passieren?

Zum Thema

Cyberwar: Alles wird zur Ware

Gewähren Sie Einsicht, Sir: die Vereinigten Staaten rüsten sich für den Cyberwar

Pizzas und Kanonen:

Die Vorbereitungen auf den virtuellen Krieg haben schon begonnen

Aus dem Maschinenraum: Kybernetische Krieger werden überschätzt Von Constanze Kurz

Zum Beispiel, weil so ein Angriff sehr teuer wäre. Allein die Entwicklung des Computerwurms Stuxnet, der vor einem Jahr die Steuerung der Uranzentrifugen im iranischen Atomkraftwerk Bushehr manipulierte, kostete mehrere Millionen Euro und beschäftigte fünfzig Personen rund ein Jahr lang, schätzt der Sicherheitsexperte Ralph Langner. Selbst relativ verletzliche Steuerungssysteme wie in Amerika (siehe Frage 14) laufen auf Tausenden unterschiedlichen Hardware-Plattformen und sind zum Teil in eigenen Programmiersprachen geschrieben. Am wahrscheinlichsten, kommentierte ein Sicherheitsexperte die in „Stirb langsam 4.0" gezeigten Risiken, sei noch, dass ein Polizeiauto mit einem Hubschrauber zusammenstößt, und zwar in der Luft.

Vor allem aber gibt es auch einen politischen Grund: Natürlich ist es vorstellbar, dass chinesische oder russische Hacker amerikanische Atomkraftwerke hochgehen lassen oder deutsche Dämme sprengen, vorausgesetzt, sie wollen einen Weltkrieg anzetteln. Sie brauchten dazu aber nicht nur eine enorme Cyberarmee, sondern vor allem: ein Motiv. Und wenn es so weit kommen sollte, würde sich wohl kein Land auf virtuelle Waffen beschränken, der Krieg per Computer wäre nur ein Element der militärischen Auseinandersetzung.

5. Und was ist mit Terroristen? Die kümmern sich doch nicht um solche Konsequenzen?

Mag sein, aber sie brauchten eben einen sehr potenten Sponsor. Vielleicht sind Terroristen deshalb bisher kaum durch Netzattacken aufgefallen. Wer von „Cyberterrorismus" spricht, meint damit eher, dass Anleitungen zum Bombenbau im Internet zu finden sind. Oder ganz einfach, dass auch Terroristen per E-Mail kommunizieren. Konkret wurde aber noch keine Autobombe online gezündet. Weshalb sogar Stephen Cummings, der Chef der britischen Behörde zum Schutz kritischer Infrastrukturen, 2008 erklärte: „Cyberterrorismus ist ein Mythos."

6. Warum schreien dann alle so laut?

Weil sie Zeitungen verkaufen wollen. Oder Software. Clarke zum Beispiel ist Chef eines Beratungsunternehmens, so etwas lebt nicht unbedingt von Gelassenheit. Schon längst ist die Vorstellung eines cybermilitärischen Komplexes keine Verschwörungstheorie mehr, weshalb oft genau jene Experten die größte Panik verbreiten, die versprechen, vor den Gefahren schützen zu können. Es gibt leider noch einen anderen Grund: Die Angriffsmöglichkeiten sind unermesslich. Und Cyberwar ist ein Krieg, der nach neuen (oder ganz ohne) Regeln funktioniert. So asymmetrisch, dass dagegen selbst Terrorismus überschaubar erschient.

7. Welche Nationen haben denn die größten Cyberarmeen?

China, Russland, die Vereinigten Staaten, Frankreich, Israel und das Kosovo, meint jedenfalls Cyberwar-Experte Sandro Gaycken von der Freien Universität Berlin. 140 Länder, so schätzte eine Studie vor drei Jahren, arbeiten mittlerweile an Cyberwar-Programmen. In drei, vier Jahren, glaubt Gaycken, wird das in ganz neuen Dimensionen zu spüren sein.

8. Was ist denn der größte Schaden, den virtuelle Waffen bisher verursacht haben?

Wenn es um Wirkung und Kosten geht, vermutlich wirklich Stuxnet. Wie groß der Schaden tatsächlich gewesen ist, lässt sich schwer bemessen, weil die Iraner zu der Sache aus verständlichen Gründen nicht viel sagen wollen. Erheblichen Schaden haben aber sicher auch die DDoS-Attacken auf das hochvernetzte Estland angerichtet, ein Land, in dem der Internetzugang als Menschenrecht gilt. Drei Wochen lang wurden Finanznetze mit DDoS-Attacken überladen, das Bankensystem brach tagelang zusammen. Und der erste bekannte große Angriff, auf eine russische Pipeline in Sibirien, die deswegen explodierte, dürfte auch ziemlich viel Geld gekostet haben. Auch da vermutet man den amerikanischen Geheimdienst als Urheber.

9. Woran erkennt man überhaupt, wer hinter einem Cyberangriff steckt?

Wenn man Glück hat: an einem Bekennerschreiben. Und deshalb meistens gar nicht. Weshalb sich auch das Pentagon etwas schwer tun dürfte mit seiner neuen Cyberwar-Strategie, die in den nächsten Tagen veröffentlicht werden soll. Die Direktive regelt nicht nur, welche digitalen Waffen die amerikanische Armee offensiv einsetzen darf, sondern sieht auch vor, schwere virtuelle Angriffe anderer Nationen künftig als kriegerischen Akt zu

betrachten und „äquivalent" zu vergelten, im Zweifelsfall mit konventionellen Mitteln. „Wer die Stromnetze unseres Landes sabotiert, muss mit Raketen im Schornstein rechnen", ist der markige Satz, mit dem ein Pentagon-Sprecher die Parole auf twitterkompatible Länge gebracht hat. Doch damit linke Pazifisten irgendwann auch gegen diese Unverhältnismäßigkeit demonstrieren können, müsste das Pentagon erst einmal wissen, wem es den Krieg erklären will.

10. Kann man den Angriff nicht zurückverfolgen?

Manchmal – zu dem Computer, von dem er gestartet wurde. Aber in der Regel sind das Geräte, die selbst gekapert oder dazu benutzt wurden, eine Attacke umzuleiten. Und was hilft das schon, wenn ein pakistanischer Hacker von einem Computer in Melbourne aus seinen Code verschickt: Der Mensch-Maschine-Gap, wie Gaycken das nennt, also der „Zwischenraum zwischen Finger und Tastatur", kann nie ganz geschlossen werden. Selbst die Angriffe auf Estland und Georgien konnten nie zweifelsfrei der russischen Regierung angekreidet werden. Dazu kommt, dass gerade Datenspuren wunderbar zu manipulieren sind. „Daten sind Märchen", beschreibt Gaycken: „Ein Schadprogramm ist immer eine geschriebene Geschichte, die von ihrem Autor, dem Programmierer, von Anfang bis Ende frei gestaltet werden kann." Ein strukturelles Problem, denn „Daten sollen schließlich veränderbar sein".

11. Weiß man eigentlich inzwischen, wer hinter Stuxnet steckt?

Nein. Wäre ja auch irgendwie schwachsinnig, sich zu einem Angriff zu bekennen, dessen größter Vorteil ist, dass man nicht sagen kann, woher er kam. Die beiden Hauptverdächtigen bleiben Israel und die Vereinigten Staaten. Im Code des Wurms finden sich ein paar Indizien, die auf Israel als Urheber hinweisen. Vielleicht ist das aber die bewusst gelegte falsche Fährte. Für Amerika als Täter spricht neben dem Motiv auch ein von Wikileaks aufgetanes Dokument aus den „diplomatic cables". Darin wird zu „verdeckten Operationen" gegen das iranische Atomprogramm aufgefordert.

12. Warum sind kritische Infrastrukturen (Atomkraftwerke, Rüstungskonzerne, Strom-versorger) überhaupt ans Internet angeschlossen?

Sind sie ja nur zum Teil. Sogar so alte Kernkraftwerke wie Biblis arbeiten in Deutschland mit sogenannten „insularen Systemen", die sind nicht ans Netz angeschlossen, sogar mit einem USB-Stick ist es ziemlich schwierig. Umgekehrt: Wie viele der Dinge, die Sie im Alltag tun, haben nichts mit Computern zu tun? Wie viele sind netzunabhängig? Wir leben in einer digitalen Welt. Von deren Vorteilen leben auch die Betreiber großer Industriemaschinen. Die Betreiber selbst müssen sich überlegen, ob ihre Steuerungsanlagen unbedingt einen W-Lan-Zugang haben müssen. Genauso oder noch gefährlicher ist die Tatsache, dass lauter für Angreifer potentiell interessante Dokumente ständig durch den Äther fliegen. Ein Bauplan als E-Mail-Attachment. Ein Zugangscode per SMS. So was ist nicht gut.

Dummerweise weiß keiner so genau, welche Anlagen direkt oder indirekt am Netz hängen. Systemkomponenten in Zügen, Notaggregate in Krankenhäusern . . . Und wenn ein dezentrales Netz nicht mit dem Internet verbunden ist, eignet sich trotzdem der Laptop des Wartungstechnikers als Einfallstor. Auch auf Parkplätzen herumliegende USB-Sticks sind ein häufiger Übermittler von Computerwürmern, wie das amerikanische Militär im vergangenen Jahr zu spüren bekam, als der Computerwurm „agent.btz" fast das komplette Militärnetz infiltrierte. Neugier ist ein zuverlässiger Komplize.

13. Warum kann eigentlich jeder picklige Teenager mit ein wenig Grips eine Website hacken?

Windows Vista hat 86 Millionen Zeilen Code, da ist viel Platz für immer neue Sicherheitslücken, sogenannte „Zero Day Exploits". Funktionalität und drollige Features waren bei der Entwicklung kommerzieller Software eben immer wichtiger als Sicherheit. Dazu kommt, dass Angreifer im Prinzip beliebig viele Versuche haben, solche Lücken zu finden: Sie dürfen unzählige Fehler machen, das System keinen einzigen. Für den Privatnutzer ist das ein Privatproblem. Aber für einen Flughafentower sehr heikel. Oder für das amerikanische Verteidigungsministerium.

14. Um Gottes willen, arbeitet das Pentagon etwa mit Windows?

Ja klar, alles andere wäre zu teuer, oder wie Microsoft so schön auf einer speziellen Seite für das Verteidigungsministerium wirbt: „Mit den Vergünstigungen unseres Lizenzprogramms können Sie ganz einfach die am weitesten verbreitete und innovative Software nutzen und gleichzeitig das Geld der Steuerzahler sparen." Da muss man sich nicht wundern, dass General Keith Alexander, der Chef der National Security Agency (NSA), 250.000 Cyberangriffe pro Stunde auf die Rechner des Pentagon zählt; mit den meisten wird wohl ein handelsüblicher Virenscanner fertig. Und trotzdem: Keine andere Nation gilt als verletzlicher als die Vereinigten Staaten. Das liegt zum einen an den vielen Billigelementen, die wer weiß wo drinstecken, vom PC bis zur Steuerungstechnik

industrieller Anlagen. Zum anderen an der unvergleichlich hohen Abhängigkeit von privaten Subunternehmern, die für die Sicherheit ihrer Daten selbst verantwortlich sind. Erst vor vier Wochen war es Hackern gelungen, in das System des Rüstungskonzerns Lockheed Martin einzudringen. Es wurde nichts beschädigt oder entwendet, behauptet das Unternehmen, aber wer weiß: Vielleicht hat nur noch niemand etwas bemerkt.

15. Tragen eigentlich alle Hacker so komische Masken?

Nein, nur die Aktivisten des Internetkollektivs Anonymous – und die auch nur, wenn Sie auf die Straße gehen. Anonymous ist zwar auch unberechenbar, scheint aber eher eine zeitgemäße Form des politischen Widerstands zu sein. Und die neuesten Unruhestifter, die Hacker der Spaßguerrilla von Lulz Security, die . . .

16. Lulz was?

„The Lulz" bedeutet so etwas wie Schadenfreude im Jargon der Ureinwohner des Internets. Der Begriff ist eine Abwandlung des Akronyms „Lough out loud" und ist in etwa das, was die Benutzer aus dem Milieu des Internetforums „4 Chan" dort haben, wo bei anderen Menschen moralische Maximen gespeichert sind. Lulz Security, kurz Lulzsec, machte in den vergangenen Wochen fast täglich durch Hacks auf sich aufmerksam, klaute Kundendaten von Sony und Sega, nahm die CIA-Website vom Netz, veröffentlichte Passwörter des amerikanischen Senats und zuletzt Ermittlungsprotokolle der Grenzpolizei von Arizona. Lulzsec beschreibt sich selbst als „Weltmarktführer in Sachen Spitzenunterhaltung auf eure Kosten".

17. Aber Anonymous und Lulzsec haben doch auch angekündigt, Regierungen lahmzulegen?

Ja. Steht ja jedem frei, das zu behaupten.

18. Im Ernst: Die haben doch eine Ionenkanone, ist das nicht gefährlich?

Die Low Orbit Ion Cannon ist eine Software, um Webserver mit Anfragen zu überfluten. Solche DDoS-Angriffe können sehr effektiv sein, verursachen aber in der Regel keinen dauerhaften Schaden. Natürlich könnten sich auch hinter der Maske der Hacktivisten wiederum kriminelle Akteure verbergen oder ausländische Cyberspione. Aber warum sollten die sich die Mühe geben, sich als virtuelle Protestbewegung auszugeben, wo sie doch problemlos anonym agieren können?

19. Das ist ja alles ganz interessant. Aber viel sicherer fühle ich mich jetzt auch nicht. Zum Glück hat ja auch Deutschland seit ein paar Tagen ein Nationales Cyber- Abwehrzentrum, oder?

Das Abschreckendste daran ist leider sein Name. Es handelt sich um zehn Beamte in einem Verwaltungsgebäude in Bonn-Mehlem. Ihre Aufgabe besteht eher in der Koordination der Behörden. Das klingt nach angenehmer Besonnenheit und ist vermutlich doch nur die Institutionalisierung der politischen Ohnmacht.

Text: F.A.Z.
Bildmaterial: dpa