Krieg der Rechner

Warum es so schwierig ist, sich vor militärischen Cyberangriffen zu schützen

Sandro Gaycken | **Datenspionage, Sabotage, Wirtschaftsmanipulation: Von Staaten getragene Übergriffe auf IT-Systeme werden immer zahlreicher, effizienter und gezielter. Eine Entwicklung mit gravierenden sicherheitspolitischen Konsequenzen, die sich mit konventionellen Schutzstrategien wie Abwehr und Abschreckung nicht beherrschen lässt.**

Das Thema Cybersecurity fristete lange ein Nischendasein. Inzwischen ist es jedoch in der öffentlichen Debatte angekommen, wie sich im Februar auf der Münchner Sicherheitskonferenz zeigte: Dort bekräftigte die Bundesregierung ihre Absicht, ein nationales Cyberabwehrzentrum zu errichten. Ob ein solcher Schritt sinnvoll ist, muss allerdings bezweifelt werden. Denn die neuen Attacken kommen nicht von den üblichen computerversierten Teenagern und Kleinkriminellen, sondern vor allem von Staaten – von Militärs und Nachrichtendiensten. Dieser Akteurswechsel bringt eine neue Qualität der Cyberangriffe mit sich, die bislang kaum verstanden wird und konventionelle Schutzkonzepte aushebelt.

In Theorie und Praxis hat sich inzwischen gezeigt, dass gegen den neuartigen Cyberwar weder eine passive direkte Abwehr nach dem Prinzip des Schutzwalls noch eine aktive präventiv über Abschreckung durch Strafverfolgung oder Vergeltung wirkende Verteidigung greift. Die vollständige Ineffizienz dieser beiden Schutzvarianten ist ein neues Phänomen für die Sicherheitspolitik – mit gravierenden Konsequenzen. Denn ohne passive oder aktive Abwehr kann weder effektiv geschützt noch reguliert werden. Die konventionelle IT-Sicherheit ist also zahnlos. Nur ein radikaler Um- und Rückbau der Informationsstrukturen kann helfen, und das auch nur an den diversen Zielsystemen selbst und nicht über Superstrukturen wie Abwehrzentren.

Diese Einsicht ist in letzter Konsequenz teuer, umständlich und gegen den Zeitgeist; doch sie ist unumgänglich. Und je früher sie kommt, desto weniger Zeit und Geld werden für Zwischenlösungen verschwendet. Diesen Fehler haben die USA bereits begangen: Dort wurden Milliarden in Forschung investiert, deren Unsinnigkeit jedem unabhängigen Wissenschaftler von Anfang an klar war. Um

der beginnenden deutschen Debatte also einen besseren Start zu ermöglichen, sollen hier die für das Versagen der klassischen Schutzkonzepte verantwortlichen Strukturprinzipien des Cyberwar erläutert werden.

Kleiner Einbruch, große Wirkung

Das erste und wichtigste Prinzip der neuartigen Cyberattacken ist ihre hohe Wirkasymmetrie: Mit einer geringen Ursache lässt sich eine immense Wirkung erzielen. Denn auch wenn hocheffizienten Angriffen ein hoher Entwicklungsaufwand vorangeht, lassen sie sich zu winzigen digitalen Bomben von nur einigen wenigen Kilo- oder Megabyte verdichten, die nur ein einziges Mal an irgendeiner Peripherie eines Netzwerks erfolgreich angebracht werden müssen, um sich von dort aus an jeden anderen Knotenpunkt weiterzuverbreiten.

Das beste Beispiel hierfür ist die unlängst von der US-Regierung bekanntgegebene „Operation Buckshot Yankee". Auf dem Parkplatz einer US-Militärbasis im Mittleren Osten wurde ein USB-Stick gefunden („verlorene" USB-Sticks sind ein klassischer Angriffsvektor). Der Finder steckte ihn in einen Laptop, um den Besitzer zu ermitteln – und installierte unwissentlich „agent.btz", ein von einem ausländischen Nachrichtendienst entwickelter Computerwurm, dem es in den folgenden 14 Monaten gelang, fast das gesamte US-Militärnetz zu infiltrieren. „agent.btz" verbreitete sich im Pentagon, in Militärbasen und Rüstungsfirmen ebenso rasant wie unbemerkt und ermöglichte seinen Urhebern den Diebstahl gigantischer Mengen geheimer Informationen. „Operation Buckshot Yankee" gilt inzwischen als der größte Spionageakt der US-Militärgeschichte.

Verglichen mit Spionage und Geheimnisverrat im analogen Zeitalter lässt sich im Informationszeitalter also ein deutlicher Sprung beobachten. Dieser Sprung ist keine unbeabsichtigte Nebenwirkung, sondern das direkte Resultat der Kernfunktionen der Informationstechnik. Sie soll ja alles einfacher, effizienter, zugänglicher machen. Diese Vorzüge können dann aber eben auch von Angreifern genutzt werden.

Das Problem der hohen Wirkasymmetrie gilt für Sabotageangriffe und elektronische Attacken auf weniger vernetzte IT-Systeme. Ein kleiner Nadelstich kann einen systemweiten Kollaps bewirken – auch hier vorausgesetzt, er ist geschickt gebaut. Die Entwicklung kleiner und unauffälliger, gleichzeitig aber hocheffizienter und sich gezielt verbreitender Angriffe ist aufwändig. Wald- und Wiesenhacker müssten schon großes Glück haben, um lange unentdeckt zu bleiben, ihre Schadprogramme in gut gesicherten Systemen zu verbreiten und vor allem dauerhafte Schäden an kritischen Strukturen anzurichten. In diesen Fällen hält die IT-Grundsicherung; das ist ein wichtiges Argument gegen vorschnelle Schreckensszenarien von Cyberterroristen. Für Militärdienste aber ist diese aufwändige Entwicklung kein Problem. Sie verfügen über die notwendigen Ressourcen, um kleine Angriffe so zu gestalten, dass sie große Wirkung zeitigen.

> Cyberattacken von Militärdiensten sind effizienter und raffinierter als die üblichen Hackerangriffe

Hinzu kommt ein weiteres Prinzip: Angreifer haben oft die Möglich-

keit, in aller Ruhe viele kleine Variationen ihrer Attacken durchzuführen.

Die betroffenen Systeme erkennen erfolglose Angriffe meist nicht, und selbst wenn sie es tun, sind sie für gewöhnlich nicht in der Lage, den Angreifer effektiv auszuschalten. Nur einer der vielen Versuche des Angreifers muss zum Erfolg führen. Der Verteidiger dagegen muss das System viele hundert bis tausend Mal erfolgreich verteidigen. Neben der hohen Wirkasymmetrie gilt also auch eine deutliche Asymmetrie in der Fehlertoleranz, die den Schutz von IT-Systemen zusätzlich erschwert: Angreifer dürfen tausende Fehler machen, Verteidiger keinen einzigen.

In der Komplexität der heutigen IT-Systeme ist es ein Leichtes, Attacken geschickt zu tarnen

Angriff im Verborgenen

Ein drittes Prinzip erwächst aus der hohen Komplexität informationstechnologischer Systeme. Windows Vista etwa enthält 86 Millionen Zeilen miteinander interagierender Befehle – eine schier unbeherrschbare Menge, die noch von vielen weiteren Programmen, von Anpassungen und Hardware-Komponenten ergänzt wird. Für Angreifer bietet diese Datenmenge zahlreiche Möglichkeiten, unerwartete Einfallswege einzuschlagen (so genannte „Zero-Days“) und Angriffe zu tarnen. Geschickte Hacks können mit einigen hundert Befehlszeilen auskommen und sind daher leicht zu verstecken.

Ein weiteres Problem der Erkennung ist die Isomorphie, also die Gleichgestalt von Gut und Böse. Angreifer verwenden die gleichen Begrifflichkeiten wie die nominellen Funktionen. Das erschwert ihre frühzeitige Enttarnung zusätzlich. Latent droht also immer das Versagen über die Zeit oder im entscheidenden Moment, was als unmittelbare Folge eine Agnosie produziert – ein chronisches Unwissen über die Integrität der informationstechnischen Systeme. Vertrauen und sichere Entscheidungen werden damit dauerhaft untergraben.

Diese Probleme sind weitgehend unbeherrschbar, da es sich um reguläre beziehungsweise notwendige Systemmerkmale handelt. Schaltet man sie aus, schaltet man das System aus. Ihre Folgen kann man zwar auf die eine oder andere Weise in den Griff bekommen – mit einer drastisch erhöhten IT-Sicherheit, mit teuren und umfänglichen Prüfverfahren und besserer, schmalerer Software-Entwicklung. Doch diesen Maßnahmen sind enge Grenzen gesetzt, und „beherrschbarer“ bedeutet definitiv nicht „beherrschbar“.

Diese Sachzwänge stellen nun die passive Abwehr von IT-Systemen vor einige Probleme, denn effektiver Schutz setzt natürlich voraus, dass der Charakter einer Attacke bekannt ist. Nur dann kann die Aufstellung eines Schutzperimeters erfolgen. Um eine schädliche Wirkung abzufangen, muss man diese erst einmal kennen. Das ist aber wegen der Komplexität vernetzter Systeme und der hohen Wirkasymmetrie kaum möglich.

Die Angriffe erfolgen auf verschiedenen Wegen: gefälschte oder bereits im Original fingierte Chips und Bauteile in Rechnern, manipulierte Software, Insider mit kleinen Datenträgern und dem Wissen zur manipulativen Reprogrammierung. All diese Ein-

Nadel im virtuellen Heuhaufen: IT-Systeme bestehen aus Millionen von interagierenden Befehlen – es ist nahezu unmöglich, Cyberattacken frühzeitig aufzudecken

bruchsarten wurden bereits beobachtet und sind äußerst schwer zu verhindern. Fazit: Ein zuverlässiger passiver Schutz ist prinzipiell unmöglich. Diese Einsicht hat sich auch in den USA durchgesetzt, wo massiv zu diesem Thema geforscht wird. Im jüngsten „Technology Horizons"-Bericht der US-Air Force wurde Cyberdefense als nicht länger realistisch eingestuft und abgehakt.

Schutz und Bestrafung

Umso wichtiger ist also die zweite Abwehrstrategie: der präventive Schutz über die Steuerung des Angriffsverhaltens durch Strafandrohung. Auch hier gelten allerdings notwendige Bedingungen. Eine ist, dass Angreifer identifizierbar sein müssen. Die Identifikation der Angreifer ist aber unmöglich, was auf einige weitere Prinzipien der Cyberkriege zurückzuführen ist.

Zunächst ist die Flüchtigkeit der physischen Spuren zu nennen, welche die forensische Identifikation eines Angreifers erschwert. Wenn ein kleiner Nadelstich in einem komplexen soziotechnischen (also aus Mensch, Organisation und Technik bestehenden) System genügt, dann hinterlässt der Angreifer auch nur eine geringe Menge an physischen Spuren. Beim „Buckshot Yankee"-Vorfall sowie dem Computerwurm Stuxnet handelte es sich um ein paar handelsübliche USB-Sticks. Die wenigen physischen Spuren, die dabei entstehen, können Nachrichtendienste außergewöhnlich gut kontrollieren. So hat man natürlich auch auf dem Buckshot Yankee-Stick keine DNA-Spur und keinen Fingerabdruck gefunden.

Die Flüchtigkeit der physischen Spuren gilt erst recht für Angriffe im Internet. Zwar lassen sich zunächst auch dort reale Spuren festmachen – etwa ein Datenspeicher, der mit einem Schadcode beschrieben wurde. Allerdings ist so ein Schadcode, der im Internet transportiert wird, immer nur

für eine kurze Zeit physisch. Er besetzt eine Zeitlang einen realen physischen Datenspeicher, wird danach aber an einen anderen Speicher weitergegeben, während der originäre Speicher freigegeben und mit neuen Informationen bespielt wird. Die physischen Spuren des Schadcodes gehen dann unwiderbringlich verloren. Hier liegt die Flüchtigkeit also im Arbeitsprinzip der digitalen Technik, in der Virtualität selbst begründet: Information ist nicht dauerhaft physisch, sondern immer diskret und flüchtig.

Daten sind Märchen

Anhand ihrer physischen Spuren können Aggressoren also nicht identifiziert werden. Theoretisch bleiben den Forensikern noch die Datenspuren, der Informationsinhalt des Schadprogramms. An dieser Stelle kommt aber eine weitere Besonderheit von Cyberangriffen ins Spiel: Datenspuren sind vollständig manipulierbar. Ein Schadprogramm ist immer eine „geschriebene Geschichte“, die von ihrem Autor, dem Programmierer, von Anfang bis Ende frei gestaltet werden kann. Bei ausreichender Fachkenntnis sind diese Informationen sogar lange nach der ersten Angriffswelle noch manipulierbar. Auch hier liegt die Ursache in der Struktur digitaler Technologie selbst. Daten sollen schließlich veränderbar sein. Man kann versuchen, einen Absender technisch festzusetzen, indem man ihm etwa einen digitalen Absenderstempel aufsetzt. Doch sobald ein Hacker den Festsetzungsmechanismus durchbricht, kann er den Absender nach Belieben verändern. Die Manipulierbarkeit der Datenspuren hängt also letztlich vom technischen Knowhow des Angreifers ab, das beim Militär hoch anzusetzen ist.

Eine Besonderheit von Cyberangriffen ist die Manipulierbarkeit des Schadprogramms

Dass sich der „erzählte“ Charakter des feindlichen Programms auf die Rückverfolgung des Urhebers auswirkt, zeigt Stuxnet. Die IT-Sicherheitscommunity ist sich aufgrund ihrer technischen Analysen sicher, dass es sich um einen gegen den Iran gerichteten Cyberangriff handelte. Ihrer Ansicht nach spricht vor allem die Verbreitung des Wurms in iranischen IT-Systemen sowie dessen Funktion der potenziellen Störung von Zentrifugen dafür. Das mögen deutliche Indizien sein.

Doch Stuxnet enthielt auch andere Funktionen, die nicht zu einem gezielten Angriff auf den Iran passten. So war etwa die weltweite Verbreitung des Wurms außergewöhnlich hoch, obwohl der Propagationsmechanismus begrenzt war. Indizien wie dieses sprechen für andere Nutzungen, etwa für einen Waffentest. Fragt man nach dem altrömischen „Cui bono“-Prinzip, wem Stuxnet überhaupt nützt, kämen dann aber ganz andere mögliche Urheber ins Spiel als bei einer Manipulation der iranischen Zentrifugen. Fast alle Nationen bauen derzeit Cyberwar-Offensivprogramme auf. Für jedes von ihnen wäre ein Feldtest außerordentlich wertvoll. Man weiß dann, was die eigenen Truppen können, wo man mit so einem Angriff überall landen kann, wie die Propagation verlaufen ist, wie die Reaktionen aussehen. So lassen sich die weiteren, auszubildenden Fähigkeiten wesentlich präziser gestalten. Eine große Kostenersparnis und zudem auch eine beeindruckende De-

monstration. Dann wäre es sogar möglich, dass die gesamte Iran-USA-Indizienkette nichts weiter ist als eine aufwändig gelegte falsche Fährte, eine „False-Flag"-Operation. Wenn man bedenkt, dass das Waffentest-Szenario auch katastrophale Ausfälle von zivilen Systemen zur Folge hätte, klingt die These der falschen Fährte nicht einmal unwahrscheinlich.

Auch eine kontextuelle Analyse von Cyberangriffen, die über den Nutzen und den strategischen Rahmen des Angriffs Schlüsse zu ziehen versucht, ist also vom märchenartigen Charakter der Datenspuren betroffen. Natürlich darf man spekulieren. Doch durch den „erzählten" Charakter des feindlichen Programms ist jedes Spekulieren ein Fabulieren. Dies ist eine wichtige Einsicht für die internationalen Beziehungen, die Diplomatie und das Militär. Daten und ihre vermeintlichen Kontexte allein beweisen überhaupt nichts. Hier muss auch zur Vorsicht im Umgang mit der IT-Sicherheitscommunity geraten werden; diese positioniert sich gerne als möglichst exklusiver Ansprechpartner. Ihre Analysen waren allerdings bisher konsequent eindimensional und naiv, was daran liegt, dass IT-Experten in der Regel das strategische und sicherheitspolitische Denken fehlt. Sie ziehen ihre Schlüsse aus dem reinen und unter Umständen manipulierten Datenbild.

Die Lücke zwischen Mensch und Maschine, Finger und Tastatur: Ob ein Computer von einem Teenager, Hacker oder staatlich beauftragten Datenspion genutzt wurde, ist kaum zu rekonstruieren

Der Mensch-Maschine-Gap

In diesem Zusammenhang ist noch ein weiteres Merkmal moderner Cyberkriege zu nennen, und zwar der „Gap" (also die Lücke) zwischen Mensch und Maschine. Sie gilt für Cyberattacken aller Art, ist aber besonders in der Diskussion um eine bessere Identifikation von Aggressoren im Internet relevant. Denn selbst wenn man es dank einer völligen Neukonzeption des Internets schaffen sollte, jeden Angriff eindeutig bis zu einer Maschine zurückzuverfolgen (was an sich bereits unglaublich teuer und auf-

grund der zuvor beschriebenen Schwierigkeiten unrealistisch ist), wäre noch lange nicht geklärt, wer diese Maschine mit welchem Motiv bedient hat. Ob Hacker, Krimineller, Teenager, staatlich beauftragter Datenspion, ob mit einer dezidierten Absicht oder aus Naivität und Unwissen, ob Deutscher, Polynesier, Amerikaner – all diese für die rechtliche Bewertung wie für den Beschluss von Maßnahmen essentiellen Informationen fehlen. Sie verlieren sich vollständig in der winzigen Lücke zwischen Mensch und Maschine, dem Zwischenraum zwischen Finger und Tastatur. Dies ist eine der größten Plagen des Cyberwar, denn diese Lücke kann unmöglich durch technische Maßnahmen geschlossen werden.

Schließlich greift noch ein letztes Prinzip: Die im Cyberkrieg eingesetzten Waffen sind alltäglich. Es handelt sich um handelsübliche Technologien wie gewöhnliche Rechner, Standard-USB-Sticks oder reguläre Programme sowie um gängige Programmierkenntnisse. Das erschwert die Verfolgung anhand bestimmter technischer Einzelteile oder anhand der Profile bestimmter Experten wie etwa bei der nuklearen Proliferation. Auch die präventive Eindämmung oder eine Ächtung von Cyberwaffen ist unter diesem Gesichtspunkt schwierig. Ein über das Internet transportierter Angriff kann etwa aus einem Internet-Café, von einem gestohlenen Handy aus oder einfach aus einem Büro gestartet werden, in das eingebrochen wurde. Selbst bei höchsten Überwachungsstandards wäre also mit der Identifizierung der für den Cyberangriff verwendeten Maschinen absolut nichts gewonnen. Man kann damit sicher den einen oder anderen marodierenden Teenager oder Kleinkriminellen überführen. Aber in einem auf hohem technischen Niveau geführten Cyberkrieg ist auf diese Weise nichts gewonnen. Die hohe Flüchtigkeit der physischen Spuren, der märchenartige Charakter der Datenspuren, der Mensch-Maschine-Gap sowie die Alltäglichkeit der Waffen machen also jede Zuschreibung – und damit jede rechtliche Regulierung sowie militärische Gegenschläge – unmöglich.

Die im Cyberkrieg eingesetzten Waffen: gewöhnliche Rechner, USB-Sticks, reguläre Programme

Rückbau und „Entnetzung“

Die skizzierten sieben Prinzipien sind wichtige Strukturmerkmale moderner Cyberkriege. Sie lassen sich teilweise mildern, sind aber nie ganz aufzuheben und in einigen Teilen schlicht unumgehbar. Daraus folgt, dass man sich weder passiv noch aktiv einigermaßen solide gegen Cyberangriffe schützen kann – zumindest nicht, wenn der Ist-Zustand der Informationstechnologie beibehalten wird. Sicherheitsexperten wenden hier zwar ein, dass es ohnehin keine hundertprozentige Sicherheit gebe. Aber das Argument gilt in diesem Fall nicht. Die Probleme sind so virulent, dass man eigentlich nur sagen kann, dass die Sicherheit weder bei null noch bei hundert Prozent liegt. Ob sie aber zehn, zwanzig, siebzig oder achtzig Prozent beträgt, ist offen. Gegenüber hocheffizienten Angreifern sollte man sie auf jeden Fall lieber niedrig ansetzen.

Die einzig zuverlässigen Maßnahmen sind der Rückbau dieser Technologie – vor allem eine „Entnetzung“

und „Entinformatisierung“ – und ein Neubau besonders wichtiger Systeme nach rigorosen Sicherheitskonzepten, von denen viele erst noch auf Anwendungsniveau entwickelt werden müssen. Abwehrzentren allerdings sind nur wenig hilfreich. Sie könnten keine militärischen Angriffe rechtzeitig aufdecken, denn diese sind zu hoch entwickelt, um mit gängigen Schemata erfasst zu werden.

Auch der Gedanke, mit einem Abwehrzentrum schnell reagieren zu können, scheint paradox, wenn man weiß, dass die meisten komplexen Angriffe erst nach Jahren entdeckt werden. Und selbst wenn ein Cyberangriff enttarnt wird – an die Hintermänner ist im Regelfall kein Herankommen. Die Nachrichtendienste hinterlassen keine physischen Spuren und alle Datenspuren sind manipulierbar. Ein Cyberabwehrzentrum könnte allenfalls eher harmlose Attacken abfangen und Konzepte für Krisenmanagement entwickeln. Das allerdings wird bereits zuverlässig und auf technisch hohem Niveau durch das Bundesamt für Sicherheit in der Informationstechnik geleistet. Die Gründung eines neuen Abwehrzentrums deutet also darauf hin, dass das Phänomen noch nicht in seiner Tragweite verstanden wurde.

Kriegerische Handlungen ohne irgendeine Möglichkeit des Schutzes, der Regulierung oder der Vergeltung sind ein neues Paradigma, dessen Konsequenzen erst langsam und nur widerwillig erkannt werden, weil sie unangenehm sind: Ohne Regulierung und effektiven Schutz ist grundsätzlich jeder in der Lage, jederzeit und unbeeindruckt von rechtlichen Konsequenzen Cyberangriffe durchzuführen. Aus philosophischer Sicht ist das eine hochspannende Situation. Erstmals befindet sich die Welt in einem sonst immer nur hypothetisch gedachten Zustand, dem Naturzustand: ein gesellschaftliches Zusammensein ohne jede Sanktionsmöglichkeit, ohne den Leviathan. Die Zeit wird zeigen, welche Folgen dieser Naturzustand nach sich zieht. Ob sich einige Menschen wie oft prognostiziert an die Kehle gehen oder ob sie sich trotz fehlender Sanktionsmöglichkeiten des eigenen Vorteils auf Kosten Anderer enthalten, ist offen.

Krieg ohne irgendeine Möglichkeit des Schutzes ist ein neues Paradigma, das nur widerwillig anerkannt wird

Für die Sicherheitsdebatte sollte der reale Ausgang dieses Experiments allerdings irrelevant sein. Auf Cyberangriffe muss reagiert werden. Und als Arbeitsgrundlage für die Sicherheitspolitik genügt das Risiko; es erfordert ein ebenso rasches wie informiertes Handeln. Eine solide Kenntnis der neuartigen Cyberkriege und ihrer Besonderheiten ist also unerlässlich. Der Krieg der Rechner muss als neues Phänomen verstanden werden. Dazu gehört zunächst einmal die Einsicht in die strukturellen Besonderheiten und in die daraus folgende Notwendigkeit einer teilweisen „Entnetzung“.

Dr. SANDRO GAYCKEN ist Technik- und Sicherheitsforscher an der FU Berlin und Experte für Cyberwar und Informationsgesellschaft.