# Angriff aus dem Netz

**Hoch entwickelte Computerviren zeigen: Viele Länder bereiten sich auf den Cyber-Krieg vor. Die Attacken können jeden treffen, der einen Internetanschluss hat.** *Von Eugene Kaspersky*

Cyber-Krieg – der Begriff dringt langsam ins öffentliche Bewusstsein. Im Jahr 2010 störte der Computerwurm Stuxnet den Betrieb iranischer Atomanlagen, gefolgt ein Jahr später von seinem verwandten Duqu, dann kam der Spionage-Virus Flame – und kürzlich entdeckten wir Gauss, eine Software, die offenbar in staatlichem Auftrag Bankdaten im Nahen Osten ausspähte. Hoch entwickelte Schadprogramme sind dies; sie stehen für den relativ neuen Trend des Cyber-Kriegs, bei dem Staaten Computerprogramme als Waffe gegen andere Staaten verwenden.

Solche Cyber-Angriffe können lebenswichtige Infrastruktur sabotieren – Stauseen, die Flugverkehrskontrolle oder die Nahrungsmittelkette – und so katastrophale Folgen haben. Jede moderne Infrastruktur ist in einem hohen Grad computergesteuert und vernetzt. Als Folge der Globalisierung ist die Technologie für diese Infrastruktur weltweit identisch. Somit ist sie überall anfällig für Cyber-Angriffe. Sogar das angreifende Land kann zum Opfer seiner eigenen Waffen werden; dann spricht man vom Boomerang-Effekt.

Die Anonymität der Cyber-Waffen macht es praktisch unmöglich, den Angreifer ausfindig zu machen. Es lässt sich nie sicher feststellen, wo und in wessen Auftrag sie entwickelt wurden. Manchmal glaubt man, Hinweise aus Kommentaren herauslesen zu können, die Programmierer im Quellcode hinterlassen haben. Oder man schaut, wem der Angriff nutzt – Beweise sind das nicht. Was wir jedoch wissen, ist, dass der Einsatz von Cyber-Waffen zunimmt, und dass nicht nur Kriminelle und Terroristen solche Software entwickeln, sondern auch staatliche Stellen. Zuverlässige Indizien dafür sind der hohe Entwicklungsgrad der Cyber-Waffen; dafür braucht es Budgets in Millionenhöhe. Die Kriegsführung im Internet ist offenbar extrem gut finanziert. Auch dass immer wieder neuartige Cyber-Waffen entdeckt werden, deutet darauf hin, dass Geheimdienste und wohl auch Armeen ihre traditionellen Einsatzbereiche erweitern. Das Internet wird immer stärker militarisiert.

Daher sollten Regierungen Verantwortung übernehmen und sich auf Kontrollen für Cyber-Waffen einigen. Denn wenn Regierungen diese Waffen unvermindert entwickeln, werden sie wahrscheinlich eines Tages in die Hände von Terroristen gelangen. Es genügt ein Fehler, dass Details einer Cyber-Waffe bekannt werden. Danach ist es einfach, die Technologie zu stehlen, zu kopieren und anzupassen, sodass plötzlich irgendjemand eine neue Cyber-Waffe in der Hand hält.

Aus meiner Sicht gibt es nur eine Möglichkeit, Cyber-Kriege abzuwehren: internationale Kooperation. Man sollte eine Internationale Cyber-Sicherheitsorganisation (ICSO) schaffen, nach dem Vorbild der Internationalen Atomenergiebehörde IAEA. Sie könnte eine unabhängige Plattform für eine weltweite Zusammenarbeit sein, deren Ergebnis dann Verträge zur Kontrolle von Cyber-Waffen wären – so, wie die IAEA Atomwaffen überprüft, wie andere internationale Verträge chemische oder biologische Waffen kontrollieren. Wenn eine solche ICSO die weltweite Gemeinschaft der IT-Sicherheitsforschung vereint, könnte sie Zwischenfälle mit Cyber-Angriffen am besten untersuchen. Natürlich müssen wir realistisch bleiben: Die ICSO könnte Cyber-Waffen nicht völlig abschaffen. Aber sie würde zumindest die derzeitige Situation enorm verbessern.

Doch eine weltweite Cyber-Behörde ist bislang ein Wunschtraum geblieben. Es wäre kompliziert, alle wichtigen Staaten an den Verhandlungstisch zu bringen. Noch schwieriger wäre es, sämtliche Staaten dazu zu bringen, sich auf Spielregeln zu einigen. Einige Staaten wollen nicht den hart erkämpften Vorsprung bei Investitionen und Fachkenntnis aufgeben. Vielleicht, weil sie ihn bereits nutzen, vielleicht, weil sie ihn künftig nutzen wollen.

## Schadprogramme gehören genauso kontrolliert wie Atomwaffen

Letztlich müssten die führenden Industrieländer die Initiative für eine Cyber-Kooperation ergreifen. Sie haben vermutlich die am weitesten entwickelten Programme – sie sind aber auch am stärksten von Cyber-Angriffen bedroht, denn sie haben die höchste Dichte an Internet-Anschlüssen, die ein Einfallstor für solche Attacken sind.

Was können Länder derzeit unternehmen, um sich zu schützen? Zunächst einmal ist es für Staaten unmöglich, sich vollständig vor Cyber-Angriffen zu schützen. Dafür müsste praktisch der gesamte existierende Quellcode für Betriebssysteme neu geschrieben werden. Das ist viel zu teuer. Je mehr grundlegende Dienstleistungen ein Land online anbietet, desto schwieriger wird der Schutz vor Cyber-Angriffen. Viele dieser Dienstleistungen werden von lokalen Behörden vor Ort verwaltet. Diese haben womöglich unterschiedliche Instrumente oder sogar Strategien für ihre Sicherheit.

Der erste Schritt wäre daher, eine verbindliche nationale Sicherheitsstrategie zu entwickeln. Anschließend könnte man ein Risikomanagement entwerfen und Maßnahmen zur Cyber-Sicherheit auf die gesamte kritische Infrastruktur ausweiten. Schließlich braucht es flexible und intelligente Überwachungsmechanismen sowie eine verbesserte Bildung in allen Belangen der Cyber-Sicherheit.

Viele fragen, ob sich normale Haushalte oder Firmen wegen der steigenden Gefahr von Cyber-Kriegen Sorgen machen sollten. Als Antwort erwartet man ein Nein, schließlich wurden Stuxnet und andere Computerwürmer sehr präzise für den Einsatz im Nahen Osten entwickelt. Warum sollten dann Menschen in Ländern wie Deutschland beunruhigt sein?

Zunächst, weil die Nebenwirkungen solcher Programme die Infrastruktur auch in Europa treffen können. Und wenn Schadprogramme außer Kontrolle geraten, können sie über das Internet zu praktisch jedem Punkt der Welt gelangen. Das geschieht durch Dateien, die an E-Mails angehängt sind, durch unbeabsichtigtes Herunterladen von Software oder wenn USB-Sticks verwendet werden. Wer kann verhindern, dass ein Deutscher auf einer Dienstreise im Libanon einen USB-Stick mit einem Virus bekommt – und dann die Bilder von der Reise am Samstag beim Grillabend zeigt?

Unwahrscheinlich? Gewiss. Aber es genügt ja schon, wenn dieses Szenario ein einziges mal passiert. Und schon kann sich das Schadprogramm exponentiell um den Globus ausbreiten und jeden treffen, auch das Land, von dem der Angriff ausging. Jeden, das heißt: private Computernutzer, Firmen, Regierungen und ganze Länder. Denn angegriffen werden homogene Infrastrukturen, Betriebssysteme und Software, die wir täglich benutzen. Es ist der Angriff auf den Alltag.

Eugene Kaspersky, 46, der in Moskau Kryptografie studierte, ist der weltweit größte private Anbieter von Sicherheitssoftware. Sein Beitrag erscheint auch in der „Security Times“ zum Cyber Security-Gipfel in München.

ÜBERSETZUNG: JANEK SCHMIDT
FOTO: KASPERSKY LAB