Präventive Cyberattacken

Hauptkriegsziele des 21. Jahrhunderts sind Mikrochips und Megabytes

Martin Hellmann

Am Anfang ist es einfach nur ärgerlich. Der moderne vernetzte Bürger öffnet sein Postfach, um die E-Mails abzurufen, und er muss die wichtige Mitteilung seines Chefs oder die Einladung zur Dinnerparty mühevoll aus einem Wust von Spam-Mails herausfischen. An die hundertfachen Viagra-Werbungen in allen Schreibweisen, um die Spamfilter der gängigen Firewalls zu durchbrechen, hat man sich ja schon gewöhnt. Ebenfalls an die Einladungen ins Online-Casino oder die zahllosen dubiosen Kredit- und Jobangebote. In letzter Zeit treten auch vermehrt Massen-Spams auf, die man überhaupt nicht lesen kann, selbst wenn man es wollte, da sie nur asiatische Schriftzeichen enthalten. Wer Pech hat, für den ist die Flut irgendwann nicht mehr zu beherrschen. Jeder Mailabruf fördert Hunderte, wenn nicht Tausende solcher Müllsendungen zutage. Die regulären Mails gehen dazwischen fast unter. Und dann kommt sie – die unheimliche Stille. Nichts geht mehr. In diesem Augenblick ist es schon zu spät. Das Speicherlimit des Postfachs ist übergelaufen, die automatischen Sicherheitssysteme des Anbieters haben den Zugang gesperrt. Wer jetzt keinen guten Draht zu seinem Provider hat, dem bleibt nichts übrig als seine E-Mails abzuschreiben und zu einem anderen Anbieter umzuziehen. Meist hat man dann für einige Zeit Ruhe. Viele Menschen haben so etwas schon erlebt, aber kaum jemand stellt sich die entscheidende Frage: Was wäre, wenn das Ziel der Attacke nicht ein E-Mail-Postfach wäre, sondern eine Computerfestplatte, und wenn der Adressat nicht der einfache Postangestellte aus Hückelhoven wäre, sondern die Frankfurter Börse? Der Londoner Flughafen? Ein Atomkraftwerk? Die Bedrohung durch den Cyberkrieg wird in der Bevölkerung nach wie vor unterschätzt. fb

Längst ist das Internet weltweit zu einem neuen Kriegsschauplatz geworden, der in den Schlagzeilen der Medien kaum auftaucht. Wie kürzlich bekannt wurde, waren die großen amerikanischen Zeitungen New York Times, Wall Street Journal und Washington Post über fast vier Monate das Ziel von Internet-Angriffen aus China. Wie das Department of Homeland Security der USA mitteilte, war auch ein Elektrizitätskraftwerk in Amerika vier Wochen lang lahmgelegt worden. Das Ministerium kündigte an, man werde sich selbst zukünftig verstärkt an der Cyber-Kriegführung beteiligen, und zwar auch präventiv.

Leider sind solche Attacken nicht nebenwirkungsfrei. Als die USA den Computerwurm Stuxnet in eine iranische Nuklearanlage einschleusten, gelang es der schädlichen Software, durch Lücken im Sicherheitssystem der befallenen Rechner ins Netz zu entweichen und sich dort millionenfach zu kopieren. Auf diese Weise konnten auch ganz unbeteiligte Bürger irgendwo auf der Welt Opfer des Online-Krieges werden.

Sicherheitsexperten großer Unternehmen zufolge wird sich dieser Trend im Jahre 2013 und danach noch verstärken. Wer glaubt, es gehe dabei lediglich darum, dass die Bürger ein paar harmlose E-Mails verlieren könnten, der unterschätzt die Gefahr gewaltig. Es ist, so die Meinung der Insider, nur eine Frage der Zeit, bis der lautlose Krieg auch Todesopfer fordern werde. *„Landesweite Attacken werden auf kritische Infrastruktur wie Energieversorgungssysteme zielen, und das schon 2013 in ungeahntem Maße“*, teilte Chiranjeev Bordoloi, CEO der US-Sicherheitsfirma Top Patch, dem Fernsehsender CNN mit. Leon Panetta, der damalige US-Verteidigungsminister, sagte bereits im Oktober 2012: *„Eine von Staaten oder gewaltbereiten Terroristen durchgeführte Cyberattacke könnte genau so zerstörerisch sein wie die Angriffe vom 11. September.“ Und der Minister fuhr fort: „Solch eine destruktive terroristische Attacke könnte eine ganze Nation paralysieren.“*

Die meisten von uns machen sich keine Vorstellung davon, auf welch fortgeschrittenem Stand die moderne Hacker-Technologie bereits ist. *„Es gibt Levels der Cyberkriegführung, die weitaus aggressiver sind als alles, was bisher im Krieg eingesetzt oder zum Einsatz empfohlen wurde.“*, sagte ein Offizieller, der ungenannt bleiben wollte, der New York Times.

Wie das Blatt weiter erfuhr, kann in den USA nur der Präsident solche Attacken anordnen. Er sei gesetzlich auch zu präventiven Angriffen über das Internet ermächtigt, kann auf diese Weise also andere Staaten angreifen, ohne dass die USA selbst zuvor angegriffen worden sein müssten.

Es ist bei den Medien umstritten, was von derlei Horrormeldungen zu halten ist. Da die meisten Informanten anonym bleiben, könnte es sich auch um ein gezieltes Informationsleck handeln, um in der Öffentlichkeit die Bereitschaft zu stärken, die Regierung zu weitergehenden Aktionen zu ermächtigen. Viele Verteidigungsministerien der westlichen Welt haben in den letzten Jahren neue Spezialabteilungen für Cyberkriegführung gegründet, und während sonst allenthalben die Verteidigungsetats zusammengestrichen werden, ist dies ein Bereich, der nach wie vor expandiert.

Auch der Finanzsektor bleibt von der Entwicklung nicht verschont. Es gab bereits Cyberattacken zur Manipulation der Märkte, einige sogar mit dem offensichtlichen Ziel, selbst damit Geld zu verdienen, teilte Sandro Gaycken mit, ein Computerwissenschaftler an der Freien Universität Berlin. Dies nehme bereits gewaltsame Ausmaße an, ebenso seien chemische Attacken und gezielte Gasexplosionen im Bereich des Möglichen. „Relativ leicht“ sei es auch, auf diese Weise Flugzeuge zum Absturz zu bringen. Moderne Flugzeuge seien heute abhängig von einer reibungslosen Kommunikation mit den Computernetzwerken der Bodenstationen, und die haben höchst unterschiedliche Sicherheitsstandards. Derartige Systeme zum Absturz zu bringen, ist für einen Experten nicht schwer.

Dave Clemente vom britischen Think Tank Chatham House wies darauf hin, dass in diesem Zusammenhang die speziell von den USA immer wieder geäußerten Forderungen nach ungehinderter Freiheit und Transparenz im Internet heuchlerisch seien. Es gehe dabei weniger um die Informationsfreiheit des einzelnen Bürgers als vielmehr darum, für den Cyberkrieg geeignete Freiräume zu schaffen. ■