Aleksandra Sowa

Vom Hacktivismus zum Cyberkrieg

Neue Formen politisch motivierter Angriffe im Netz

»Life is nothing but a competition to be the criminal rather than the victim«, stellte Bertrand Russell fest – lange vor dem Start des Wettrennens um die Oberhand bei Cyberkrieg, -terrorismus und -vandalismus. Das Internet wird mehr und mehr der Austragungsort politischer, wirtschaftlicher oder militärischer Konflikte.

Aleksandra Sowa

leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst Görtz Institut für Sicherheit in der Informationstechnik. Sie ist Autorin zahlreicher Fachpublikationen und aktuell in einem großen Telekommunikationskonzern tätig.

Stellen Sie sich vor, Sie melden sich wie immer in Ihrem E-Mail-Postfach an. Sie rufen die Domain www.google.com auf und tragen dort Login-Daten sowie das Passwort ein. Wie gewohnt lesen und beantworten Sie nun Ihre Mails und loggen sich wieder aus. Unverhofft läuft wenig später folgende Meldung über Google über den Newsticker: Eine SSL-Zertifikate ausstellende Organisation *(Certification Authority)* wurde von Hackern attackiert. Die Angreifer sind in die Systeme des Ausstellers dieser »digitalen Ausweise« eingedrungen und stellten sich dort falsche Zertifikate aus – unter anderem auch eines für die Domains von google.com. (Zur Erklärung: Mit einem SSL-Zertifikat wird gegenüber den Internetbrowsern die Authentizität und Integrität einer Domain bestätigt.)

In diesem Moment ahnen Sie womöglich noch nicht, was das für Sie, Ihren Mail-Account und die dortigen Informationen bedeutet. Möglicherweise ist es für Sie tatsächlich irrelevant – allerdings nur solange Sie kein iranischer Dissident sind, für den die Vertraulichkeit der Informationen und Personen, die Sie über den betroffenen Account kontaktieren, unter Umständen lebensentscheidend ist.

Zu genau diesem Vorfall kam es im Sommer 2011. Anonyme Angreifer drangen in die Systeme des niederländischen Zertifikatsausstellers DigiNotar ein, um sich zahlreiche falsche Zertifikate für google.com und weitere Internetdomains auszustellen. Mit einem falschen Zertifikat kann den Internetnutzern per Umleitung des Internetverkehrs ein Google-Mailserver (GMail) im Iran vorgetäuscht werden. Der Vorfall wurde nach seiner Entdeckung von unabhängigen Experten untersucht und geht als »Operation Black Tulip« (Operation schwarze Tulpe) in die Geschichte ein.

Dies ist kein Einzelfall. Die Attacken auf die Zertifikate ausstellenden Organisationen, die sich gezielt auf die im Iran betriebenen Internetdomains richten, lassen eine politische Motiviertheit vermuten: »It's likely that the government of Iran is using these techniques to monitor local dissidents« – wird von Experten behauptet.

Politisch motivierte Attacken nehmen laut *McAfee Thread-Report* jährlich zu. Ihre Art hat sich jedoch grundlegend gewandelt.

Auch »Hacktivismus« genannt, erscheinen diese Attacken im Gegensatz zu professionellem Hacking häufig als technisch simpel. Bei Hacktivismus steht weder die Methode im Vordergrund noch – wie oft beim

traditionellen, technisch oder wirtschaftlich motivierten Hacking – der Wunsch zu beweisen, dass man dazu in der Lage ist. Die politische Botschaft steht für die Hacktivisten im Vordergrund. Es werden neue Plattformen und Modelle des Online-Protestes getestet, wie z.B. elektronische »Sitins«, gegen politische und wirtschaftliche Organisationen gerichtete Spam-Aktionen, Blockaden, Löschung oder Veränderung von Internetseiten oder Überlastung der Netzressourcen. Hauptziel der Hacktivisten ist es, Aufmerksamkeit zu erregen.

Diese Art politisch motivierter Attacken ist heute selten und findet kaum noch öffentliche Notiz. Inzwischen ist das Internet fast täglich der Austragungsort politischer, wirtschaftlicher oder militärischer Konflikte von ganz anderer Dimension.

2011 war ein Jahr prominenter Angriffe auf Behörden, Regierungen und Staatsverwaltungen. Fast täglich konfrontieren Medien die Öffentlichkeit mit derartigen Meldungen. Nach Erkenntnissen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden durchschnittlich fünf gezielte Angriffe täglich auf Personen als Nutzer des Regierungsnetzes detektiert und abgewehrt. Laut BSI können öffentliche Stellen oder kriminelle Organe die Urheber sein.

Neben den Webservern von Parteien, Verwaltungen und öffentlichen Organisationen sind auch jene von privatwirtschaftlichen Unternehmen heute das Ziel derartiger Attacken. Wie das Beispiel des Wurms »Stuxnet« zeigt, zielen die Angreifer beispielsweise darauf ab, kritische Infrastrukturen eines Staates (Wasser- und Energieversorgung, Post, Telekommunikation, etc.) anzugreifen. Diese befinden sich in Deutschland fast alle in privaten Händen. So kann ein Angriff auf private Unternehmen sehr schnell eine Bedrohung der öffentlichen Sicherheit darstellen.

Die politisch motivierten Attacken entladen sich heute in hoch spezialisierten und technisch ausgereiften Angriffen, bei denen von Cyberkriminalität, -spionage oder -terrorismus die Rede ist.

Die aufgedeckten und medial aufgearbeiteten Fälle sind aber nur die Spitze des Eisbergs. Interessanter sind die Attacken, die nicht öffentlich werden. Ist das Ziel des Angriffs politische bzw. wirtschaftliche Spionage oder Sabotage, so legen die Angreifer großen Wert darauf, nicht entdeckt zu werden und keine Aufmerksamkeit zu erzielen.

Der im Herbst 2011 vom Symantec entdeckte und analysierte »Duqu-Wurm« dient als hervorragendes Beispiel für diese Vorgehensweise. Duqu wurde unter anderem bei Herstellern von Industrieanlagensteuerungen entdeckt und war auf den Diebstahl von Betriebsgeheimnissen sowie die Ausspähung von Informationen für weitere Angriffe ausgelegt. Um bei der Installation unentdeckt zu bleiben, aktivierte sich der Wurm erst 15 Minuten nach der ersten Ausführung und »spionierte« das infizierte System wochenlang aus. Nach 36 Tagen löschte sich die Software selbstständig und verwischte ihre Spuren.

»The motivations of vandals are different from those of criminals, and these of warriors are very different from those of criminals«, stellt der IT-Experte Steven Ross fest. Es sind nicht die Cyber-Kids oder Hobby-Hacker, die diese Schadsoftware entwickeln oder in Systeme einbrechen, um Anerkennung zu ergattern oder Schaden anzurichten. Heutzutage verfolgen gut organisierte und professionell ausgerüstete Gruppen politisch und wirtschaftlich motivierte Ziele. Dabei agieren sie nicht selten im Auftrag Dritter.

Hinter den prominenten Attacken auf Behörden, Unternehmen und Organisationen, zu denen auch die US-Amerikanische Firma Citigroup und der Internationale Währungsfonds (IWF) gehören, werden oftmals Regierungen oder regierungsnahe Organisationen vermutet. Auch deswegen, weil zu den Opfern Organisationen gehören, die auf nationaler und internationaler

Ebene zu den größten und mächtigsten zählen. Technische Infrastrukturen solcher Organisationen sind darauf ausgerichtet, ihre kritischen und sensitiven Informationen entsprechend dem neuesten Stand der Sicherheit und Technik zu schützen. Dass dennoch in ihre Systeme eingebrochen wurde, belegt die besonderen Fähigkeiten und die exzellente Ausstattung der Angreifer.

Neue Cyberstrategien

Aufgrund des Umstandes, dass die Regierungen Kompetenzen entwickeln und fördern, um für einen möglichen Cyberkrieg gewappnet zu sein, werden die Fähigkeiten und Möglichkeiten, derart spezialisierte Attacken durchzuführen, in der Hauptsache den staatlich finanzierten und regierungsnahen Organisationen zugetraut. Der Chef des US Strategic Command, General Kevin P. Chilton, kündigte an, dass im Fall einer Cyberattacke auf die USA »the law of armed conflict will apply«. Zahlreiche Staaten bereiten sich auf einen Cyberkrieg vor und verfügen über die technischen und finanziellen Mittel dafür. So wird in den USA aktuell erneut eine Cyberstrategie entwickelt; in Deutschland wurde 2010 das Nationale Cyber-Abwehrzentrum (NICAZ) gegründet, um Bedrohungen aus dem Internet abzuwehren; mit der »European Network and Information Security Agency« (ENISA) gründete die EU bereits im Jahr 2003 ein Amt für Cybersicherheit, das aktuell neu ausgerichtet wird.

Auf doktrinaler Ebene unterscheidet man folgende drei Formen von Cyberkrieg: Computer Network Attack (CNA), Computer Network Exploitation (CNE) – die Fähigkeit, gegnerische Netzwerkkapazitäten zu zerstören bzw. auszuspähen – und Computer Network Defense, Maßnahmen zur Abwehr von CNA und CNE. So ist die Gefahr von Cyberattacken zugleich der Antrieb für die Staaten und Regierungen, eigene Kompetenzen auf diesem Gebiet zu erweitern. Diese können sowohl zur Abwehr gegen potenzielle Angriffe durch andere Staaten, als auch offensiv bzw. präventiv eingesetzt werden, wie das Beispiel des sogenannten Bundestrojaners zeigt.

Die negative Berühmtheit, die früher durch die Hacktivisten und heute durch die professionellen, politisch und wirtschaftlich motivierten Cyberattacken erzeugt wird, lässt den Ruf verschiedener regierungsnaher Gremien und Organisationen, Behörden, Geheim- und Nachrichtendienste nach größeren Budgets und verbesserten Zugriffsmöglichkeiten auf die bislang geschützten Bereiche gerechtfertigt erscheinen. Da das Internet keine Staatsgrenzen respektiert, wird der Angreifer außerhalb aber auch innerhalb der eigenen Landesgrenzen vermutet. Auch Bürger des eigenen Landes geraten dabei unter Generalverdacht und die Diskussion darüber, ob die öffentliche Sicherheit oder die Bürgerrechte Vorrang haben, entflammt immer wieder. Zugleich wird der Ruf nach neuen Gesetzen und der konsequenteren Umsetzung bestehender Gesetze laut.

Bereits heute vermuten Experten, dass die Lösung der aktuellen Cyberprobleme – anders als im Kalten Krieg – eher auf Modellen der Kooperation als auf Wettbewerb basieren wird. Ein Umdenken – in Politik und Wirtschaft gleichermaßen – wird daher gefordert.

Als nicht ganz so folgenschwer wie vermutet wird inzwischen der Angriff auf DigiNotar und der Diebstahl von SSL-Zertifikaten für *.google.com beurteilt. Die Angreifer haben zahlreiche Spuren hinterlassen, die Rückschlüsse auf ihre Motivation und Herkunft zulassen. Die Attacke wurde der iranischen Regierung zugeschrieben – in entsprechenden Foren sollen sich die Angreifer bereits zu dem Angriff bekannt haben. Zum Glück, möchte man in diesem Fall sagen. So war es DigiNotar möglich, noch am selben Tag Gegenmaßnahmen zu ergreifen und die falschen Zertifikate zu deaktivieren. ■