Sicherheit im Netz?

Beim IT-Sicherheitskongress „IT-Defense“ 2014 in Köln wurde die Verletzlichkeit des Internets aufgezeigt. Es gibt jedoch kaum Alternativen.

Gibt es eine Alternative zum Internet in seiner jetzigen Form?“, fragte Marcus Ranum bei der IT-Defense 2014. Er verwies darauf, dass im Grunde eine technologische Vormachtstellung einer Nation bestehe, von der der Rest der Welt abhängig sei. Aber: Wer kann es sich leisten, ein eigenes Internet aufzubauen? Und selbst wenn das gelingen würde, müssten die Chips der Rechner neu entwickelt werden, um Hintertüren auszuschließen, die Zugriffe ermöglichen könnten.

„Man kann keinem Code vertrauen, den man nicht selbst entwickelt hat.“ Plausibler sei es, eine Art „Chinesische Mauer“ als Firewall um die IT-Systeme einzelner Staaten herumzuschließen; eigene Domain-Name-Systeme (DNS) für den Fall zu entwickeln, dass die bestehenden abgeschaltet würden und eigene Software-Entwicklung als ein strategisches Problem von ähnlicher Bedeutung wie Nahrungs- und Energieversorgung zu sehen.

Mit Sicherheitsproblemen bei der Verlagerung von Daten in die Cloud beschäftigte sich Tim Pierson. Wie sicher Daten dort sind, könne kaum überprüft werden. Neben dem Erfordernis, sichere Passwörter zu verwenden, sollten Daten lediglich in verschlüsselter Form in der Cloud abgelegt werden. Zu bedenken ist, dass Daten zur Verarbeitung in Niedriglohnländer ver- und von dort wieder zurückgesendet werden.

Stefan Krebs berichtete über Sicherheitsmanagement in der Praxis, speziell im Bankenbereich. Technische Gegenmaßnahmen wirken, wie Krebs anhand einer Statistik des Schadensverlaufes im Überweisungsverkehr aufzeigte: Immer dann, wenn technische Neuerungen, wie etwa TANs, eingeführt wurden, sank die Schadenssumme zunächst, stieg aber wieder. Nach Einführung von *smsTAN* und *chipTAN* etwa Mitte 2012 konnten die Schadenssummen beträchtlich reduziert werden.

Im Gegenzug waren vermehrt Phishing-Angriffe festzustellen – was die Grenzen technischer Maßnahmen aufzeigt und wo an den Hausverstand appelliert werden muss. Das Ausweichen auf weniger gut gesicherte Bereiche lässt sich auch bei Geldausgabeautomaten feststellen. Vermehrt wird statt bei Banken in Bankomaten eingebrochen, die in Baumärkten oder Tankstellen aufgestellt sind. Bei Skimming ist das Problem, dass in außereuropäischen Staaten bei Geldausgabeautomaten immer noch Kreditkarten akzeptiert werden, die nicht chipgesichert sind. Durch bloßes Auslesen der Daten am Magnetstreifen und Ausspähen der PIN, etwa durch Filmen bei einer Geldbehebung, können Duplikate hergestellt und zur Bargeldbehebung verwendet werden.

Krebs rät, nicht erst im Krisenfall Kontakte zu den Sicherheitsbehörden herzustellen, sondern schon vorher mit diesen zusammenzuarbeiten und Erkenntnisse auszutauschen.

Rechtssicherheit. Bei IT-Sicherheit gebe es keine Rechtssicherheit, sagte Rechtsanwalt Dr. Wolfgang Hackenberg. Rechtssicherheit liege vor, wenn der Einzelne die rechtlichen Folgen seines Verhaltens im Voraus erkennen kann. Im IT-Bereich, mit einer Unzahl von Vorschriften, Normen, Compliance-Regelungen, AGBs, könne man das nicht. Man kann vielleicht noch die inländische Rechtsprechung abschätzen, doch in Verträgen werden vielfach Gerichtsstände im Ausland vereinbart, mit anderen Rechtssystemen und einem anderen Zugang zum Recht. Das Denken im nationalen Normengefüge helfe nicht weiter. Besser sei es, einen Schaden nicht entstehen zu lassen, als hinterher nach einem Schuldigen zu suchen. Dabei müsse ein Restrisiko in Kauf genommen werden, sodass also ein Schaden in einem noch vertretbaren Ausmaß bleibt.

Die Rechtsordnung könne nicht als eine Art Vollkaskoversicherung angesehen werden, dass immer und überall jemand gefunden wird, der für einen eingetretenen Schaden haftet. Grundsätzlich habe jeder für seine eigene Sicherheit zu sorgen.

Nach dem *Veracode State of Software Security Report* 2013 sind bei 69 Prozent der Softwareprodukte beim ersten Ausrollen zumindest einige der 25 gefährlichsten Programmierfehler enthalten. Das werde offenbar bei Software akzeptiert, wäre aber beispielsweise in der Automobilbranche nicht möglich, betonte Hackenberg. Dazu komme, dass in der Praxis Softwareprodukte verschiedener Hersteller eingesetzt werden, wobei diese Produkte nicht unbedingt vollständig kompatibel sind.

Ein Angreifer suche sich jenen Weg aus, über den er am leichtesten zum Ziel kommt. Es werde zu produktlastig gedacht, sagte Hackenberg. IT-Sicherheit müsse ganzheitlich gesehen werden. Technik, Organisation, Recht und Unternehmenskultur müssten zusammenspielen und ineinander greifen. Ein Mitarbeiter habe am

IT-DEFENSE

Vorträge

Die Firma „Cirosec“, ein auf IT- und Informationssicherheit spezialisiertes Unternehmen, veranstaltet seit 2003 jedes Jahr abwechselnd in verschiedenen Städten Deutschlands die *IT-Defense*.

Auf einen Vorabend folgen zwei Tage mit Vorträgen, die sich strategisch mit der IT-Sicherheit befassen; weiters mit neuen Entdeckungen und Entwicklungen in und aus der Hackerszene. Letztlich werden auch Referate mit Unterhaltungswert geboten, die in pointierter Form Themen aus der digitalen Welt aufgreifen.

In einem Round Table am dritten Tag werden einzelne Themen mit den Referenten vertieft behandelt. Die Teilnehmerzahl ist auf 200 begrenzt.

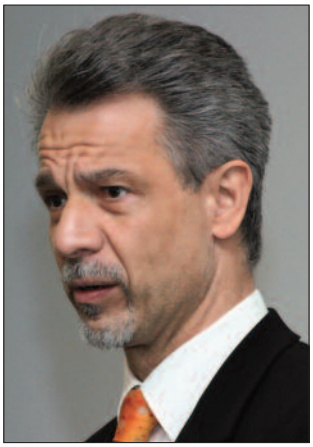
Die 12. IT-Defense hat vom 12. bis 14. Februar 2014 in Köln stattgefunden. Die IT-Defense 2015 wird vom 4. bis 6. Februar 2015 in Leipzig abgehalten.

www.cirosec.de

Mark Benecke: „Software im IT-Bereich ist vergleichbar mit der DNA.“

Marcus Ranum: „Man kann Codes nur vertrauen, die man selbst entwickelt hat.“

Tim Pierson: „Die Sicherheit von Daten in der Cloud kann kaum überprüft werden.“



Wolfgang Hackenberg: „Bei IT-Sicherheit gibt es keine Rechtssicherheit.“

leichtesten Zugang zu Daten – wobei man sich fragen müsse, ob ein Administrator tatsächlich nicht nur zum System, sondern auch auf alle Daten Zugriff haben sollte.

Informationstheorie. „Software im IT-Bereich ist vergleichbar mit der DNA“, sagte Kriminalbiologe Mark Benecke. „Für sich allein sind beide pure Information.“ Manches in dieser Information sei verkapselt und erst in der Anwendung zeige sich, was dahinter steckt; oder, was es für unerwartete Auswirkungen haben kann, wenn an irgendeiner Stelle dieser Information Veränderungen vorgenommen werden.

Der Mensch sei für die DNA ein Betriebssystem. Man dürfe nicht mit vorgefassten Meinungen an die Lösung eines Problems herangehen, sondern vorurteilsfrei „mit den Augen eines Kindes“, zog Benecke eine weitere Parallele zu gerichtsmedizinischen Untersuchungsweisen. Wer sich eine Zeitlang in einem Raum aufhält, hinterlässt DNA-Spuren. Ähnlich verhält es sich mit Spuren, die verwendete Software auf Datenträgern hinterlässt. Wenn die Festplatte gespiegelt ist, kann man Vergleiche mit anderen Informationen herstellen. DNA kann von überall abgenommen werden, etwa von Fingerabdrücken von Trinkgläsern, und das sogar dann, wenn bereits eine daktyloskopische Behandlung dieser Abdrücke vorgenommen wurde. Bei der Vielzahl der Informationen ergibt sich ein gewisses „Grundrauschen“, das weggefiltert werden muss, um zu den Informationen zu gelangen.

In den Industriestaaten wäre es technisch und ökonomisch möglich, alle Einwohner über ihre DNA zu erfassen. Aber: Soll jeder unter Anfangsverdacht gestellt werden? Benecke verneinte diese Frage und verwies auf Gerichtsentscheidungen.

Lulzsec. Michael T. McAndrews war von 2006 bis Dezember 2013 als Special Agent für das FBI in der Bekämpfung der Computerkriminalität tätig und als Mitglied des FBI Cyber Action Teams mit den weltweit wichtigsten IT-Einbrüchen befasst. Er gab einen Überblick über die Tätigkeit von Hacktivisten wie Anonymous und berichtete über die Ermittlungen gegen die Gruppierung „Lulzsec“ und die Verhaftung ihrer Mitglieder.

„Anonymous ist eine Bewegung, keine strukturierte Organisation“, erläuterte McAndrews. „Es gibt keine hierarchische Ordnung, jeder kann für sich die Mitgliedschaft in Anspruch nehmen.“ Die Bewegung trat ursprünglich für die Freiheit des Internets ein, wendete sich gegen jede Art von Zensur, insbesondere durch staatliche Stellen. Sie will Korruption aufdecken und Menschen zu politischer Aktion („Occupy Wall Street“) motivieren.

Eine der Anonymous zugeschriebenen Attacken war die „Operation Payback“ im Oktober 2010. Damals wurden unter anderem große Kreditkartenfirmen durch DDos-Attacken angegriffen – als „Vergeltung“ dafür, dass sie ihre Geschäftsverbindungen zu *Wikileaks* eingestellt hatten. Die Angriffe wurden unter Verwendung des Tools *LOIC (Low Orbit Ion Cannon)* durchgeführt, eines einfach zu bedienenden Programms, das Rechner an die Grenzen ihrer Belastbarkeit bringt. Zum Unterschied von zentral gesteuerten Botnetzen bedarf es einer Vielzahl untereinander abgesprochener Angriffe, um mit diesem Tool wirkungsvolle Attacken zu starten.

Eine ähnliche Aktion erfolgte im März 2011 gegen einen japanischen Konzern wegen eines gegen einen Hacker eingeleiteten Gerichtsverfahrens, der den Code einer Spielkonsole des Konzerns geknackt und veröffentlicht hatte. Als der Inhaber der mit Regierungsbehörden in Verbindung stehenden US-Sicherheitsfirma *HBGary, Aaron Barr,* Anfang Februar 2011 öffentlich erklärte, die Identität führender Mitglieder von Anonymous aufgedeckt zu haben, wurde das Unternehmen unter Ausnützung von IT-Sicherheitsmängeln angegriffen und es wurden Dokumente und geschäftliche Korrespondenz des Unternehmens im Internet veröffentlicht. Die dafür und für den eingetretenen geschäftlichen Schaden verantwortliche Gruppierung, die das „zum Spaß“ („for the lulz“) gemacht hatte, ist durch IT-Angriffe gegen staatliche Behörden und Einrichtungen hervorgetreten, mit dem Ziel, Informationen zu erlangen und zu veröffentlichen. Unter anderem wurden persönliche Daten von Polizisten des Bundesstaates Arizona veröffentlicht, nicht nur Namen und Wohnadresse, auch Handy-Nummern, Kfz-Kennzeichen und -Typen, E-Mail-Accounts, Passwörter und IP-Adressen.

Nachdem die Identität von „Sabu“, einem der führenden Köpfe, ermittelt worden war, erklärte sich dieser zur Zusammenarbeit mit den Behörden bereit. Die übrigen Mitglieder der Gruppierung konnten ausgeforscht und in den USA, England und Irland zu zum Teil mehrjährigen Haftstrafen verurteilt werden. *Kurt Hickisch*

FOTOS: KURT HICKISCH