HACKER SIND TERRORISTEN ODER WIESO DIE DEBATTE UM IT-SICHERHEIT IN DEUTSCHLAND SCHIEF LÄUFT

Aktualisiert am 7. Dez. 2016 Von Martin 7 Kommentare

von Martin Schmetz

Der angebliche Hack von etwa 900.000 Telekomroutern hat in Deutschland das Thema IT-Sicherheit wieder einmal auf die Tagesordnung gesetzt. In den folgenden Tagen kristallisierte sich heraus, dass der Ausfall der Router mit Internetkriminalität in Verbindung stand. Dabei hätte es bleiben können, aber es sollte nicht lange dauern, bis das ebenfalls immer aktuelle Reizthema Terrorismus mit den Vorfällen in Verbindung gebracht wurde: Rainer Wendt,

Bundesvorsitzender der Deutschen Polizeigewerkschaft, ließ im Zuge des angeblichen Hackerangriffs folgendes verlautbaren: "Cyber-Kriminalität ist Terrorismus."

Die Gleichsetzung von Hackern mit Terroristen, die Herr Wendt in seinem Interview vornimmt, ist derart absurd und gleichzeitig symptomatisch für eine unproduktive und hysterische Debatte zu IT-Sicherheit (vulgo: Cybersicherheit) und dem vagen Begriff des Cyberterrors, dass es sinnvoll ist, sie in einen kritischen Kontext zu setzen. Dieser Beitrag betrachtet daher, ausgehend vom Ausfall der Telekomrouter, die Ereignisse und diskutiert wieso die Debatte um IT-Sicherheit in Deutschland fundamental an den eigentlichen Sicherheitsproblemen in der IT und aus Sicht der Terrorbekämpfung vorbei geht.

WAS IST PASSIERT? MIRAI UND DIE TELEKOMROUTER

Dem Angriff auf die Telekomrouter ging eine Welle von Angriffen auf "smarte" Geräte und einige Router voraus. Die Angriffe wurden durchgeführt mit Hilfe der Schadsoftware "Mirai". Die mit Mirai infizierten Geräte wurden zu einem Botnet zusammengeschlossen, also einem von einer Partei gesteuerten Netzwerk von infizierten Geräten. Dieses Botnet konnte dann beispielsweise für Distributed Denial of Service Angriffe, bei denen Server durch eine Flut sinnloser Anfragen lahmgelegt werden, gemietet werden. Nachdem Mirai und die Betreiber aufgedeckt wurden, wurde der Quellcode der

Schadsoftware im Netz veröffentlicht, was zur Folge hatte, dass nun viele verschiedene Varianten der Schadsoftware begannen, ihr Unwesen zu treiben.

Um neue Geräte mit Mirai zu infizieren, scannen diese das Internet nach weiteren anfälligen Geräten. Diese Scans waren es auch schließlich, die die Telekomrouter lahmlegten. Die Router waren zwar nicht anfällig für die Schadsoftware an sich, hatten aber einen Fehler in ihrer Software, der dazu führte, dass die vielen Scans der Miraiderivate zu einem Absturz der Router führten. Damit fiel dann auch das Internet der betroffenen Kunden sowie alle auf das Internet aufbauenden Dienste (beispielsweise Fernsehen oder Telefonie) aus. Die Telekomrouter waren also weder spezielles Ziel noch wurden sie infiziert. Ebensowenig war dies ein bewusster Angriff auf Deutschland. Ihr Ausfall war schlichtweg eine Kombination aus einer unabhängigen Welle von Schadsoftware und einem Bug - ein ungünstiger Zufall. Wenn überhaupt zeugte dies davon, dass die Qualität der Software auf Routern und "smarten" Geräten erheblich verbesserungswürdig war und ist - sowohl bei Telekomroutern als auch bei von Mirai befallenen Geräten.

DIE GLEICHSETZUNG VON TERRORISMUS UND HACKING IST KONTRAPRODUKTIV

Mirai und darauf aufbauende Derivate haben einen kriminellen Hintergrund. Der Betrieb eines Botnets ist zwar

illegal, aber kann sehr lukrativ sein. Allerdings ist das Szenario, das in Deutschland aufgetreten ist, aus mehreren Gründen für Kriminelle denkbar ungünstig: Erstens sollten Infektionen möglichst unbemerkt ablaufen und zweitens sollte das Gerät auch in infiziertem Zustand noch erreichbar sein. Ansonsten können die Geräte auch nicht Teil eines Botnets werden. Und bemerkt man ihren Ausfall, werden wahrscheinlich die Lücken in der Software, die die Infektion erst ermöglichten, geschlossen.[1] Aufmerksamkeit und der Ausfall der Geräte sind also für einen Kriminellen schlecht für das Geschäft.

Die Geschäftskomponente ist es aber auch, die Kriminalität (im Netz wie auch anderswo) fundamental von Terrorismus unterscheidet. Zwar gibt es keine allgemein akzeptierte Definition von Terrorismus, jedoch ist allen gängigen Definitionen die politische Komponente gemein. Letztlich werden Anschläge durchgeführt, um ein politisches Ziel zu erreichen. Es geht nicht um maximalen finanziellen Gewinn, sondern um politische Wirkung. Terroristische Aktivitäten können also ein finanzielles Verlustgeschäft sein und sich aus Sicht der Terroristen trotzdem "lohnen", im Gegensatz zu Kriminalität, die finanziellen Gewinn an sich anstrebt.

Das heißt nicht, dass die Mittel nicht potenziell gleich sein können: Terroristen könnten, ebenso wie staatliche Akteure, Botnets für Angriffe einsetzen. Bei Terroristen ist dies nach momentanem Wissensstand momentan noch nicht in signifikanter Weise vorgekommen, was sicherlich auch mit

der Tatsache zu tun hat, dass der Ausfall von Webseiten oder sogar Teilen des Internets für einige Stunden für die meisten Bürger sicherlich nervig ist, aber weniger Angst verbreitet als etwa ein Bombenanschlag auf einen Bus oder Zug – und letzterer für die meisten Terrororganisationen deutlich einfacher durchzuführen ist.

Dies bedeutet aber auch, dass die Mittel, die man gegen Terrorismus und Kriminalität einsetzt, andere sind: Zwar kann es auch Sinn machen, die finanziellen und materiellen Strukturen von Terrororganisationen anzugreifen, aber letztlich geht es um eine politische oder weltanschauliche Herausforderung einer etablierten Institution oder eines Staates. Nicht umsonst wird (auch in diesem Blog) viel über Deradikalisierungsstrategien geschrieben – dies ist ein valides Mittel im Kampf gegen Terrorismus. Im Kampf gegen Kriminalität wird es kaum Sinn machen. Im Bereich der Kriminalität im Internet geht es vielmehr darum, Geldströme nachzuvollziehen und zu verhindern, und vor allem die Verletzlichkeit von Geräten zu verringern. Letzteres ist eine primär technische Fragestellung.

Der Kampf gegen den Terrorismus wird zudem anders geführt: Er hat inzwischen eine stark militarisierte Komponente und findet in enger Zusammenarbeit mit international vernetzten Geheimdiensten statt. Der Kampf gegen Internetkriminalität erfordert zwar ebenfalls internationale Vernetzung, ist aber die Aufgabe ziviler Strafverfolgungsbehörden. Ein Bundeswehreinsatz gegen

Kriminelle erscheint reichlich absurd. Letztlich kann dies sogar eine Gefahr für die Demokratie darstellen, wenn zivile Strafverfolgungsbehörden zu Gunsten von Geheimdiensten geschwächt werden.

Schließlich ist die eingangs von Wendt erwähnte Gleichsetzung von Hacking und Kriminalität an sich ein erhebliches Problem, denn Hacking ist nicht zwingend kriminell. Es kann ebenso bedeuten, Geräte für einen nicht intendierten Zweck einzusetzen (und dafür zu modifizieren) oder aber Sicherheitslücken aufzudecken. Möchte man sicherere Computer haben, muss man diese Art von Hacking sogar unterstützen, denn sie ist unerlässlich um die Software (und Hardware) in Geräten auf ihre tatsächliche Sicherheit zu überprüfen. Umgekehrt erfordert Internetkriminalität nicht zwingend Hacking: Das Versenden von Spammails oder der Verkauf von illegalen Medikamenten über das Internet sind beispielsweise auch ohne Hacking möglich.

Hacking mit Terrorismus gleichzusetzen ist also aus mehrfacher Hinsicht extrem problematisch und letztlich kontraproduktiv. Internetkriminalität hat gänzlich andere Ziele als Terrorismus – und entsprechend muss man sie auch anders bekämpfen. Diese gleichzusetzen und damit auch die gleichen Mittel zu verwenden ist nicht nur für die Bekämpfung wenig sinnvoll, sondern kann letztlich sogar die Demokratie an sich beschädigen. Schließlich ist Hacking an sich nicht kriminell und dies zu behaupten sorgt nur dafür,

dass eine sehr aktive Szene stigmatisiert wird, deren Arbeit die Sicherheit der Computer, die wir alle einsetzen, erhöht.

EINE RESILIENTERE GESELLSCHAFT

Schlussendlich verstellt die Verwendung des Begriffs "Terror", am besten noch mit dem allseits beliebten Cyberpräfix, den Blick auf die eigentlichen Sicherheitsherausforderungen, die sich durch Mirai und den Ausfall der Telekomrouter ergeben. Terrorismus ist ein politisches Problem und die Lösung muss letztlich auch politisch sein (wenn auch in Kombination mit geheimdienstlichen, juristischen und polizeilichen Mitteln). Damit kann letztlich tatsächlich die gesamtgesellschaftliche Sicherheit erhöht werden. Das immer wieder herumgereichte Schreckgespenst des Cyberterrorismus stellt sich bei näherer Betrachtung als schlichtweg nicht existent heraus. Es gab bis jetzt keine cyberterroristischen Angriffe, die bekannt geworden wären, und es scheint sich wenigstens momentan für Terroristen auch noch nicht zu lohnen, derart viel technischen Aufwand für vergleichsweise wenig öffentliche Angst zu betreiben.

Für die IT-Sicherheit hingegen ist es unerheblich, ob die Angriffe von einem gelangweilten Jugendlichen, einem Kriminellen, einem Terroristen oder einem staatlichen Akteur ausgehen – die Auswirkungen sind immer gleich. Vielmehr muss es daher darum gehen, Sicherheit bei Industrie 4.0 und IoT (Internet of Things, also den erwähnten "smarten" Geräten) erheblich zu stärken um die Resilienz der

vernetzten Gesellschaft insgesamt zu verbessern. Vor allem aber muss es Rahmenbedingungen geben, die überhaupt erst IT-Sicherheit zu einem marktwirtschaftlichen Faktor machen. Denn momentan ist IT-Sicherheit primär ein Kostenfaktor, dessen Ausgaben im Vorhinein oftmals als unnötig erachtet werden. IT-Sicherheit wird erst dann relevant, wenn es schon zu spät ist, weil schlechte IT-Sicherheit erst in dem Moment Kosten verursacht, wo das System bereits infiziert, gehackt oder anderweitig kompromittiert wurde. Wirkliche staatliche Intervention sollte aber vor allem darin bestehen, Anreize für Investitionen in IT-Sicherheit und das Design von sicheren IoT- und Industrie 4.0-Systemen zu setzen, etwa durch Versicherungspflichten oder die Haftbarmachung von Herstellern bei besonders fahrlässigen Designs.

Ebenso zentral bleibt zu betonen, dass dies kein Problem von Krieg oder Terror ist. Es ist primär ein technisches Problem und ein problem ziviler Sicherheit. Hier sollte der Versicherheitlichung dieser Thematik entschieden entgegen getreten werden: Die Frage bei diesem Problem sollte nicht primär sein, *wer* angreift, sondern wie einfach ein solcher Angriff ist und wie verletzlich die angegriffene Infrastruktur. Davor schützt uns im Zweifelsfall keine von der Telekom geforderte Cyber-NATO[2], sondern eher Geräte, die von Anfang mit Sicherheit im Hinterkopf designt werden und deren Entwicklung für Sicherheitstests ausreichend Raum lässt.

1. Dies gilt aus verschiedenen Gründen für Mirai nicht zwingend, allerdings würde dies für diesen Blogbeitrag zu weit führen. Die Folgen 433 und 434

des Podcasts Risky Business geben aber einen guten ersten Überblick über das Phänomen Mirai und die technischen Aspekte davon.

2. Anmerkung am Rande: So wie beispielsweise das NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, das seit 2008 existiert?

Tags: cyber cyber cyber krieg Cyber Terror cyber überall Internet it-sicherheit Kriminalität

7 KOMMENTARE

Pingback: Presseschau KW 49 | Florian Röpke

Ben Dezember 7, 2016

Mit der Sachlichkeit der Analyse bin ich einverstanden, aber es verkennt ein bisschen die Rollen der Beteiligten. Wendt ist kein unparteiischer, sachlicher Beobachter (wenn es so was überhaupt gibt). Er vertritt die Polizeigewerkschaft. Die Perlokution seiner Aussage ist klar: die Polizei ist die Antwort auf „Unsicherheit“ aber braucht dafür Ressourcen; also gilt diese Identifikation einer Quelle der Unsicherheit als Forderung nach Ressourcen; also sind die Pflichten des Vertreters erfüllt, und er verdient damit selber Ressourcen.
Die Aussage ist zwar ein Sprechakt in einer politischen Auseinandersetzung, aber es hat nur nebenbei mit IT zu tun. Er hätte genau so gut „Raser sind Terroristen“ sagen können und hätte es wahrscheinlich ähnlich (un)ehrlich und „ernst“ gemeint.

Antworten

Martin

Dezember 8, 2016

Dass Herr Wendt parteiisch ist, ist natürlich zu erwarten und an sich erst einmal nicht unproblematisch.
Problematisch ist die Versicherheitlichung, der er durch solche Sprechakte Vorschub leistet. Die Diskussion verschiebt sich so in Richtung gewisser Problemlösungen und blendet zunehmend andere aus. Das ist denke ich das eigentliche Problem.
Zudem hat es natürlich durchaus etwas mit IT zu tun. In dem Moment, wo die Polizei Ressourcen zur Bekämpfung der Unsicherheit bekommt, muss sie diese Unsicherheit – und die ist nun einmal auch technischer Natur – bekämpfen können. Dies gilt insbesondere vor dem Hintergrund, dass die Ressourcen begrenzt sind, wahrscheinlich also woanders nicht mehr zur Verfügung stehen. Es ist fraglich, ob die Zuteilung dieser Ressourcen an Strafverfolgungsbehörden tatsächlich demokratisch und sicherheitstechnisch wünschenswert ist. Ich bleibe da erst einmal skeptisch.

Antworten

Thomas Reinhold

Dezember 7, 2016

Hi Martin, danke für die ausführliche Analyse. Der Umgang mit dem Vorfall ist auch vor dem

Hintergrund der zivilen und militärische Aufrüstung im Bereich der offensiven Cyber-Aktivitäten sehr bedenkenswert. Ich habe hier meine Gedanken von diesem Standpunkt aus betrachtet zusammen getragen

http://cyber-peace.org/2016/12/02/nachlese-zum-hackerangriff-auf-das-telekom-netz-analyse-und-implikationen/

viele Grüße
Thomas

Antworten

Martin

Dezember 8, 2016

Hi Thomas,
vielen Dank! Und ich gebe Dir recht, die Aufrüstung im Bereich offensiver Cyber-Aktivitäten bringt noch einmal einen weiteren problematischen Aspekt rein.
Dein Beitrag ist ebenfalls super. Ich hab den gleich mal auf Twitter geteilt.

Viele Grüße
Martin

Antworten

Thomas Reinhold

Dezember 8, 2016

Dankeschön

Antworten

Pingback: Kritik an Gleichsetzung von Hacking und Kriminalität | Freier Ingenieur Hasler

SCHREIBE EINEN KOMMENTAR

Deine E-Mail-Adresse wird nicht veröffentlicht.

Kommentar

Name

E-Mail-Adresse

Website

Ich bin kein Roboter.
reCAPTCHA
Datenschutzerklärung - Nutzungsbedingungen

Kommentar abschicken

Benachrichtige mich über nachfolgende Kommentare per E-Mail.