2011/12 Inland

https://shop.jungle.world/artikel/2011/12/der-staat-hackt-mit

Die Gründung des »Nationalen Cyberabwehrzentrums«

Der Staat hackt mit

Von **till grefe**

Wenn es dem Schutz vor dem »Cyberwar« dient: Am »Nationalen Cyberabwehrzentrum«, das im April seine Arbeit aufnimmt, wird die Trennung von Polizei und Geheimdiensten aufgehoben.

Eigentlich wollte Bruce Dang vom Microsoft Security Response Center gemeinsam mit seinem Kollegen Peter Ferrie Ende vergangenen Jahres auf dem Chaos-Computer-Kongress über seine »Adventures in Analyzing Stuxnet« referieren. »Bevor ich anfange: Ich möchte hier nichts über den Mossad sagen«, begann Dang seine Ausführungen und sorgte damit für Heiterkeit im Saal. Sein Kollege Ferrie sei auf einem Fußweg von einem Auto angefahren worden und könne nun nicht dabei sein, sagte Dang mit einem Schmunzeln. Nach den verschwörungstheoretischen Randbemerkungen widmete er sich Stuxnet. Die Software habe aus seiner Sicht zwei interessante Aspekte: Erstens wurden in der Schadsoftware vier bis dahin unbekannte Schwachstellen von Windows-Betriebssystemen ausgenutzt, und zweitens war ihr Zweck die Manipulation von Steuertechnologien.

Ein Bericht von Siemens vom Juli 2010, demzufolge ein Schadprogramm Industriesteuerungsanlagen der Firma infiziert habe, hatte Computer- und Technikexperten in Unruhe versetzt. Stuxnet, wie die Sicherheitsfirma Symantec das Problem taufte, stellte sich bei den Untersuchungen als ein komplexes Schadprogramm heraus, das dazu geschrieben worden war, Prozesse in Gaszentrifugen zu manipulieren, die mit Steuerungen von Siemens kontrolliert werden. »Nach der von uns durchgeführten Analyse können wir feststellen, dass Stuxnet kein zufälliges Produkt eines Hackers sein kann«, sagte ein Pressesprecher von Siemens Ende September 2010 in der NZZ. Hauptziel der Schadsoftware sei entweder die iranische Anreicherungsanlage Natanz oder der Reaktor in Bushehr gewesen, vermuteten viele Kommentatoren.
Anfang Oktober erklärte Siemens, weltweit sei bei 15 Kunden die Schadsoftware entdeckt worden, in fünf Fällen in Deutschland. Ende Oktober beschäftigte sich der Innenausschuss des Bundestags in einer nichtöffentlichen Sitzung mit dem Thema. Ein Bericht des Bundesministeriums des Innern und des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) zur »Gefährdung der Internetkommunikation in Deutschland

durch die Schadsoftware Stuxnet« wurde vorgelegt. Ende Dezember 2010 gab die Bundesregierung dann bekannt, ein Nationales Cyberabwehrzentrum (NCAZ) unter der Führung des BSI zu gründen. »Die Erfahrungen mit dem Schadprogramm Stuxnet zeigen, dass auch wichtige industrielle Infrastrukturbereiche von gezielten IT-Angriffen nicht mehr ausgenommen sind«, zitierte der Spiegel aus der als geheim eingestuften Kabinettsvorlage vom Februar 2011.
Am 1. April soll das NCAZ mit Mitarbeitern des BSI, des Verfassungsschutzes, des Bundesamts für Bevölkerungsschutz und der Katastrophenhilfe, des Bundeskriminalamts, der Bundespolizei, des Zollkriminalamts, des Bundesnachrichtendienstes und der Bundeswehr seine Tätigkeit aufnehmen. In einer Presseerklärung ließ das Bundesinnenministerium auch ausführlich Branchenvertreter zu Wort kommen. »Die ITK-Branche begrüßt sehr, dass sich die Bundesregierung dem Kampf gegen Cyber-Kriminalität so stark annimmt. Bei der Umsetzung der Strategie müssen Staat und Wirtschaft eng zusammenarbeiten«, wurde Dieter Kempf vom Branchenverband Bitkom zitiert. Etwa drei Viertel der gefährdeten Infrastruktur befänden sich in privatem Besitz, schrieb das Bundesinnenministerium.

Das Vorhaben der Bundesregierung, nach dem Vorbild des Gemeinsamen Terrorismusabwehrzentrums eine weitere Institution zu schaffen, in der die verschiedenen Sicherheitsbehörden zusammenarbeiten, stieß bei der Opposition auf Widerspruch. »Kaum glaubt der Bundesinnenminister, die Tragweite der Stuxnet-Cyberattacke gegen das iranische Atomprogramm verstanden zu haben, herrscht in der Bundesregierung in Sachen IT-Sicherheit Aktionismus«, kritisierte der Bundestagsabgeordnete Jan Korte (Linkspartei) in einer Presseerklärung den Plan, ein »IT-Heimatschutzministerium NCAZ« zu schaffen. »Im Eiltempo und am Parlament vorbei versucht die Bundesregierung seitdem, für den Cyberwar massiv aufzurüsten. Verfassungsrechtliche Bedenken werden ignoriert.« Die Trennung von Polizei und Geheimdiensten werde aufgehoben. Auch das Verbot von Bundeswehreinsätzen im Inneren werde »geschickt, aber verfassungsrechtlich bedenklich« ausgehebelt.
Eine grundsätzliche Kritik betreffe den Begriff »Cyber«, sagt Konstantin von Notz, der innen- und netzpolitische Sprecher der grünen Bundestagsfraktion, im Gespräch mit der Jungle World. »›Cyber‹ ist ein sehr schwammiger Begriff und erschwert die präzise Analyse der tatsächlichen Bedrohungslage, die jetzt eigentlich erforderlich wäre.« Die Bundesregierung spreche von weit mehr als zehn Millionen Angriffen im Jahr. »Aber es wird nicht gesagt, was für Angriffe das sind, vor welchem Hintergrund und in welcher Qualität sie stattfinden«, gibt Notz zu bedenken.
Einige Experten versuchen, ein differenzierteres Verständnis von Stuxnet zu vermitteln. Die Schadsoftware sei zwar sehr aufwendig, aber zu leicht zu entdecken und zu entschlüsseln gewesen, sagte der britische IT-Sicherheitsexperte Tom Parker, weshalb er vermute, dass keine Behörde westlicher Staaten hinter der Software stehe. Es sei auszuschließen, dass es sich bei Stuxnet um einen gezielten Angriff auf den Iran gehandelt habe, urteilte Sandro Gayken von der Freien Universität Berlin. Bei dem Programm habe es sich eher um einen »Waffentest« gehandelt. »Da wollte jemand mit sehr viel Wissen ausprobieren, wie seine Erfindung funktioniert«, wurde Gayken in der österreichischen Zeitung Standard zitiert. Nationale Abwehrzentren seien »Augenwischerei«, die Jagd nach Tätern im Internet sei nahezu aussichtslos. »Um zu bestrafen, muss man erst einmal den

Missetäter identifizieren können, und eben das ist im Internet meist nicht möglich. Angreifer können sich geschickt tarnen.« Gayken, der auch die Bundeswehr berät, empfiehlt deshalb die vollständige Abkopplung gefährdeter Infrastruktur vom Internet und die Umrüstung militärischer Computersysteme.

Die Bundesregierung hofft offensichtlich, dem Problem institutionell beizukommen. Neben dem NCAZ soll ein nationaler »Cyber-Sicherheitsrat« die »übergreifenden Politikansätze für Cybersicherheit« koordinieren, in dem Vertreter des Kanzleramts, des Auswärtigen Amts, des Innen-, Verteidigungs-, Justiz-, Wirtschafts- und Finanzministeriums des Bundes sowie »assoziierte Mitglieder« aus der Wirtschaft sitzen. Zusätzlich soll es im Wirtschaftsministerium eine »Task-Force« geben, die ab nächster Woche mittlere und kleine Betriebe in Fragen der IT-Sicherheit berät.
Überdies wurde kürzlich das Vorhaben des Bundeskriminalamts (BKA) bekannt, unter eigener Führung eine weitere »Cyberabwehr« einzurichten, die sich um Banken und Sparkassen kümmern soll. Ziel ist BKA-Präsident Jörg Ziercke zufolge eine »institutionalisierte Public-Private-Partnerschaft«. Ähnliche Verbindungen gibt es schon beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Dort wird gerade eine »länderübergreifende Krisenmanagement-Übung (Lükex)« für den Herbst vorbereitet. In den vergangenen beiden Jahren hieß die Übung »Schmutzige Bombe«, dieses Mal soll ein Szenario aus einem »Cyberwar« durchgespielt werden: die Reaktion auf zielgerichtete Angriffe und Zusammenbrüche von IT- und anderer Infrastruktur.