„Cyber-Gedöns“

Warum der neue Vorstoß zur Cyber-Sicherheit am Kern des Problems vorbei geht.

Jeden Tag soll es rund 6500 Cyber-Angriffe auf Bundeseinrichtungen geben. Bisher ist es glücklicherweise noch zu keinem massiven Ausfall eines Kraftwerks oder ähnlich sensibler Infrastruktur gekommen. Nun hat Verteigigungsministerin Ursula von der Leyen bekanntgegeben, bei der Bundeswehr eine eigene Truppenorganisation „Cyber- und Informationsraum“ (CIT) mit 13 500 Soldaten und zivilen Mitarbeitern aufzustellen. Warum?

Es handelt sich dabei um den Versuch des Verteidigungsministeriums, den Bereich Netzwerksicherheit als Handlungsfeld zu besetzen. Aus meiner Sicht ist das reines Machtkalkül und wenig zielführend. Der Versuch, das Feld zu militarisieren und zu „vergeheimdienstlichen“ geht am Kern des Problems vorbei: schlechte Software, mangelnde Ausbildung und fehlende Haftungsregeln für Unternehmen. Zu glauben, man könne hier mit militärischen Mitteln irgendetwas anderes als eine Eskalation bewirken, ist naiv.

Die Lage fasste ein Bundeswehr-General mir gegenüber auf einer Veranstaltung treffend zusammen: „Solange ich über das Bundeswehr-Logistiksystem nicht einmal zuverlässig Toilettenpapier bestellen kann, brauche ich auch kein Cyber-Gedöns.“ Die Bundeswehr könnte sicher mehr IT-Experten vertragen, um ihre internen Probleme besser und sicherer zu lösen. Sich einzubilden, man bekäme qualifizierte Mitarbeiter, in dem man „Cyber Cyber“ auf Plakate druckt, ist jedoch einfach nur lächerlich.

Welche technischen, rechtlichen und ethischen Fragen wirft diese neue Art der Kriegsführung auf?

Es gibt im digitalen Raum keine Attribution. Das heißt ein „Gegenschlag“ ist kaum treffsicher zu führen, jeder Akteur wird mehrschichtige Methoden der Tarnung anwenden. Daraus folgt auch, dass es keine wirksame Abschreckung gibt. Wenn man abschrecken will, muss man in der Lage sein, glaubhaft zu machen, dass man

Angriffe zuordnen, eben attribuieren kann. Das ist jedoch selbst in einem umfassenden Überwachungssystem nicht sicher möglich.

Aus meiner Sicht ist das reines Machtkalkül und wenig zielführend.

Wird die Bundeswehr allein für Deutschlands Cyber-Sicherheit sorgen oder wie müsste eine Arbeitsteilung mit Polizei, Bundesnachrichtendienst, Ministerien und anderen Behörden aussehen?

Zuallererst ist hier das Bundesamt für die Sicherheit in der Informationstechnik zuständig. Deswegen muss es aus der Verantwortung des Innenministeriums befreit und zu einem wirklich unabhängigen Dienstleister für digitale Sicherheit gemacht werden, bei dem nicht der Verdacht der Kungelei mit Sicherheitsbehörden mit angriffsorientierten Interessen besteht. Weder Militär noch Geheimdienste haben irgendeinen strukturellen Vorteil, der ihre Verantwortlichkeit für das Gebiet nahelegt, im Gegenteil. Das Kernproblem ist und bleibt angreifbare Software, und das lässt sich nur mit massiven Förderprogrammen für eine Verbesserung der technischen Lage beheben, nicht mit Cyber-Soldaten oder Cyber-Agenten.

Ist die deutsche Cyber-Strategie mit europäischen und internationalen Maßnahmen vereinbar?

Es gibt derzeit keine Strategie, weder national noch international. Es gibt Wunschträume und Machtgerangel. Insofern passt der Bundeswehr-Vorstoß ins Bild.

Die Fragen stellte <link ipg unsere-autoren autor ipg-author detail author anja-papenfuss>Anja Papenfuß.



Frank Rieger
Berlin

Frank Rieger ist seit 1990 einer der Sprecher des Chaos Computer Clubs

(CCC). Er hat verschiedene Startup-Unternehmen in den Bereichen Datensicherheit, Navigationsdienste und E-Reading mitgegründet und arbeitet derzeit als Geschäftsführer eines Unternehmens für Kommunikationssicherheit.

19 LESERBRIEFE

Ramms schrieb am 03.05.2016

Wenn ein Bundeswehrgeneral über das "Bundeswehr-Logistiksystem" Toilettenpapier anfordern oder erhalten möchte, sollte er entlassen werden, denn er kennt offensichtlich weder den Versorgungsweg für Toilettenpapier noch das Bundeswehr- Logistiksystem. Solche Generale braucht die Bundeswehr nicht.

Galgenstein schrieb am 03.05.2016

Zur Erinnerung: als es einen Hockerangriff auf den Bundestag gab, durfte diesen das Bundesamt für Informationssicherheit tagelang nicht abstellen. Die Abgeordnete der Linkspartei empfand dies als einen nicht zulässigen Eingriff in die Unabhängigkeit der Abgeordneten.
Es gilt halt auch: es nützt die schönste Waffe nichts, wenn man sie im Ernstfall nicht zum Einsatz bringt.

ingar frauding schrieb am 03.05.2016

@Galgenstein:
Zur Erinnerung: es war eine Abgeordneten-Mitarbeiterin der Die.Linke-Fraktion, der die Bundestags-IT Wochen vor dem großen Aua auf den möglicherweise initialen Trojanerbefall hinwies.
Es war die Spionageabwehr des Verfassungsschutzes, die von ausländischen Diensten DREI WOCHEN vor dem Skandal Hinweise auf fette Datenlecks im BT-Server bekam.
Was nutzt eine waffenstarrende IT-Abteilung, wenn sie nur auf Anordnung des Generalstabs (nach dem langen Wochenende) mal an der Frontlinie vorbeischaut?

Und ja: die Rechner der Abgeordneten sind ihr wichtigstes Arbeitsinstrument. Das Parlament ist das vom Staatsvolk gewählte Kontrollorgan der Regierung. Abschalten nur mit Genehmigung. Punkt. Der Skandal hier: dass es kein Rückfallsystem zur Aufrechterhaltung der Arbeitsfähigkeit gibt

Freeflight schrieb am 03.05.2016

@Galgenstein
Dann sollten Sie mal Ihre "Erinnerung" richtig auffrischen, das ist nämlich absoluter Käse was Sie da erzählen. Abschaltung der Systeme, zum Absichern, wurde am 12.08.2015 verschoben, wegen einer Sondersitzung zum Thema Griechenland.

Aber recht passend das Sie direkt im Anschluss von "schönsten Waffen" reden beim Thema "Cyber-Bundeswehr" (Gnahaha), da ist jemand dem Cyber-Gedöns ganz schön auf den Leim gegangen. Ist ja aber auch kompliziert dieses "Neuland" Zeug.

Tim schrieb am 03.05.2016

@Ramms Es ist ein Bild, eine Metapher. Der hat ziemlich genau verstanden wie das System funktioniert. Schaue Dir das Beschaffungssystem an, es ist ein Moloch, ein absoluter Moloch!

Er hier schrieb am 03.05.2016

@Ramms: Ich glaube, das mit dem Toilettenpapier war eher als anschauliches Beispiel bzw. als Metapher

gemeint. Wenn man nicht mal Triviales hinbekommt, wie will man sich dann mit Elite-Crackern anlegen?

Eignete sich übrigens gut als Zitat, wenn der Name des Generals bekannt wäre ...

Jens/BlauerBote schrieb am 03.05.2016

Ich frage mich da immer, ob diese Gegenschläge auch gegen die eigene Bevölkerung gerichtet sein können, die man der Feindpropaganda ("Informationskrieg") bezichtigt.

Synapsenkitzler schrieb am 03.05.2016

Es ist ein Unding, dass die Dienste den Handel mit Sicherheitslücken durch Kauf/Nutzung fördern, statt diesen zu verhindern. So wird aktiv ein Bedrohungsszenario geschaffen/aufrecht erhalten. Das ist perfide, und den Zielen, Schutz der Bevölkerung/des Landes, widersprechend. Wobei auch hier Nationaldenken überholt ist. Die Früchte darf der Verfassungsschutz Sachsen-Anhalt gerade kosten (Ransomware).

Isabelle schrieb am 03.05.2016

Clickworker im Cyber-Sicherheitsgewand will man uns hier verkaufen. Zensursula bleibt sich selbst treu.

Peter schrieb am 03.05.2016

In Zeiten von Web 2.0. (3.0? 4.0?) und der Mentalität von wir machen alles online ist es nur offensichtlich das die BW auch Gebrauchsartikel wie Toilettenpapier gern über online Formulare abwickeln möchte. Dass das wohl nicht klappt wie geplant sollte wohl die Aussage des Generals sein. Und mit dem Kenntnisstand einen "cyber"-Krieg zu führen ist mindestens abenteuerlich.

Michi schrieb am 04.05.2016

@Galgenstein
Es ist absolut nachvollziehbar das die Abgeordneten der Linken das BSI nicht an ihre Rechner lassen wollen. Das BSI ist dem Innenministerium unterstellt, ebenso wie der Verfassungsschutz, der wen beobachtet? Richtig, die Partei "Die Linke".

Um das BSI an seinen Rechner zu lassen, obwohl man vom Verfassungsschutz beobachtet wird, muss man ganz schön naiv sein. Dass vom BSI nicht nur Defensiv-Aufgaben ausgeführt werden (die dem eigentlichen Aufgabenbereich entsprechen) ist spätestens klar seitdem 2015 bekannt wurde das das BSI aktiv am verfassungswidrigem Staatstrojaner mit gearbeitet hat.

Ansonsten hat Frank natürlich recht. Vor Angriffen schützt nur sichere Software. Wer sich auf "Cyberwar" einlässt VERHINDERT sichere Software, weil er von Sicherheitslücken abhängig ist

---

blafasel schrieb am 04.05.2016

@Galgenstein:
Das ist ja genau das Problem: das BSI ist dem BMI unterstellt. Wäre es unabhaengig und vertrausnewürdig, dann haette die Linke sicher auch kein Problem mehr damit.

NeindochOh schrieb am 04.05.2016

Galgenstein

Was ja auch Sinn ergibt. Im Moment untersteht das Bundesamt für die Sicherheit in der Informationstechnik dem Innenministerium, welchem auch der Inlandsgeheimdienst untersteht. Aus sieht einer Demokratie und der Unabhängigkeit eines Abgeordneten wäre es unerträglich diesem Zugang zur Kommunikationsinfrastruktur der Legislative zu geben. Genau deswegen muss das BIS auch vom BIM getrennt werden.

Dr. Valentin schrieb am 04.05.2016

Durch Cyber-Uschis Leben als Politiker-Ersatz ziehen sich als roter Faden vor allem die Schnellschüsse aus der Hüfte. Leider ist sie kein Cowboy und trifft auch nie. Erinnert sei an ihre Stoppschild-Kampagne gegen Kinderpornographie und an ihre Anstrengungen, das Internet generell zu zensieren, wofür sie auch den Kosenamen "Zensursula" verliehen bekam. Nichts wird von ihr oder ihrem Umfeld bis zum Ende gedacht oder gar bis zum bitteren Ende weiter verfolgt. Immer wieder nur billige Propaganda und nur auf eben diese Effekte berechnet nach dem Motto "Die Uschi, die macht wenigstens was!" So wird man bundeskanzlertauglich,

jedenfalls bei den Auftraggebern dieser Politik.,

Klaus Bombe schrieb am 04.05.2016

"Cyber-Gedöns" - als IT-Revisior kommt mit das bekannt vor. In vielen Bereichen, welche ich selbst gesehen und beurteilen durfte, werden Personen zur Administration eingesetzt, welche noch nicht einmal jährlich wenigstens 4Wochen IT-Schulung bekommen. Wenn schon die Führungskräfte so wenig für IT-Sicherheit ausgeben wollen, dass Schulung zu teuer ist... gute Güte Deutschland!
Als Revisor darf man das dann nicht mal in das Prüfungsergebnis rein schreiben, weil es keine konkreten Schulungsvorgaben gibt und es nicht zum "Unternehmensziel: SPAREN" passt.
#Deutschland schafft sich ab - dank neoliberaler Idiotie auf allen Ebenen!

---

kdm schrieb am 04.05.2016

Kommentator Ramms hat die treffliche Metapher des Generals nicht verstanden. Dieser General verdeutlicht Frank Riegers Vorbehalte kurz & verständlich. Und

deshalb hat Rieger ihn zitiert.
(Himmelhilf, dass man alles immer erklären muss...)

Max schrieb am 04.05.2016

@ramms: Verstehendes Lesen müssten Sie eigentlich in der Schule gehabt haben. Der General hat nicht gesagt, dass er selbst Toilettenpapier bestellt. Statt "ich" hätte er auch "man" sagen können. Er hat einfach nur gesagt, dass das Bundeswehr Logistiksysten scheiße ist, da man noch nicht einmal zuverlässig Toilettenpapier darüber bestellen könnte. Man muss also erstmal die Basics richtig machen, bevor man mit der ich dem Cyber-unsinn loslegt.

Alex schrieb am 04.05.2016

@Ramms: Ein Großteil des Toilettenpapiers wird von Gebäudereinigungs-Dienstleistern gemäß Rahmenvertrag bereitgestellt - und die sind Privatwirtschaft, also relativ zuverlässig. Es gibt allerdings Bereiche, in denen nicht oder nur unregelmäßig Gebäudereinigungs-Dienstleister zum Einsatz kommen. Daher gibt es in mindestens einer Kaserne tatsächlich die Möglichkeit, Toilettenpapier

über den Nachschub anzufordern.

Wenn das mal wieder nicht rechtzeitig geklappt hatte, kamen die genervten "Bunkerratten" bei mir vorbei auf dem Weg zur "öffentlichen" Toilette (im normal gesicherten Bereich). Das nervigste daran war wohl, dass man beim Betreten des gesicherten Bereichs jedes Mal durch die Schleuse muss.

Bei uns im Stab fehlte nur vier Wochen lang das Druckerpapier, das ging noch...

Meo schrieb am 04.05.2016

Ich teile die Perspektive von Frank durchaus. Schaut man in Politik und Verwaltung, hat niemand "das mit dem Internet" und der IT im allgemeinen verstanden. Da jetzt auch noch Krieg auszurufen erinnert zum einen an kleine Kinder, welche zusammen nicht im einzigen Buddelkasten spielen wollen und zum anderen an das übliche Gerangel um Gelder aus den Töpfen.
Wollte hier jemand wirklich was mit "Cyber" machen, wäre der schnelle Zugang zum Netz ebenso selbstverständlich wie die Straße zum Haus und der

Wasseranschluss. Unternehmen würden vor IoT/Industrie 4.0 gewarnt und beraten, anstatt solche Blindflüge gehypt. Kommunen hätten richtiges eGov und Webseiten, statt ePerso/Gesundheitskarte/DeMail/... und würden dank freier Software weder finanziell noch datenmäßig abgezogen.
