15. Feb. 2013

von Martin

in Cyber Security, Sicherheitskultur

Kommentare (1)

Verteidigung ist die beste Verteidigung

Warum die Cybersicherheitsstrategie der EU und die Executive Order von Obama zur Cybersicherheit Sinn machen.

von Martin Schmetz

Dass Cybersicherheit aktuell ein hippes Thema ist um ganz schnell viel Aufmerksamkeit zu bekommen (1), ist inzwischen zur Binsenweisheit geworden. Die Presse betet das Thema rauf und runter, und die Politik unternimmt erste konkrete Schritte, zum Beispiel die vor kurzem veröffentlichte Cybersicherheitsstrategie der EU und die nun in Kraft getretene Executive Order zum Thema Cybersicherheit von Präsident Obama. Beide haben viel Kritik eingefangen – teilweise unberechtigt, wie ich finde.

Die *Executive Order* sieht drei Punkte vor: Erstens vereinfacht sie das Teilen von Informationen über Cyberangriffe zwischen privaten und staatlichen Akteuren in beide Richtung, mit zentraler Verantwortung beim Department of Homeland Security. Zweitens wird ein *Cybersecurity Framework* ausgearbeitet. Dies sieht verschiedene *best practice* Vorgehensweisen vor, die vom National Institute of Standards and Technology zusammen mit privaten Akteuren ausgearbeitet werden und die auf freiwilliger Basis implementiert werden können. Drittens wird Wert auf Privatspähre und Schutz der Bürgerrechte gelegt. Es gibt einen Rahmen basierend auf bestehenden rechtlichen Regeln und zudem sind regelmäßige Audits vorgesehen.

Der Entwurf der EU-Richtlinie zur Cybersicherheit bzw. die Cybersicherheitsstrategie der EU sieht ebenfalls den Informationsaustausch zwischen privaten und staatlichen bzw. europäischen Akteuren vor, wenn dieser auch deutlich asymmetrischer zugunsten der staatlichen und europäischen Akteure ausfällt. Betreiber kritischer Infrastruktur und "zentraler Dienste der Informationsgesellschaft" müssen Risikomanagement betreiben und Einbrüche in ihre Systeme melden. Außerdem sieht es vor, dass in jedem Mitgliedsstaat in Zukunft nur eine Behörde für Cybersicherheit zuständig ist und jeder Mitgliedsstaat eine Strategie zur Cybersicherheit ausarbeitet.

Bevor ich nun auf die Kritik daran eingehe, macht es Sinn diese grob in drei Lager einzuteilen. Die erste Form der Kritik kommt aus der Zivilgesellschaft

und stößt sich vor allem an der zunehmenden Militarisierung des Internets und der Gefährdung von Grundrechten. Je mehr der Staat sich demnach über die Sicherheitsapparate in das Internet einmischt, desto mehr gefährdet er potenziell Bürger. Die zweite Form der Kritik kommt vor allem aus dem Umfeld einiger privater Cybersicherheitsanbieter sowie von militärnahen Politikern und Beratern. Sie stoßen sich an der eher defensiven Ausrichtung und fordern offensivere Maßnahmen. Für sie ist Angriff die beste Verteidigung. Die dritte Kritik kommt – vor allem in den USA – aus der Wirtschaft und stößt sich an der Tatsache, dass Cybersecurity teuer ist. Es gibt noch einige andere Kritikpunkte, etwa dass die Cybersicherheitsstrategie der EU zu vage sei – was meiner Meinung nach absolut stimmt – aber auf diese soll hier nicht näher eingegangen werden, weil reine Zustimmung unspannend zu lesen ist.

Dass Cybersecurity teuer ist ohne dass die Investitionen sich sofort bezahlt machen ist durchaus einleuchtend. Man kann, ist man nicht sowieso Anbieter von Sicherheitsoftware oder –dienstleistungen, diese nicht sofort an den Kunden für Geld weiterreichen. Stattdessen kann es sich aber lohnen darauf zu hoffen, dass der Kelch des Hacks am eigenen Unternehmen vorüber geht. Es ist natürlich einigermaßen schwer, dies mit Äußerungen, dass etwa in den USA inzwischen jedes größere Unternehmen Opfer eines Hacks geworden sei und jährlich über 1 Billion USD Schaden dadurch entstehe (2), unter einen Hut zu bringen. Insbesondere wenn Vertreter der gleichen Seite beide Meinungen vertreten. Entsprechend sollten sich Unternehmen eigentlich eher glücklich schätzen, wenn alle durch staatliche Vorschriften gleichermaßen gezwungen werden, Maßnahmen zur Erhöhung ihrer Cybersicherheit durchzuführen. So hat wenigstens niemand einen geldwerten Vorteil davon nichts zu tun.

Die Kritiker, die sich an der defensiven Ausrichtung stören führen die gefühlte Hilflosigkeit an. Eine Verbesserung der eigenen Systeme mag Hacks erschweren, verhindern wird es sie kaum. Daher möchte man – je nachdem ob die Meinung aus militärischen oder zivilem Umfeld kommt – entweder direkt als Unternehmen zurückschlagen oder aber den Staat absichern durch übermäßige Cyberwar-Kapazitäten, die als Abschreckung dienen sollen. Meiner Meinung nach kann das kaum klappen und mit dieser Überzeugung stehe ich nicht allein. Über den Sinn der Entwicklung von Cyberwar-Kapazitäten an sich soll hier nicht diskutiert werden, aber diesen eine Priorität gegenüber der Sicherung der eigenen Systeme einzuräumen erscheint unausgegoren. Erstens ist die auch von Neelie Kroes angeführte Gefahr des Wettrüstens nicht von der Hand zu weisen – und dies ist eine gerade für den Westen eher unerfreuliche Entwicklung. Denn zweitens stellt sich die Frage, wie abschreckend die westlichen Staaten sein sollen wenn sie die Staaten sind, die mit ihrer stark vernetzten Infrastruktur das mit Abstand verletzlichste Ziel darstellen. Und drittens taucht wieder einmal das altbekannte Attributionsproblem auf – eine Abschreckung impliziert, dass man weiß wer angreift und vernichtend zurückschlagen kann. Den Angreifer zu identifizieren ist durchaus möglich, wenn auch nicht zwingend mit absoluter Sicherheit und zeitnah. Aber es wäre bedeutend einfacher wenn

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

It's not Cyberwar, stupid!

KATEGORIEN

Außenpolitik (59)

Bürgerkriege (16)

Cyber Security (42)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (28)

Pandemien (2)

Podcast (7)

Popkultur (21)

Sanktionen (8)

Security Culture (14)

defensive Maßnahmen ergriffen würden, die eine präzisere Überwachung der eigenen infiltrierten Netzwerke erlauben und die zudem einen schnellen und umfassenden Informationsaustausch zwischen den betroffenen Parteien ermöglichen. So könnte man schneller erkennen wer angreift und dies zum Beispiel öffentlich kommunizieren, wie etwa die New York Times vor kurzem. Nur dagegen wird sich gerade gewehrt. Auf die Idee, dass Unternehmen am besten in Selbstjustiz zurückschlagen soll hier gar nicht groß eingegangen werden. Es ist fraglich, ob dies – abgesehen von Honeypots – überhaupt legal ist. Und welches Unternehmen möchte schon für einen eskalierenden diplomatischen Konflikt verantwortlich sein, weil es aus Versehen gegen den falschen Akteur zurückgeschlagen hat?

Die Kritik aus der Zivilgesellschaft halte ich für die stichhaltigste. Die Executive Order Obamas ist davon interessanterweise weniger betroffen, sieht sie doch Maßnahmen zum Datenschutz und der demokratischen Überwachung vor (CISPA auf der anderen Seite nicht). Die Richtlinie zur Cybersicherheit hingegen muss sich einige Kritik anhören und meiner Meinung ist auch vieles davon berechtigt. Die Frage der bürokratischen Organisation ist in der Tat eine umstrittene – eine zentralisierte Organisation bringt eine Gefährdung der Gewaltenteilung und eine inakzeptable Machtbündelung mit sich, aber ein dezentraler Ansatz bedeutet wahrscheinlich mangelnde Handlungsfähigkeit. Hier gilt es, eine demokratische Überwachung, Transparenz und eine regelmäßige Rechtfertigungspflicht zu sichern und trotzdem handlungsfähig zu bleiben. Beunruhigend ist aber vor allem der Einbezug geheimdienstlicher Organisationen. Damit geht fast zwangsläufig einher, dass der daraus resultierende Apparat nicht vernünftig demokratisch überwacht werden kann und vermutlich militarisiert wird. Geht es vor allem um den Schutz der Zivilgesellschaft, der gesellschaftlichen Infrastruktur und vor Kriminalität im Netz, müssen logischerweise auch primär zivilgesellschaftliche Akteure und zivile Strafverfolgungsorgane eingebunden werden, und zwar in einer demokratischen Struktur.

Trotz dieser Kritikpunkte halte ich die beiden Papiere für einen Schritt in die richtige Richtung. Es muss in der Tat noch viel nachgebessert und vor allem in der Praxis ausformuliert werden. Aber es ist wichtig, dass überhaupt etwas getan wird und das Problem aus einem defensiven Blickwinkel angegangen wird. Cybersicherheit ist in der Tat ein Problem, aber es ist eben primär ein zivilgesellschaftliches – es geht vor allem um Cyberkriminalität und in gewissem Maße um Spionage. Möchtegern-Cyberkriegern und Komplettverweigerern das Feld zu überlassen wäre ein großer Fehler, denn beide haben ein großes Interesse daran, keine Regeln zu erlassen, ob mit oder ohne demokratische Überwachung. Und darunter leidet am Ende vor allem die Idee eines demokratisch organisierten Internets.

(1) Ich bin mir der Ironie bezüglich dieses Blogbeitrags bewusst. Trotzdem: Mehr Hits, bitte.

(2) Eine nicht unumstrittene Zahl.

Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (22)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War

Bild von marsmet481 @ flickr

Tags: cybersecurity, cybersicherheit, EU, executive order, Obama, richtlinie

« Kritische Polizeiforschung: Ein unvollständiger Tagungsbericht
Online Talk »

Trackbacks/Pingbacks

1. **IB Online (3/2): Eine kleine Netzschau « Bretterblog** - 18. Feb. 2013

   [...] Tatort Geschichte und der Blogpost fast fertig. Drei Links habe ich noch. Es geht um Sicherheit. Martin Schmetz bewertet drüben im Sicherheitspolitik-Blog die europäische Cybersecurity-Strategie und die Executive Orders Obamas zur Cybersicherheit. Gegen [...]

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein. reCAPTCHA

netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.