TAGESSPIEGEL
BACKGROUND

Cybersecurity

EU-Cyberdiplomatie mit Zähnen versehen

Die Threat Reports von ENISA und BSI zeigen, wie gravierend die Cybersicherheitsbedrohung für europäische Unternehmen, Regierungen und staatliches Handeln ist. Deutschland als größte Volkswirtschaft in einem Binnenmarkt der EU-27 braucht eine gemeinsame Cybersicherheit und Cyberabwehr.

von **Annegret Bendiek & Matthias Schulze**

veröffentlicht am 02.12.2021
aktualisiert am 28.12.2022

Im Koalitionsvertrag finden sich **Hinweise auf das cyberaußenpolitische Profil**, das sich die **Bundesregierung** geben könnte. So lehnt die Ampelkoalition beispielsweise Hackbacks als Mittel der Cyberabwehr ab. Wenn die Regierung diese grundsätzlich **richtige strategische Ausrichtung** in der Cybersicherheitspolitik durchhalten will, ist es dringend geboten, nicht nur das IT-Schwachstellenmanagement und die Vorgaben **„security-by-design/default“** zu stärken.Vielmehr setzt es zwingendermaßen eine **Attributionsfähigkeit Deutschlands und der EU** voraus, um Verantwortliche für scherwiegende Cyberangriffen glaubhaft zur Rechenschaft zu ziehen – und diese muss dringend verbessert werden.

Dabei muss **klarer nach Angriffstypen unterschieden** und die **geltenden Rechtsprinzipien zur Beurteilung von Angriffen** geschärft werden. Um dem Primat der Politik den Vorrang vor militärischen

Gegenmaßnahmen, wie im Falle von sogenannten „Hackbacks“, einräumen zu können, ist es nur konsequent, den **politischen und diplomatischen Instrumentenkasten** auszubauen. Klar ist, dass Deutschland hier wenig allein ausrichten kann, umso wichtiger wird **die Rolle der EU-Kommission** in der Cybersicherheit. Cybersicherheit ist eine Gemeinschaftsaufgabe.

Die **27 EU-Staaten** haben sich im Dezember 2020 auf ihre letzte Cybersicherheitsstrategie geeinigt. Im Vergleich zu klassischen Fragen der gemeinsamen Außen- und Sicherheitspolitik ist der Konsens in der EU-27 in der Cybersicherheit relativ leicht hergestellt. **Qualifizierte Mehrheitsentscheidungen** einzuführen, um Cybersanktionen zu beschließen, dürfte kein Hexenwerk sein.

Die **EU-Cyberdiplomatie setzt auf die zivilpolitischen Cybersanktionen** und will offensive militärische Gegenmaßnahmen möglichst vermeiden. Cyberdiplomatie ist ein Kernelement von Cybersicherheit, denn ohne vertrauens- und sicherheitsbildende Maßnahmen keine Sicherheit. **Cyberdiplomatie und die Rolle der EU** klingen ungemein bürokratisch, dabei sind sie politisch durchaus brisant, wenn etwa Staatsbedienstete des **ehemaligen russischen Geheimdienstes GRU** mit Reise- und Kontensperrungen belegt werden. Zudem kann diplomatisches Versagen immer in eine nicht-intendierte Konflikteskalation münden. Umso wichtiger ist es, dass die Cyberdiplomatie Europas Ross und Reiter von schwerwiegenden Cyberangriffen gegen die EU benennen kann. Diese **Fähigkeit zur Attribution** steckt noch in den Kinderschuhen wie eine neue Studie der Stiftung Wissenschaft und Politik feststellt.

Politische Attributionen sind zu beschleunigen

Die **Attribution von Cyberoperationen** ist eine technisch und rechtliche Voraussetzung für die effiziente Cyberdiplomatie, aber nicht alle Mitgliedstaaten haben entsprechende Kapazitäten. Allerdings ist sie nicht Sache der EU, sondern der Mitgliedstaaten. Dabei agieren diese im Zweifel opportunistisch g bei der politischen Benennung von Verantwortlichen für Cyberangriffe. Da diplomatische Reaktionen auf

Cyberangriffe im Rat einstimmig beschlossen werden, müssen jedoch alle mitgehen, um sich der **gemeinsamen EU-Attribution** und der Verurteilung einer im staatlichen Auftrag agierenden Person/Gruppe anzuschließen. Das ist praktisch wenig realitätstauglich.

Ob danach die Verurteilung auch noch öffentlich gemacht werden kann, um international den Druck gegen Angreifer durch das **„naming und shaming“** zu erhöhen, ist damit auch noch nicht beschlossen. Die derzeitige Schwäche ist hausgemacht und das Resultat der Einstimmigkeit im Rat. Das ist insofern schwerwiegend, als dass der **Erfolg des EU-Binnenmarkts** maßgeblich davon abhängig ist, dass die Wertschöpfungs- und Lieferketten, aber auch **demokratisch verfasste Strukturen und Prozesse** einwandfrei funktionieren können.

Diplomatie mit mehr Zähnen versehen

Die EU-Cyberdiplomatie sieht schärfere, diplomatische Maßnahmen jenseits geschriebener Protestnoten vor, allerdings sind diese Instrumente vergleichsweise schwach – ganz im Gegensatz zu den Mitteln der **USA und ihrer Five-Eyes-Partner**. Die Verhängung von internationalen Haftbefehlen oder „Cybersanktionen“, wie Einreiseverbote oder das Einfrieren von Bankkonten gegen ausländische Geheimdienstmitarbeiter, dürfte deren Arbeit kaum operativ beeinträchtigen und ist in erster Linie rein **symbolischer Natur.**

Dennoch versucht die EU damit **die Geltung des Völkerrechts** zu unterstreichen, vereinbarte Normen für verantwortliches Staatenverhalten ernsthaft zu untermauern und nicht zuletzt andere „like minded“ Staaten dazu zu animieren, sich den **EU-Cybersanktionen** anzuschließen. Das Unterbinden von derartigen Angriffen wird allerdings durch nicht-bindende Moralprinzipien kaum gelingen. Eine primär politische Lösung und eine schnelle **Reaktionsfähigkeit seitens der EU** ist eine notwendige Bedingung für Cybersicherheit. Der Instrumentenkasten ist an dieser Stelle noch weiter auszubauen.

Was nun getan werden muss

Analysiert man die Fälle, in denen die EU bisher **Cybersanktionen** verhängt hat, zeigen sich weitere Defizite der bisherigen Attribution. Beginnend bei der Tatsache, dass nicht alle EU-Mitgliedsstaaten eindeutig darüber sind, was einen **Cyberangriff** ausmacht. Ob eine Organisation einem tatsächlichen Angriff oder nur einem Angriffsversuch ausgesetzt ist, ist mitunter schwer zu beantworten. Können Täter, wie im Falle der **„close access operation" des russischen Geheimdiensts gegen die Organisation für das Verbot chemischer Waffen** in Den Haag 2018 physisch verhaftet werden, lässt sich die Frage positiv beantworten.

Von den Millionen Cyberangriffen pro Jahr werden etliche von IT-Sicherheitsmaßnahmen abgefangen und stellen somit nichts weiter als **unbedeutende Ereignisse aus dem IT-Security-Alltag** von Administratoren da. Diese sind a priori oft nicht als böswillige Angriffsversuche von Staaten zu erkennen, da sich die Wirkung eines Angriffs erst bei der **Ausführung von Schadcode** manifestiert. Erst wenn nach forensischer Analyse solcher Malware unter Bezugnahme von zusätzlicher Threat-Intelligence Verbindungen zu Angriffsinfrastrukturen oder Tools von bekannten APT-Gruppen sichtbar werden, wird dieser Vorfall von betroffenen Organisationen als bedrohlicher Akt von außen interpretiert werden. Genau dieses Muster zeigte sich auch **beim Hack des Deutschen Bundestages**. Das Problem: Bei einer Großzahl von Cybervorfällen wird diese Analyse aber aufgrund von Personalmangel nicht durchgeführt.

Genauso ist der **Ursprung eines Cyberangriffs**, technisch gesehen, nur schwer zu lokalisieren. Diese Attribution setzt technisches Know-how und finanzielle Ressourcen voraus, um fehlende Informationen bei privaten IT-Sicherheitsunternehmen einkaufen zu können. Zudem setzt Attribution oft nachrichtendienstliche Erkenntnisse voraus.

Die EU ist aber **finanziell und personell in der Cybersicherheit** auch durch die mitgliedstaatlichen Fähigkeiten im Vergleich zu anderen Akteuren schlecht aufgestellt. **ENISA** ist immer noch mehr eine Beratungs- und Awareness-Agentur, als dass sie faktisch in der konkreten Cyberabwehr vor Ort oder bei der technischen Attribution koordiniert durch den **EAD** und unter **Hilfestellung der EU-Cybereinheit in der**

Kommission tätig werden könnte. Noch vertrauen viele Mitgliedstaaten eher auf nationale Strukturen. Dabei können nationale Behörden aber nicht die kollektive Handlungsfähigkeit der EU schultern, sondern bestenfalls nur ergänzen. Es braucht einen konsequenten **Ausbau der Threat Intelligence auf EU-Ebene**. Dabei ist zumindest ermutigend, dass die Bereitschaft der Mitgliedstaaten Attributionsinformationen zu teilen, deutlich zugenommen hat.

Die Politik hinkt dem Recht hinterher

Nicht zuletzt zeigt die Studie auf, dass neben der technischen Attribution die rechtliche Bewertung von Cybervorfällen in den Mitgliedstaaten und damit die diplomatische Gegenreaktion sehr unterschiedlich ausfallen kann. Wenn der gleiche **Vorfall wie WannaCry 2017** von Mitgliedstaaten unterschiedlich bewertet wird, wird es problematisch. Sieht Land A cyberkriminelle Motive wie die Erpressung von Lösegeld, Land B und C aber den Vorfall als politische Zwangsmaßnahme eines marginalisierten Nordkoreas, wird eine einheitliche Gegenreaktion unwahrscheinlich. Die EU will auf **Cyberoperationen** angemessen reagieren. Niedrigschwellige Angriffe sollten mit Soft-Power Maßnahmen beantwortet werden, größere Angriffe mit Milliarden von Schäden auch mit schärferen Maßnahmen, bis hin zur militärischen Reaktion bei **extremen Katastrophenereignissen**. Das ist in der Theorie plausibel, wird aber in der Praxis bisher nicht kohärent angewendet.

Cyberspionage gegen politische Institutionen ist Normalität, da sie völkerrechtlich nicht verboten ist – alle Staaten spionieren. Beim Angriffsversuch auf die Organisation für das Verbot chemischer Waffen in Den Haag konnten die Täter gefasst werden, bevor auch nur irgendein Schaden entstanden ist. Obwohl diese Fälle extrem unterschiedlich gelagert sind, hatten alle die gleichen Konsequenzen zur Folge: Haftbefehle wurden erlassen, Konten eingefroren und Reisebeschränkungen verhängt. Gleichzeitig zogen andere, krassere Fälle wie der **konkrete Versuch der Beeinflussung** der französischen Präsidentschaftswahl 2017, zu keiner Reaktion der EU und das obwohl hier der Kern der Demokratie betroffen war.

Die EU handelt hier also bisher nicht nach den Rechtsprinzipien, die sie zur **Klassifizierung von Cyberangriffen** zugrunde gelegt hat. Das ist insofern problematisch, als dass Deutschland und die EU mit ihrer Cyberdiplomatie Normen für staatliches Verhalten im Cyberraum stärken wollen. Cybersanktionen sollten hohen rechtlichen Kriterien genügen, da gegen sie Berufung vor dem **Europäischen Gerichtshof** eingelegt werden kann. Deutschland und die EU müssen ihre Cyberdiplomatie jetzt stärken, wenn sie ihr cybersicherheitspolitisches **Paradigma von Resilienz und rechtstaatlich abgesicherter Cyberabwehr** aufrechterhalten wollen und müssen.

Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU/Europa, Matthias Schulze stellvertretender Forschungsgruppenleiter für Sicherheitspolitik bei der Stiftung Wissenschaft und Politik.

In unserer Reihe „Perspektiven“ ordnen unsere Kolumnist:innen regelmäßig aktuelle Entwicklungen, Trends und Innovationen im Bereich Cybersicherheit ein. Bisher erschienen:

Sven Herpig: Digitalbehörde: Nur mit Sicherheit!

Oleg Brodt: Das Land der Cybereinhörner

Sven Herpig: Cybersicherheitsarchitektur am Limit