European Union Agency for Cybersecurity

Europäische Cyberabwehrfähigkeiten durch eine Stärkung der ENISA erhöhen, um eine engere außen- und sicherheitspolitische Zusammenarbeit zu fördern und aktuellen und zukünftigen Bedrohungslagen zu begegnen.

Konferenz zur Zukunft Europas

Themenfeld: Europäische Außenbeziehungen

Berlin, 04.01.2022

Inhaltsverzeichnis

1. Abstract

Cyberangriffe sind kein nationales, sondern ein grenzüberschreitendes Problem, daher muss die **Verbesserung der Cybersicherheit** auf EU-Ebene erfolgen. Durch gehäufte Angriffe aus dem Ausland hat sie an Bedeutung für die Gemeinsame Außen- und Sicherheitspolitik der EU gewonnen. Die Eindämmung dieser Angriffe muss also nicht nur auf EU-Ebene erfolgen, sondern auch zu einem Bestandteil der EU-Sicherheitspolitik werden.

Daher schlagen wir vor, an die 2004 gegründete Agentur ENISA über die Verordnung [COM (2017) 477] hinaus im Rahmen eines erweiterten Aufgabenfeldes operative und weitere koordinierende Befugnisse durch eine neue Verordnung zu vergeben. Besonders wichtig in unseren Augen ist die Einsetzung eines europäischen Cyber-Abwehrzentrums, angesiedelt in der ENISA. Ein solches Zentrum hat die Chance, die Koordinierung der Cybersicherheit in den kommenden Jahren aktiv zu gestalten und somit perspektivisch zu einer wichtigen Säule der EU-Sicherheit zu werden.

Fraglich bleibt, ob für die Summierung von operativen Befugnissen auf EU-Ebene die Einstimmigkeit im Rat gefunden werden kann.

Eine Stärkung der ENISA ist dringender denn je. Spätestens mit der Corona-Pandemie ist uns allen bewusst geworden, wie abhängig wir als Gesellschaft, unsere staatlichen Institutionen und unsere Wirtschaft von funktionstüchtiger Infrastruktur sind. Vom Umspannwerk über Krankenhausversorgung bis hin zur Universität hängt alles am weltweiten Datennetz und birgt bei geringem Schutz immense Risiken. Daher braucht es nach der Entfristung der ENISA 2017 nun eine breite Stärkung der Agentur, weil die ENISA für weitere koordinierende und operative Mittel und Fähigkeiten ein ausgezeichnetes Fundament bietet.

2. Problemaufriss

2.1 Aktuelle Probleme im Themenfeld

Gestohlene oder geleakte Daten, Angriffe auf Unternehmen, Bürger oder staatliche Einrichtungen mit Schadsoftware, Betrug, Geldwäsche und Erpressung und Angriffe auf Demokratien und Wahlen sind Probleme einer vielseitigen Cyberbedrohungslage. Cybervorfälle haben neben Einzelpersonen auch negative Folgen für Gemeinschaften und Organisationen. Sie sind spürbar auf nationaler, europäischer sowie globaler Ebene. Die Cybersicherheit ist ein diplomatisches Thema in den Außenbeziehungen und wird verstärkt Bestandteil der sich neu entwickelnden Verteidigungspolitik der EU. Eine Schwierigkeit Cyberangriffe abzuwehren, liegt darin, dass die Angriffe sehr lange unentdeckt bleiben, da digitale Systeme sehr komplex sind. Auch ist die Ermittlung, Abwehr und Schadensbehebung von Cyberangriffen sehr kostenintensiv. Ein besonders großes Problem ist, dass auf EU-Ebene keine gemeinsamen Richtlinien für die Bekanntmachung von Sicherheitsvorfällen vorhanden sind. Dadurch kommt es zu einer Verzögerung von Meldungen von Sicherheitsverletzungen und es können nicht rechtzeitig Abwehrmaßnahmen ergriffen werden. Des Weiteren ist die Fähigkeit der EU auf politischer und operativer Ebene zu handeln beschränkt, wenn es einen größeren, grenzüberschreitenden Cyberangriff gibt. Grund

dafür ist die fehlende Integration der Cybersicherheit in die auf EU-Ebene bestehenden Mechanismen, welche die Krisenreaktionen koordinieren. Bisher bestand eine Abhängigkeit zwischen den EU-Mitgliedstaaten und Dritten aus technologischer sowie industrieller Sicht. Deshalb fordern Abgeordnete des EU-Parlaments, dass die EU aus technologischer Sicht unabhängiger werden muss und die Investitionen in Personal und Cyberabwehrfähigkeiten erhöht werden.

2.2 Künftige Herausforderungen im Themenfeld

Eine große Herausforderung in dem Themenfeld ist die immer weitere Zunahme von Cyberangriffen, die um einiges raffinierter werden und größere Schäden anrichten können. Ein Grund der Zunahme dieser Cyberattacken ist die Corona-Pandemie, denn immer mehr Unternehmen bringen ihre Mitarbeiter*innen dazu, im Home-Office zu arbeiten, weshalb der Bedarf an technischen Geräten gestiegen ist. Dazu gehört, dass es zur digitalen Kommunikation kommt und private bzw. geheime Informationen an Dritte gelangen können, da viele Unternehmen bis heute immer noch nicht über ausreichende Schutz- und Abwehrmaßnahmen verfügen, um ein sicheres Remote Working zu ermöglichen. Dies wird von kriminellen Cyberangreifern leicht erkannt, weshalb sie häufiger angreifen. Zum einen werden von den Unternehmen Informationen gestohlen, genauso wie von verschiedenen Organisationen, die unter Angriffen leiden, da Angreifer ihre eigenen Tatmotive haben.
Durch die vielen Angriffe auf die Unternehmen ist es notwendig, den Bürgern ein sicheres Netz zu bieten, da nur so die Vorteile der Digitalisierung genutzt werden können und Schaden abgewehrt werden kann.
In der Zeit, in der die Digitalisierung und die Vernetzung mit anderen wesentlich zugenommen haben, ist es wichtig, bestehende Maßnahmen auf EU-Ebene zu aktualisieren, um zum Beispiel bestimmte Dienste und Infrastrukturen vor Cybergefahren zu schützen.
Durch Cyberangriffe entsteht vermehrt ein finanzieller Schaden, doch nicht nur die Angriffe bringen Kosten mit sich, auch der Schutz vor diesen Angriffen, wie auch die Ermittlung und die Schadensbehebung muss bezahlt werden. Die Verluste von Unternehmen sind dabei nicht nur materieller Natur, sondern auch das Image eins Unternehmens kann unter einer geglückten Attacke leiden.

3. Lösungsvorschläge

3.1 Präsentation Idee für politische Veränderungen:

Die Cyberabwehr wird für die Wirtschaft größtenteils durch private Unternehmen gewährleistet, aber auch staatliche Akteure sind an der Abwehr und vor allem der Ermittlung nach Angriffen beteiligt. So nimmt das Nationale Cyber-Abwehrzentrum (Cyber-AZ) in Deutschland eine zentrale Rolle ein, da dieses die Arbeit von acht Behörden koordiniert, so z. B. des BND und des BSI. Um den zukünftigen Herausforderungen im Bereich Cyberabwehr zu begegnen und auch mit dem Blick auf eine noch in ferner Zukunft liegende Europäische Armee, welche durch eine Zusammenarbeit im Bereich der Cybersicherheit realistischer wird, kann es sich als sinnvoll erweisen, auf EU-Ebene die European Union Agency For Cybersecurity (ENISA) als zentrale Behörde auszubauen. Die Koordination der Cyberabwehr und der Informationsaustausch der nationalen Behörden soll von der ENISA gewährleistet werden, da diese bereits jetzt beratend und koordinierend tätig ist, während Institutionen wie

das Kompetenzzentrum für Cybersicherheit in Bukarest vor allem die Forschung und Ausbildung im Bereich der Cybersicherheit stärken sollen. Eine zentrale Institution zur Koordination ist sinnvoll, da so ein Flickenteppich von verschiedensten Kompetenzen und Informationswegen vereinfacht wird. Außerdem kommt es zu einer schnelleren Kommunikation zwischen den staatlichen Behörden, wodurch der Schaden durch Angriffe minimiert wird. So können trotz sich schnell entwickelnder Bedrohungslagen im Bereich der Cybersicherheit Sicherheitslücken schneller gefunden und bekämpft werden.

3.2. Zur Umsetzung benötigte Instrumente/Mechanismen

3.2.1 Vorhandene Instrumente:

Die NIS Richtlinie von 2016 legt fest, dass Behörden über stattgefundene relevante Cyberattacken informiert werden müssen, sowie die Einrichtung von Computer Security Incident Response Teams, welche durch die Task Force (TF C Sirt) akkreditiert werden. Sie bestehen aus IT-Sicherheitsfachleuten, welche bei der Warnung und Lösung von Sicherheitslücken mitwirken. Unterstützt werden diese von der ENISA, welche einzelstaatlichen Behörden sowie EU-Institutionen Sicherheitsratschläge erteilt und als Austauschforum für bewährte Verfahren fungiert. Auf deutscher Ebene besitzt das Cyber-AZ eine koordinierende Aufgabe, in welcher sich deutsche Behörden über aktuelle Herausforderungen, Sicherheitslücken und Lösungsoptionen austauschen. Die EU setzt auch auf internationale Kooperation, primär mit der NATO z.B. durch Abwehrübungen wie die jährliche “locked Shield” Übung.

3.2.2 Neu einzuführende Instrumente:

Einführung eines gesetzlichen EU-weiten Sicherheitsstandard NIS II für IT-Systeme sowohl für kritische Infrastruktur sowie staatliche Akteure und dessen ständige Anpassung an neue Technologien und Bedrohungsszenarien. Einführung eines Sanktionsmechanismus gegen staatlich organisierte Cyberattacken, um abschreckend zu wirken. Schaffung einer EU-weiten Datenbank über Cyberangriffe unter der Aufsicht der ENISA. Einrichtung einer Versammlung in der ENISA von Vertretern des Cyber-AZ und den anderen europäischen Pendants in einer monatlichen Versammlung. Einrichtung eines Kontrollorgans unter der Leitung der ENISA, um stichprobenartig Sicherheitssysteme auf den EU-weiten Standard zu überprüfen. Einrichtung einer Kooperations-Abteilung, um die Cyberdiplomatie, Übungen mit der NATO und anderen Partnern zu intensivieren und zu zentralisieren.

4. Chancen und Risiken

4.1 Skizze zur Umsetzung/Vorgehensweise

Nachdem die Europäische Kommission und das Parlament seine Zustimmungen gaben, wird im Jahr 2022 interinstitutionelle Verhandlungen zur Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS II) starten. Anschließend haben die Mitgliedstaaten zwei Jahre Zeit, NIS II in die nationalen Gesetze einzuarbeiten.

Die Einführung von Sanktionsmechanismen gegen staatlich organisierte Cyberattacken müsste als neues Instrument im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU einstimmig vom Europäischen Rat beschlossen werden. Der Idee der Schaffung einer EU-weiten Datenbank unter der Aufsicht der ENISA geht voraus, dass die Nationalstaaten bereits Datenbanken für Cyberangriffe etabliert haben. Daraufhin können die Länder ihre gesammelten Daten an die ENISA weitergeben, die in einer neuen Abteilung diese sammeln, auswerten und speichern würde. Der Vorschlag einer monatlichen Versammlung in der ENISA, bestehend aus Vertretern des Cyber-AZ und anderer europäischer Pendants erfordert Vorbereitungen. Die ENISA könnte hierbei eine eigene Abteilung bereitstellen, die sich mit der Planung und Vorbereitung solcher Meetings beschäftigt und sich um das Agenda-Setting, passend zu den aktuellen Themen kümmert. Die Errichtung eines Kontrollorgans und einer Kooperations-Abteilung unter der Leitung der ENISA sind mögliche, neu einzuführende Instrumente. Hierbei ist es vorwiegend wichtig, dass man diese mit genügend Personal und Spezialisten ausstattet, die das nötige Fachwissen mitbringen, um die geforderten Ergebnisse erzielen zu können.

4.2 Hindernisse und ungeklärte Fragen

Beim Ausbau der Cyberabwehrfähigkeiten in Europa gibt es weitreichende Vorteile, die eine Vernetzung und Zusammenarbeit zwischen verschiedenen europäischen und nationalstaatlichen Institutionen zweckdienlich machen. Neues Know-how auf dem Gebiet kann zur Bekämpfung von Terror und Kriminalität genutzt werden. Inwiefern das mit nationalem und EU-Recht vereinbar ist, muss geklärt werden. Man kann auch überlegen, ob die gemeinsamen Ressourcen auch für die Entwicklung neuer Technologien genutzt werden sollen. Eine besonders problematische Möglichkeit, die sich aus einer besseren Cyberabwehr ergibt, ist das Wissen um Sicherheitslücken und die Frage, ob diese durch europäische Geheimdienste genutzt werden sollten. Spionage ist auch einer der größten Konflikte in der Thematik, da man sich überlegen muss, gegen wen man sich verteidigen will. Gruppen von Kriminellen mit wirtschaftlichen Interessen? Russland und China oder auch eigene Verbündete wie die USA, die seit dem NSA-Skandal bewiesen haben, dass auch sie europäische Interessen missachten? Aufgrund dieser weiten Spanne an potenziellen Bedrohungsszenarien und Angriffen, ist eine hochfrequentierte, umfassende und regelmäßige Evaluierung durch Experten wichtig.

5. Fazit

Cyberangriffe sind kein nationales, sondern ein grenzüberschreitendes Problem, daher muss die Verbesserung der Cybersicherheit auf EU-Ebene erfolgen. Durch gehäufte Angriffe aus dem Ausland hat sie an Bedeutung für die Gemeinsame Außen- und Sicherheitspolitik der EU gewonnen. Die Eindämmung dieser Angriffe muss also nicht nur auf EU-Ebene erfolgen, sondern auch zu einem Bestandteil der EU-Sicherheitspolitik werden.

Daher schlagen wir vor, an die 2004 gegründete Agentur ENISA über die Verordnung [COM (2017) 477] hinaus im Rahmen eines erweiterten Aufgabenfeldes operative und weitere koordinierende Befugnisse durch eine neue Verordnung zu vergeben. Besonders wichtig in unseren Augen ist die Einsetzung eines europäischen Cyber-Abwehrzentrums, angesiedelt in der ENISA. Ein solches Zentrum hat die Chance, die Koordinierung der Cybersicherheit in den kommenden Jahren aktiv zu gestalten und somit perspektivisch zu einer wichtigen Säule der EU-Sicherheit zu werden.
Fraglich bleibt, ob für die Summierung von operativen Befugnissen auf EU-Ebene die Einstimmigkeit im Rat gefunden werden kann.
Eine Stärkung der ENISA ist dringender denn je. Spätestens mit der Corona-Pandemie ist uns allen bewusst geworden, wie abhängig wir als Gesellschaft, unsere staatlichen Institutionen und unsere Wirtschaft von funktionstüchtiger Infrastruktur sind. Vom Umspannwerk über Krankenhausversorgung bis hin zur Universität hängt alles am weltweiten Datennetz und birgt bei geringem Schutz immense Risiken. Daher braucht es nach der Entfristung der ENISA 2017 nun eine breite Stärkung der Agentur, weil die ENISA für weitere koordinierende und operative Mittel und Fähigkeiten ein ausgezeichnetes Fundament bietet.