CYBERSICHERHEIT

Im März 2018 bestätigte das Bundesinnenministerium einen gravierenden IT-Sicherheitsvorfall. Demnach sind ausländische Hacker in das Datennetzwerk des Bundes und der deutschen Sicherheitsbehörden eingedrungen. Dabei wurde Schadsoftware eingeschleust, um Daten illegal abzugreifen. Cyberangriffe nehmen seit Jahren zu. Allein die Bundeswehr verzeichnet jeden Tag rund 4.500 illegale Zugriffsversuche von außen auf ihre Netzwerke. Zahlreiche dieser Cyberangriffe werden der „Gefahrenstufe hoch" zugerechnet.

Formen von Cyberbedrohungen

Staat, Wirtschaft und Gesellschaft profitieren von der zunehmend vernetzten, digitalisierten Welt. Gleichzeitig werden sie jedoch verwundbarer gegen Angriffe im Cyberraum, also im Internet und den damit verbundenen Netzwerken. Urheber dieser Attacken sind andere Staaten, terroristische Organisationen und kriminelle Vereinigungen. Da Schadsoftware leicht und kostengünstig erhältlich ist, handelt es sich auch zunehmend um einzelne Cyberkriminelle. Die kriminellen Methoden sind vielfältig, Angriffe häufen sich und werden seit Jahren immer schwerwiegender: Die Bedrohungen reichen von Datenmissbrauch und Wirtschaftsspionage über die Schädigung kritischer Infrastrukturen wie Stromnetze bis hin zur Störung der Regierungs- und Militärkommunikation. Auch die Server und digital gesteuerten Waffensysteme der Bundeswehr können zur Zielscheibe werden.

Eine besondere Gefahr für offene, demokratische Gesellschaften ist die gezielte Beeinflussung der öffentlichen Meinung mithilfe digitaler Kommunikation. Dazu zählt zum Beispiel die Steuerung von Diskussionen in sozialen Netzwerken oder die Manipulation von Informationen auf Nachrichtenportalen. Bei dieser so genannten hybriden Kriegführung nutzen Angreifer eine Kombination aus Militäreinsätzen, wirtschaftlichem Druck, Cyberangriffen und Propaganda. Ziel ist es nicht nur, Schaden anzurichten, sondern Gesellschaften zu destabilisieren. Die Täter operieren entweder anonym oder bestreiten ihre Beteiligung an den Vorfällen. So werfen die USA Russland vor, die US-amerikanischen Präsidentschaftswahlen im Jahr 2016 beeinflusst zu haben. Am 15. März 2018 verhängten die USA deshalb Sanktionen gegen 19 Russen, die im Verdacht stehen, sich in die US-Wahl eingemischt zu haben. Mögliche Bankkonten und Vermögenswerte der Betroffenen wurden in den USA eingefroren und US-Staatsbürgern wurde verboten, mit ihnen Geschäfte zu machen. Russland kündigte daraufhin „Vergeltungsmaßnahmen" an. Am 16. April 2018 haben Großbritannien und die USA zudem eine gemeinsame Erklärung veröffentlicht, in der sie Russland vorwerfen, illegal auf britische und US-amerikanische Regierungsnetzwerkgeräte zugegriffen zu haben. Ziel sei es gewesen, diese Geräte für weitere Cyberangriffe zu nutzen.

nach: Bundesministerium der Verteidigung: Hybride Bedrohungen, www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen, Bundeswehr-Journal: „Russische Cyber-Attacken auf westliche IT-Infrastrukturen?", www.bundeswehr-journal.de/2018/russische-cyber-attacken-auf-westliche-it-infrastrukturen, 18. April 2018, „Mutmaßliche Wahlbeeinflussung. USA verhängen Sanktionen gegen Russland", www.tagesschau.de/ausland/usa-russland-sanktionen-wahlbeeinflussung-101.html, 15. März 2018, Bundesministerium der Verteidigung: Weißbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Juni 2016, Seite 36 f.

Gruppenarbeit/Plenum: Teilen Sie sich in neun etwa gleich große Gruppen auf. Jede Gruppe befasst sich mit einer aktuellen Cyberbedrohung aus dem Kapitel „2.5 Aktuelle Phänomene" (S. 10 bis 23) des Berichts „Cybercrime. Bundeslagebild 2016" des Bundeskriminalamts, erhältlich unter www.bka.de > Aktuelle Informationen > Statistiken und Lagebilder > Lagebilder und Jahresberichte > Bundeslagebilder Cybercrime. Fassen Sie die beschriebene Bedrohung und das im Text genannte Fallbeispiel stichpunktartig in einem Handout zusammen. Recherchieren Sie bei Bedarf weitere Informationen, zum Beispiel beim Bundesamt für Sicherheit in der Informationstechnik unter www.bsi.bund.de. Verteilen Sie die Handouts im Plenum.

Strategien und Partnerschaften für Cybersicherheit

In ihrer Cyber-Sicherheitsstrategie hat die Bundesregierung daher Maßnahmen zum Schutz des Cyberraums festgelegt. Besonders wichtige Gremien sind das Nationale Cyber-Abwehrzentrum und der Nationale Cyber-Sicherheitsrat. Ihre Einrichtung wurde im Jahr 2011 beschlossen. Im **Nationalen Cyber-Abwehrzentrum** tauschen sich alle Bundesbehörden regelmäßig über die aktuelle Bedrohungslage im Cyberraum aus und koordinieren ihre Maßnahmen. Das Nationale Cyber-Abwehrzentrum soll IT-Sicherheitsvorfälle früh erkennen, schnell und umfassend bewerten und Handlungsempfehlungen erarbeiten. Im **Nationalen Cyber-Sicherheitsrat** arbeiten Staat und Wirtschaft zur Abwehr von Cyberbedrohungen zusammen. Mögliche Krisenursachen sollen so frühzeitig identifiziert und beseitigt werden. Der Cyber-Sicherheitsrat tagt dreimal jährlich. Außerdem kommt er bei aktuellen Anlässen zusammen. Vertreten sind verschiedene Bundesministerien sowie Verbände und Organisationen der Wirtschaft. Zur Abwehr von Cyberbedrohungen und zur Verteidigung des Cyberraums hat die **Bundeswehr** außerdem den militärischen Organisationsbereich Cyber- und Informationsraum (CIR) gegründet. Er schützt und betreibt das IT-System der Bundeswehr, sowohl im Inland als auch im Einsatz. Aufklärung und Wirkung im Cyberraum sollen so gestärkt und weiterentwickelt werden. Außerdem arbeitet das Verteidigungsministerium mit dem **NATO Cooperative Cyber Defense Centre of Excellence** zusammen. Jedes Jahr nehmen IT-Spezialisten der Bundeswehr an der NATO-Übung Locked Shields teil. Darin wird ein Cyberangriff simuliert, der von den Teilnehmern abgewehrt werden muss. Nach dem neuesten Hackerangriff auf das Regierungsnetzwerk fordert das Bundesinnenministerium, dass die sogenannten Logfiles, also alle Daten, die der Nutzer eines Computers erzeugt – Informationen über besuchte Websites und verschickte E-Mails –, länger gespeichert werden sollten. Denn je länger ein Angriff durch die Analyse der Logfiles zurückverfolgt werden kann, desto mehr Informationen bekommt man über die Strategie des Angreifers.

nach: Bundesministerium der Verteidigung, www.bmvg.de/de/themen/cybersicherheit

Partnerarbeit/Plenum: Neue Sicherheitsmaßnahmen im Internet haben immer auch Auswirkungen auf Grundrechte wie die freie Meinungsäußerung oder das Recht auf Privatsphäre. Erörtern Sie, inwieweit Unternehmen, der Staat und die Bürgerinnen und Bürger selbst Verantwortung für mehr Sicherheit im Cyberraum übernehmen sollten.

Präventive IT-Schläge?

„Der Kampf gegen die dunkle Seite der Macht in der Computerwelt ist kein einfacher. Die Guten haben häufig das Nachsehen, denn sie sind immer einen Schritt zurück. Sie sind zum Reagieren verdammt. Während die Hacker ständig agieren und ihre schädlichen Quellcodes in fremde Rechner einschleusen, sitzen die Männer und Frauen der Cyberabwehr in Lauerstellung und fahnden nach fremden Datenspuren in ihren Netzwerken. Selbst aktiv werden dürfen sie nicht. Die deutsche Rechtsprechung erlaubt kein ‚Hack back'. Leider. Die Bundesregierung ist bisher gescheitert, Versuche zu legalisieren, um bei Angriffen im Internet zurückschlagen zu dürfen. Viele Experten warnen zudem vor aktiven ‚Back Hacks', weil sie der Ansicht sind, dies führe nur zu einer weiteren Eskalation und würde letztlich keine Angriffe auf kritische Infrastrukturen wie Elektrizitäts- und Wasserwerke verhindern. Diese Entscheidung gilt es in der Zukunft zu überdenken."

Dirk-Ulrich Brüggemann: „Hacker-Angriff auf deutsche Ministerien – Computerwelt ist verwundbar", Neue Westfälische, www.nw.de, 1. März 2018

Plenum: Sollte es einem Staat bei einem Cyberangriff aus dem Ausland möglich sein, gegebenenfalls einen Server im Ausland unschädlich zu machen? Bislang gibt es keine internationalen Regeln, wie Staaten auf einen Cyberangriff reagieren könnten. Führen Sie eine Pro-Kontra-Diskussion zu sogenannten aktiven „Hack-backs".