BSI

Zur Zukunft der Cyber-Sicherheit

[13.05.2026] Mit Blick auf hybride Bedrohungen, Cyber Conflict und digitale Souveränität zieht BSI-Chefin Claudia Plattner eine programmatische Zwischenbilanz. Cyber-Sicherheit wird zur Schnittstelle von Sicherheits- und Digitalpolitik. Im Fokus der Arbeit stehen automatisierte Angriffe, zivile Cyber Defense und digitale Souveränität.

Ein Jahr, nachdem die jetzige Bundesregierung ihre Arbeit aufgenommen hat, zieht die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI), Claudia Plattner, eine ausführliche Zwischenbilanz. Erstmals arbeite das BSI als Deutschlands Cyber-Sicherheitsbehörde mit zwei Bundesministerien eng zusammen: in Fragen der Sicherheit wie gewohnt mit dem Bundesinnenministerium, und hinsichtlich Digitalisierung mit dem neu gegründeten Bundesministerium für Digitales und Staatsmodernisierung. Staatliche Sicherheit und Digitalisierung müssten heute zusammen gedacht werden. Das BSI versteht sich als Schnittstelle zwischen Sicherheitsbehörden und Digitalpolitik – möglich sei dies wegen der hervorragenden Zusammenarbeit mit Innen- und Digitalressort.

Cyber-Sicherheit automatisieren

Cyber Crime hat sich in den vergangenen Jahren zu einer teilautomatisierten Industrie mit hochprofessionellen Strukturen entwickelt. Die Angriffe werden immer komplexer und performanter. „Das bedeutet, dass wir Cyber-Sicherheit genauso automatisieren müssen wie unsere Gegner ihre Angriffe“, so Plattner. Daher baue das BSI gemeinsam mit dem Bundesinnenministerium einen Cyberdome für Deutschland. Diese nationale Schutz-Infrastruktur zur Früherkennung, Analyse und Abwehr von Cyber-Angriffen soll Kritische Infrastrukturen, staatliche Institutionen, Unternehmen und die Gesellschaft schützen und Schäden durch Cyber-Angriffe minimieren. Zur technischen Ausgestaltung oder konkreten Aufbauschritten des digitalen Schutzschirms äußerte sich die BSI-Präsidentin nicht.

Sie verwies indes auf zwei neue Gesetze: die nationale Umsetzung der EU-Richtlinie NIS2 und der Cyber Resilience Act (CRA). „Diese beiden Cyber-Sicherheitsgesetze werden – parallel mit den Automatisierungsmaßnahmen des Cyberdomes – die Resilienz Deutschlands im digitalen Raum signifikant und spürbar stärken“, so Plattner.

BSI als zivile Verteidigung

Die veränderte Qualität der Cyber-Angriffe geht mit einer veränderten Motivation einher. „Wenn Cyber-Kriminelle, Hacktivisten und weitere Akteure sich in den Dienst staatlicher Interessen stellen, haben wir es mit Cyber Conflict zu tun: Cyber-Aggression mit ideologischem, politischem oder militärischem Hintergrund“, so die BSI-Chefin. Deutschland sei mit komplexen hybriden Angriffen konfrontiert, die durch fremde Mächte initiiert, gesteuert und umgesetzt werden. Die Antwort darauf laute Cyber Defense. Die Bundesregierung ist dabei, die staatliche Cyber-Sicherheitsarchitektur Deutschlands zu verbessern. Im Zusammenspiel der Sicherheitsbehörden nehme das BSI die Rolle der zivilen Verteidigung ein, gemeinsam mit militärischen Cyber-Streitkräften, den Strafverfolgungsbehörden und den nachrichtendienstlichen Aufklärungseinheiten. Im Nationalen Cyber-Abwehrzentrums (NCAZ), das am BSI

verankert ist und bereits 15-jähriges Bestehen feiert, kombinieren ausgewiesene Expertinnen und Experten ihre spezifischen Expertisen. Zur Rolle des BSI sagte Plattner: „Wir sind und bleiben dabei die Tekkies im Team."

Optionen schaffen für digitale Souveränität

Souveränität mit Blick auf digitale Technologien habe das Kernanliegen, dass Staaten und Organisationen die endgültige Entscheidungshoheit über ihre Aktivitäten und Prozesse haben oder zurückerlangen. Die BSI-Chefin vertrat die Position, dass digitale Souveränität aus Cyber-Sicherheitsperspektive in erster Linie bedeute, Optionen zu schaffen: Je mehr vertrauenswürdige Produkte verfügbar seien, desto souveräner könne entschieden werden und desto sicherer werde die digitale Zukunft. Es gelte nun, einen strategischen Ansatz zu finden, der klärt, welche digitalen Technologien eingekauft und „out of the box" verwendet werden können und welche digitalen Technologien perspektivisch in Deutschland oder Europa entwickelt werden sollen. Auch mögliche „Kontrollschichten" bei der Nutzung außereuropäischer digitaler Angebote gelte es zu entwickeln, um die Kontrolle über Daten und Steuerung zu behalten.

Die deutsche und die europäische Sicherheit im digitalen Raum hänge auch vom eigenen digitalen Erfolg ab. „Wir müssen parallel zu einem automatisierten Cyber-Schutz die eigene Digitalisierung strategisch voranbringen", betonte Plattner. Sie sprach sich entschieden für eine Stärkung heimischer Digitalunternehmen aus: „Es liegt auf der Hand, dass der europäische Markt und die hiesige Digitalindustrie in wichtigen Technologiefeldern gestärkt werden müssen. Nationale und europäische Anbieter unterstützen wir zum Beispiel dabei, Systeme und Architekturen zu entwickeln, die für Bundes- und Landesbehörden nutzbar gemacht werden können – das betrifft auch und gerade den Umgang mit sensiblen Informationen."

(sib)

• Zur vollständigen Rede der BSI-Präsidentin

Stichwörter: IT-Sicherheit, BSI, Bundesamt für Sicherheit in der Informationstechnik (BSI), Cyber-Abwehr, Cyber-Sicherheit