kaspersky

Acht Impulse zur Cybersicherheitspolitik für eine sichere, resiliente, vertrauenswürdige, transparente digitale Zukunft.

Der Klimawandel, die Corona-Pandemie und zuletzt der russische Angriffskrieg auf die Ukraine haben die Anfälligkeit und Verwundbarkeit von Gesellschaften, Volkswirtschaften, Staaten und deren (kritischen) Infrastrukturen besonders deutlich gemacht. Ob bei Industrieunternehmen, digitalen Plattformen, kritischen Infrastrukturen, öffentlichen Einrichtungen und zivilgesellschaftlichen Organisationen, **der vertrauensvolle und sichere Umgang mit Daten, digitalen Infrastrukturen und Lösungen ist eine der wichtigsten Grundlagen für Freiheit, Frieden, Gesundheit und Wohlstand.** Deshalb gilt es, diese Daten zu schützen und die Steigerung von **Cybersicherheit** und **Resilienz** zu einem politischen Schwerpunkt zu machen.

Vor diesem Hintergrund plädiert Kaspersky für einen Paradigmenwechsel in der Cybersicherheits- und Digitalpolitik. Immer komplexer werdende, zielgerichtete Angriffe mit Schadsoftware, insbesondere **Ransomware- und Supply Chain-Angriffe,** haben in der jüngsten Vergangenheit gezeigt, wie verwundbar Unternehmen, kritische Infrastruktur, Verwaltungen, zivilgesellschaftliche Einrichtungen und Bürger/Verbraucher sind. Allein die volkswirtschaftlichen Schäden von Cyberattacken sind enorm: Die Europäische Kommission hat errechnet[1], dass die finanziellen Schäden von 2015 bis 2020 weltweit von 2,5 Billionen Euro auf 5,5 Billionen Euro gestiegen sind. Für Deutschland werden die entstandenen Schäden auf jährlich mehr als 100 Milliarden Euro taxiert[2].

Kasperskys acht Impulse zur Cybersicherheitspolitik für die kommenden Jahre lauten:

1. Security by Design umsetzen

Eine sichere, resiliente digitale Infrastruktur ist das Rückgrat der Digitalisierung in Deutschland. Das wichtigste Gestaltungsprinzip, um die Resilienz digitaler Infrastrukturen sowie Lösungen sicherzustellen, ist Security by Design. Man kann sich die aktuelle Cybersicherheit, um eine Analogie mit der Pandemie zu ziehen, wie eine Schutzmaske vor dem Gesicht vorstellen. Ein hilfreicher, praktischer Schutz mit einer externen Komponente. Künftige Cybersicherheit sollte jedoch noch weitergehen und idealerweise der Grundidee einer vollständigen Immunisierung folgen. Auch wenn diese Immunisierung eine Infektion nicht 100%ig verhindern kann, schützt sie vor schwerwiegenden und insbesondere tödlichen Verläufen. Übertragen auf die Cybersicherheit heißt das, dass dieser Immunitätsgedanke bereits in der Design- und Konzeptionsphase für digitale Produkte, Lösungen und Services berücksichtigt werden muss. So können nicht nur einzelne Teile der Infrastruktur geschützt werden, sondern Gesamtsysteme resilient gegenüber umfassenden, technisch ausgefeilten und langanhaltenden Cyberattacken gemacht werden. Ein konsequenter Security-by-Design-Ansatz führt dazu, die Angriffsfläche deutlich zu reduzieren und die Kosten für Cyberangriffe wesentlich zu erhöhen. Kaspersky plädiert für einen Paradigmenwechsel von der ergänzend entwickelten Cybersicherheit hin zu einer inhärenten, durch Security by Design erzeugten, Cyberimmunität.

2. Kompetenzen in der Cybersicherheit bündeln und für europäische Lösungen eintreten

Als globales Cybersicherheitsunternehmen beobachtet Kaspersky sich ständig verändernde und immer ausgefeiltere Bedrohungsszenarien sowie eine enorme Zunahme von Cyberangriffen, die die Netzwerk- und Informationssysteme von Betreibern kritischer Infrastrukturen, systemrelevanten Unternehmen und staatlichen Institutionen gefährden. Es ist deswegen notwendig, die Expertise aller Akteure, die sich der Stärkung der Cybersicherheit verschrieben haben, zu bündeln. Der Informationsaustausch und das Teilen von Threat Intelligence zwischen staatlichen und privaten Akteuren müssen intensiviert und qualitativ verbessert werden. Die koordinierte und vertrauensvolle Offenlegung von Schwachstellen muss weiter gefördert werden. Kaspersky hat ethische Prinzipien für die sogenannte Coordinated Vulnerability Disclosure[3] veröffentlicht. Großes Potenzial liegt zudem darin, den europäischen digitalen Binnenmarkt weiter zu harmonisieren und die vorhandene Fragmentierung zu verringern, die sich aus unterschiedlichen Gesetzgebungen und der Auslegung von Richtlinien in den einzelnen EU-Mitgliedsstaaten ergibt. Die NIS2-Richtlinie

[1] Baldini, G., et al. (2020): Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020.

[2] Bitkom (2019): Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr, 06.11.2019, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr

[3] Kaspersky (2020): Ethical principles of vulnerability disclosure, 18.05.2020, abrufbar unter https://www.kaspersky.com/blog/vulnerability-disclosure-ethics/35581/

sollte in den Mitgliedsländern so einheitlich wie möglich umgesetzt werden. Der in Vorbereitung befindliche Cyber Resilience Act muss den bestehenden europäischen Rechtsrahmen zielgerichtet und überschneidungsfrei ergänzen. Die europäischen Zertifizierungsschemata nach dem EU Cybersecurity Act müssen marktorientiert entwickelt werden. Dazu sollte Deutschland verantwortungsbewusste Beiträge leisten.

3. Cybersicherheits-, Wettbewerbs- und Beschaffungspolitik faktenbasiert weiterentwickeln

Deutschland und Europa müssen leistungsfähige Cybersicherheits-Ökosysteme aufbauen, die alle Kompetenzträger einbeziehen, die an der Steigerung der Cybersicherheit werteorientiert mitarbeiten. In der Politikgestaltung empfiehlt Kaspersky einen ausgewogenen Mix, bestehend aus (i) einer faktenbasierten technischen Regulierung der IKT-Lieferkette im Sinne von Supply-Chain-Security, (ii) der Schaffung eines attraktiven Investitionsrahmens und (iii) einer Fokussierung auf Supply-Chain Security sowie Security by Design. Digitale Souveränität bedeutet in diesem Zusammenhang, die Kriterien zu definieren und zu benennen, die Anbieter von Cybersicherheitslösungen zu erfüllen haben. Diese Definition sollte europäisch abgestimmt erfolgen. Kaspersky hat mit seiner globalen Transparenzinitiative[4] ein umfassendes Maßnahmenpaket geschnürt, das beispielgebend für den Beleg der Vertrauenswürdigkeit sein könnte. Hierzu zählen die Möglichkeit für staatliche Stellen und Partner, den Source Code der Software zu prüfen, unabhängige SOC2-, CC- sowie ISO 27001-Zertifizierungen sowie weitere Maßnahmen. Das BSI sollte politisch unabhängig aufgestellt werden und das BSI-Gesetz konkretisiert werden. Beides erscheint dringend erforderlich, um die wertvolle Arbeit des BSI zur Steigerung von Cybersicherheit und Resilienz als technisch-wissenschaftliche Bundesbehörde nicht zu gefährden und eine nachhaltige Basis für eine vertrauensvolle Zusammenarbeit mit Wissenschaft, Wirtschaft und Zivilgesellschaft zu schaffen.

4. Fachkräfte gewinnen und weiterentwickeln

Ein wesentliches Wachstumshemmnis für eine nachhaltige Steigerung der Cyberresilienz in Deutschland (und Europa) ist der Mangel an qualifizierten Fachkräften. Dieser verringert die Fähigkeiten von Unternehmen und öffentlichen Einrichtungen, die eigene IT mit einer am Risiko ausgerichteten, angemessenen Sicherheit zu betreiben, auf Cyberangriffe vorbereitet zu sein und schnell sowie qualitativ hochwertig reagieren zu können. Daten aus Europa[5] und Deutschland[6] zeigen, dass im Jahr 2020 viele IT-Stellen unbesetzt geblieben sind. Vom Fachkräftemangel sind KMUs sowie öffentliche Einrichtungen oftmals besonders betroffen, da diese in der Regel nicht über die finanziellen Mittel verfügen, gefragtes Personal auf dem Markt zu rekrutieren. Zur Umsetzung der cybersicherheitspolitischen Zielsetzungen ist ein effektives Cyber-Capacity-Building in Wirtschaft, Verwaltung, Wissenschaft und Zivilgesellschaft erforderlich. Dem Fachkräftemangel muss dringend mit speziellen Angeboten in der schulischen, universitären sowie beruflichen Aus- und Weiterbildung begegnet werden. So sollte Cybersicherheit zu einem wesentlichen Bestandteil einer digitalen Grundausbildung werden. Bereits in der Grundschule sollten junge Menschen für das Thema Cybersicherheit sensibilisiert werden. Auch die Zahl der Abschlüsse in Studiengängen mit einem Bezug zu Cybersicherheit muss deutlich gesteigert werden. Zudem sollten in allen Studiengängen Seminare und Vorlesungen zur Cybersicherheit zum Pflichtprogramm gehören. Eine weitere wichtige Maßnahme liegt in der gezielten Förderung von Frauen in der IT- und Cybersicherheitswirtschaft[7]. Neben Lesen, Schreiben und Rechnen sollte Programmieren als vierte Schlüsselqualifikation in die Lehrpläne der Grundschulen aufgenommen werden.

5. Die Gesellschaft sensibilisieren und befähigen

Das Digitalbarometer des BSI aus dem Jahr 2020[8] zeigt die Cyberbedrohungslage für die Bevölkerung deutlich auf: Jeder vierte Bürger ist 2020 Opfer einer Cyberattacke geworden. Trotz dieser hohen Zahl zeigen die Werte auch, dass die Bevölkerung nicht ausreichend sensibilisiert ist. So gaben 10% der befragten Personen an, über gar keine Schutzmaßnahmen zu verfügen. Auch nutzen nur 57% der Befragten ein aktuelles Virenschutzprogramm, nur 25% installieren regelmäßig Updates und nur 28% erneuern regelmäßig ihre Passwörter. Gleichzeitig sind IT-Tools mit großer Sicherheitswirkung, wie Passwortmanager und Virenschutz-Software, so einfach und kostengünstig verfügbar

[4] Siehe: https://www.kaspersky.com/transparency-center

[5] ENISA (2020): Cyber Security Skills Development in the EU

[6] Statista (2021): Deutschland fehlen IT-Experten, 13.01.2021, abrufbar unter https://de.statista.com/infografik/16584/zu-besetzende-it-stellen-in-der-deutschen-gesamtwirtschaft/

[7] Siehe hierzu auch die Aktivitäten von Kaspersky: https://wit.kaspersky.com/#

[8] Bundesamt für Sicherheit in der Informationstechnik (2020): Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit – Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.pdf;jsessionid=A6635EFCF86C87043E24A2D8557CF602.internet471?__blob=publicationFile&v=1

wie noch nie. Deshalb glauben wir, dass es dringend ambitioniertere Maßnahmen benötigt, die Bevölkerung für die Gefahren im Cyberraum sowie die richtigen Abwehrmaßnahmen zu sensibilisieren. Hierzu bieten sich interaktive Schulungen an, die dem Gamification-Ansatz folgen und nicht nur Fakten vermitteln, sondern Cybersicherheit mit der in der Praxis wichtigen emotionalen Komponente erlebbar machen.

6. Cyberresilienz im Mittelstand stärken

Nicht nur bei kritischen Infrastrukturen, sondern insbesondere in der industriellen Produktion ist die Steigerung der Cybersicherheit und Resilienz für die weitere Entwicklung des Wirtschaftsstandortes Deutschland von herausragender Bedeutung. Das gilt vor allem für den deutschen Mittelstand. Viele Hidden Champions zählen in ihren jeweiligen Branchen zu den Weltmarktführern und verarbeiten besonders schützenswerte Datensätze. Eine unberechtigte Offenlegung oder ein Verlust solcher Daten kann zu erheblichen juristischen und ökonomischen Schäden sowie Reputationsverlust führen. Vor diesem Hintergrund sollte der Staat KMUs dazu motivieren und Anreize setzen, mehr finanzielle Mittel in die eigene Cybersicherheit zu investieren. Neben Investitionen in Software und der Schaffung von Stellen für Cybersicherheitsfachkräfte, sind Bildungsprogramme zur Cybersicherheit zu fördern. Denn laut dem ENISA Threat Landscape Report 2020[9] setzen knapp 84% aller Cyberattacken teilweise oder ganz auf den Faktor Mensch als Einfallstor für Schadsoftware. Ein besserer Kenntnisstand würde die Cyberresilienz in Deutschland deutlich erhöhen.

7. Die Digitalisierung der öffentlichen Verwaltung sicher und vertrauensvoll gestalten

Eine effiziente und bürgerorientierte öffentliche Verwaltung ist eine wichtige Voraussetzung für die ökonomische, soziale und gesellschaftliche Entwicklung in Deutschland und Europa sowie für das Vertrauen der Bürgerinnen und Bürger sowie Unternehmen in den Staat. Werden öffentliche Einrichtungen und Behörden kompromittiert, sinkt das Vertrauen in öffentliche Online-Services sowie digitale Infrastrukturen. Das BSI hat in seinem Lagebericht 2020[10] aufgezeigt, dass sich die Bedrohungslage für Verwaltungen und öffentliche Einrichtungen in den letzten Jahren in Deutschland analog zum globalen Trend verschärft hat. Budgetrestriktionen und der Fachkräftemangel erschweren es, eine angemessene IT-Sicherheit zu gewährleisten. Die öffentliche Hand muss daher mehr Mittel in den Ausbau der Resilienz stecken. Denkbar hierzu wäre eine verpflichtende Quote für Ausgaben in die Cybersicherheit bei öffentlichen IT-Projekten. Zudem sollten innovative Cybersicherheitstrainings für Beamtinnen und Beamte entwickelt und umgesetzt werden sowie Minimalstandards für das IT-Sicherheitsmanagement basierend auf internationalen Standards, wie zum Beispiel ISO 27001 oder dem BSI Grundschutz, flächendeckend verpflichtend werden.

8. Maßnahmen gegen die Nutzung von Stalkerware ergreifen

Die Aufnahme digitaler Computerprogramme mit dem Zweck des digitalen Ausspähens von Personen als eine Tathandlung nach Absatz 1 Nummer 5 des §238 StGB[11] bei der jüngsten Änderung des Strafgesetzbuches zur besseren Erfassung des Cyber-Stalkings begrüßen wir als Gründungsmitglied der Koalition gegen Stalkerware[12] sehr. Ein weiterer Punkt, den es zu adressieren gilt, ist die „legale" Entwicklung und der Verkauf von Stalkerware. Kein Softwareprogramm sollte eine Überwachung durchführen können ohne die Zustimmung des Benutzers, ohne eine dauerhafte Benachrichtigung des Benutzers und deutlich gekennzeichnete Symbole auf dem Gerät des Benutzers, die sowohl das Vorhandensein der Software als auch ihre Funktionalität hervorheben. Kaspersky fordert daher eine klare Definition von Anforderungen an Überwachungssoftware und ein Verbot, wenn diese Anforderungen nicht erfüllt werden.

Über Kaspersky:

Kaspersky ist ein globales Cybersicherheitsunternehmen mit einer starken Präsenz in Deutschland und Europa. Seit 25 Jahren setzt sich das Unternehmen für Sicherheit und Resilienz im Cyberraum ein. Weltweit vertrauen mehr als 400 Millionen Nutzer und 240.000 Unternehmens- sowie Behördenkunden auf die Produkte, Lösungen und Services von Kaspersky. Europa und Deutschland sind Schlüsselmärkte für das Unternehmen. Dabei geht es nicht nur um die Absicherung von Geräten, Infrastrukturen und Anlagen, sondern um die Entwicklung eines Ökosystems, in dem alles, was durch Technologie verbunden ist, immun gegen Cyberbedrohungen wird. Weil Antworten auf die dringenden Fragen der Cybersicherheit nur gemeinschaftlich von Akteuren aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft erarbeitet und umgesetzt werden können, verfolgt Kaspersky einen dedizierten Multi-Stakeholder-Ansatz und arbeitet vertrauensvoll mit zahlreichen staatlichen Behörden, wissenschaftlichen Einrichtungen, Verbänden und Organisationen der Zivilgesellschaft sowie anderen Akteuren der Cybersicherheits-Industrie zusammen, um den Cyberraum sicherer zu machen.

---

[9] ENISA (2020): From January 2019 to April 2020. Main Incidents in the EU and worldwide. ENISA Threat Landscape, abrufbar unter https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents

[10] Bundesamt für Sicherheit in der Informationstechnik (2020): Die Lage der IT-Sicherheit in Deutschland 2020, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1

[11] Deutscher Bundestag (2021): Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings, abrufbar unter https://dserver.bundestag.de/btd/19/286/1928679.pdf

[12] Coalition Against Stalkerware (2019), Überblick, abrufbar unter https://stopstalkerware.org/de/uber-uns/