EU-Mitgliedstaaten fordern die Einrichtung eines Notfallfonds für Cybersecurity

Die europäischen Regierungen haben eine Erklärung zur Stärkung der Cybersicherheitskapazitäten der EU ausgearbeitet, einschließlich der Einrichtung eines neuen Fonds und der Aufstockung der EU-Mittel zur Unterstützung nationaler Bemühungen. Die jüngsten Cyberangriffe im Kontext des Ukrainekrieges und der damit einhergehende „Cyber-Spillover" auf EU-Staaten zeigen die Notwendigkeit der Unterstützung der Cyber-Resilienz auf, weshalb die EU einen umfassenden Plan für ihre Cybersicherheit vorantreibt. Eine Reihe von Maßnahmen und ein Notfallfonds für Cybersicherheit sollen die EU zukünftig auf groß angelegte Cyberangriffe vorbereiten. Außerdem sollen zusätzliche EU-Mittel die Mitgliedstaaten beim Ausbau ihrer Cybersicherheitskapazitäten unterstützen.

Green IT: Abwärme aus Rechenzentren zum Heizen nutzen

Die Abwärmenutzung von Rechenzentren soll einen Beitrag zur Wärmewende leisten. Bisher wird die wertvolle Wärme zum Großteil in die Umgebungsluft geblasen, jedoch könnte man durch eine bessere Standortplanung künftig viel mehr von der IT profitieren. Die deutsche Bundesregierung hat das Potenzial der Rechnerwärme, auch in Hinblick auf ökologische Nachhaltigkeit und Klimaschutz, erkannt und fordert die Errichtung von neuen Rechenzentren ausschließlich in Gebieten, wo Unternehmen und Wohngebiete die Abwärme nutzen können. Mittels Wasserkühlung würde sich die Abwärme der Server zudem einfacher nutzen lassen, weshalb das deutsche Umweltbundesamt für eine staatliche Förderung von Wasserkühlung plädiert. Welches Potenzial die Nutzung von Rechnerabwärme für das Heizen birgt zeigt vor allem das Beispiel Frankfurt am Main, Deutschlands größter Standort für Rechenzentren. Hier würde die Hitze der Computer ausreichen, um die gesamte Stadt zu beheizen.

Einigung über den Digital Markets Act (DMA)

Das EU-Parlament und der Europäische Rat haben sich am 24.03.2022 vorläufig auf neue EU-Vorschriften zur Begrenzung der Marktmacht großer Online-Plattformen geeinigt. Der Rechtsakt über digitale Märkte (Digital Markets Act, DMA) wird künftig bestimmte Praktiken großer Plattformen, die als „Gatekeeper" agieren, auf eine schwarze Liste setzen und der EU-Kommission ermöglichen, Marktuntersuchungen durchzuführen und nicht konformes Verhalten zu sanktionieren. Der DMA soll kleineren Mitbewerber:innen bessere Überlebenschancen bieten, Nutzer:innen größere Freiheit bei der Wahl von Onlinediensten einräumen und eine Monopolbildung verhindern. Ziel des Rechtsakts ist demnach eine gerechtere und stärker wettbewerbsorientierte Gestaltung des digitalen Sektors. Zum ersten Mal seit 20 Jahren wurden nun klare Regeln für große Online-Plattformen definiert, womit „eine neue Ära der Regulierung im Technologiebereich" eingeleitet werden soll.

UN-Konvention gegen Cyberkriminalität

Im Herbst 2020 hatte die UN-Vollversammlung in der Resolution 74/247 entschieden, Verhandlungen zu einer neuen UN-Konvention gegen Cyberkriminalität aufzunehmen. An der ersten zweiwöchigen Verhandlungsrunde waren über 1000 Delegierte aus 160 Ländern beteiligt. Dazu kamen über 200 nicht-staatliche Organisationen als Beobachter. Konfliktpunkte sind das Verständnis von nationaler staatlicher Souveränität im Cyberspace bei der Verfolgung von Straftaten, die Definition von Straftaten im Cyberspace, die internationale Zusammenarbeit bei der grenzüberschreitenden

Strafverfolgung im digitalen Raum, die technische Hilfe und qualifizierte Ausbildung, um Strafverfolger und ihre Behörden in die Lage zu versetzen, effektiv gegen Cyberkriminelle vorzugehen und die Beteilung von nicht-staatlichen Akteuren bei der Ermittlung von Cyberstraftätern. Die nächste Verhandlungsrunde ist für Ende Mai/Anfang Juni 2022 in Wien geplant.

Privacy Shield 2.0: Europäische Kommission und Vereinigte Staaten gaben grundsätzliche Einigung zum Transatlantischen Datenschutzrahmen bekannt

Die EU-Kommission und die USA haben sich grundsätzlich auf einen neuen Transatlantischen Datenschutzrahmen geeinigt. Der neue Datenschutzrahmen soll den vom EuGH in der Schrems-II-Entscheidung vom Juli 2020 geäußerten Bedenken Rechnung tragen. Im Rahmen des Transatlantischen Datenschutzrahmens werden die Vereinigten Staaten neue Schutzmaßnahmen einführen, um sicherzustellen, dass die signalerfassende Aufklärung zur Verfolgung der festgelegten Ziele der nationalen Sicherheit erforderlich und angemessen ist. Zudem werden sie einen zweistufigen unabhängigen Rechtsbehelfsmechanismus einrichten, durch den Abhilfemaßnahmen verbindlich angeordnet werden können, und die signalerfassende Aufklärung einer strengen, mehrstufigen Aufsicht unterstellen, um die Einhaltung der Beschränkungen für Überwachungsmaßnahmen zu gewährleisten. Die Ankündigung wurde nicht mit einem Text unterlegt und es wird noch einige Monate dauern, bis die Vereinbarung auf technischer Ebene abgeschlossen ist.

Gaia-X Hub Austria offiziell bestätigt

Auf Initiative des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW) und des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) wurde der Gaia-X Hub Austria gegründet. Der Hub ist die nationale Vertretung der Europäischen Leitinitiative Gaia-X. Ziel des Hubs ist es, österreichischen Organisationen den Einstieg in Datenräume zu ermöglichen. In der europäischen Initiative Gaia-X werden die Rahmenbedingungen für die Entwicklung von Datenräumen gestaltet. Entstehen soll ein Ökosystem zur Kooperation, zum Datenaustausch und zur Erstellung von neuen Daten-Diensten und Geschäftsmodellen für unterschiedlichste Märkte. Beispiele dafür sind die deutsch-österreichischen Leuchtturmprojekte EuProGigant und ChampI4.Ons im Bereich der digitalen und nachhaltigen Produktion.

Windkraftanlagenhersteller Nordex nach Cyberangriff weiterhin beeinträchtigt

Nach einem Cyberangriff auf die interne IT-Infrastruktur am 31. März ist der Hersteller von Winkraftanlagen Nordex weiter beeinträchtigt. Das Unternehmen hat, um die Anlagen zu schützen, den Fernüberwachungszugriff aus der IT-Struktur auf die unter Vertrag stehenden Turbinen vorsorglich deaktiviert. Die Turbinen laufen nach Angaben von Nordex uneingeschränkt weiter, alternative Überwachungsdienste wurden aufgesetzt. Systeme Dritter wurden im Rahmen des Cyberangriffs nicht beeinträchtigt.

Sichere Digitalisierung für den öffentlichen Sektor: Präventivmaßnahmen zur Cybersicherheit

Behörden und Verwaltungen arbeiten mit einer enormen Menge an personenbezogenen Daten: Sie sammeln und verarbeiten sowohl Kontaktdaten als auch sensible Informationen, die u.a. Aufschluss über Wohnort, Beruf, Einkommen und Familienstand von Personen geben. Der komplette Ausfall einer Behörde ist nicht nur für Mitarbeiter:innen und die betroffenen Personen schädlich, die Qualität und Schnelligkeit der Arbeitsabläufe in Behörden haben hohen Einfluss auf die Zufriedenheit

der Bürger:innen mit dem Staat. Das alles sind Gründe, warum der öffentliche Sektor ein beliebtes Ziel von Cyberkriminellen ist. In so einer Situation sind die richtigen Präventivmaßnahmen gefragt – allen voran Geräte- und Applikationskontrolle. Des Weiteren bieten sich folgende Maßnahmen speziell für den öffentlichen Sektor an:

- Die Verschlüsselung von sensiblen Daten am Speicherort und auf Wechselmedien.
- Überwachung und Protokollierung jeglicher Zugriffe/Änderungen im System.
- Mitarbeitersensibilisierung zur Vermeidung menschlichen Fehlverhaltens.

Der zuverlässige Schutz von Daten, Geräten und Systemen ist für den öffentlichen Sektor unabdingbar. Um die dafür notwendigen Maßnahmen mit eigenem Personal stemmen zu können, benötigt es Investitionen in Fachkräfte, Ausbildung und Systeme. Eine hohe Cybersicherheit spielt nicht zuletzt die Schlüsselrolle für eine gelungene Digitalisierung.