EU-Cyber-Sicherheitspaket: Ziel ist es, die Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen zu erhöhen.

Widerstandsfähigkeit erhöhen

Die Europäische Kommission stellt sich den Herausforderungen, Bedrohungen und Risiken der Entwicklung der Informationstechnologie mit einem neuen Cyber-Sicherheitspaket.

Die Digitalisierung unseres Alltags und der kritischen Dienste schreitet in einem enormen Tempo voran, damit verbunden ist eine höhere Verwundbarkeit. Die Covid-19-Pandemie beschleunigte die Abhängigkeit von Informationstechnologie und vergrößerte die Angriffsfläche für Cyber-Kriminelle.

Eine Studie des Digitalverbandes Bitkom aus den Jahren 2020 und 2021 in Deutschland ergab, dass jedes neunte Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen ist. Die Schadenssumme betrug 220 Milliarden Euro pro Jahr, sie ist doppelt so hoch wie in den Jahren 2018 und 2019. Experten gehen davon aus, dass Cyber-Angriffe im laufenden Jahr weltweit Kosten in der Höhe von sechs Billionen Euro verursachen werden.

Besonders risikoreich sind Angriffe auf kritische Einrichtungen wie beispielsweise Krankenhäuser. Solche Angriffe häuften sich in den letzten beiden Jahren. Hinzu kommen geopolitische Aspekte, insbesondere, dass autoritäre Regime immer stärker versuchen, ihre Interessen (wirtschaftlicher und politischer Art) im Cyber-Raum geltend zu machen. Abgesehen von den Risiken wirtschaftlicher Natur hat die Bevölkerung ein hohes Interesse an einem reibungslosen Funktionieren kritischer Einrichtungen.

Abwehrfähigkeit stärken. Im Lichte dieser Entwicklungen stellte die Europäische Kommission am 16. Dezember 2020 ein Cyber-Sicherheitspaket vor, das die Abwehrfähigkeit der EU gegen Cyber-Bedrohungen stärken soll. Es soll dazu beitragen, dass man die Vorzüge vertrauenswürdiger und zuverlässiger digitaler Dienste uneingeschränkt nutzen kann. Die Cyber-Sicherheitsstrategie setzt vor allem auf Normsetzung auf europäischer Ebene und eine Stärkung der Kooperation bei der Cyber-Sicherheit.

Im Bereich Normsetzung wurden zwei Vorschläge präsentiert: eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cyber-Sicherheit in der gesamten Union (überarbeitete NIS-Richtlinie, kurz „NIS 2“) und eine neue Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (kurz „RKE“). Das Ziel dieser beiden Richtlinien ist ein koordiniertes und komplementäres Vorgehen bei künftigen Online- und Offline-Risiken. Im Bereich Kooperation setzt die Europäische Kommission auf den Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion („Joint Cyber-Unit“). Sie will die Zusammenarbeit der verschiedenen „Cyber-Communitys“ (unter anderem Strafverfolgung, Diplomatie, Privatwirtschaft) stärken.

NIS-2-Richtlinie. Erstens stellte die Europäische Kommission einen Vorschlag für eine NIS-2-Richtlinie vor. Dieser Vorschlag baut auf der Richtli-

Foto: Sy_Sarayut/Stock.Adobe.com

nie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) auf, die der erste EU-Rechtsakt über Cyber-Sicherheit war. Die NIS-Richtlinie hatte wesentlich zur Verbesserung der Cyber-Sicherheitskapazitäten auf nationaler/europäischer Ebene beigetragen und verbesserte die Cyber-Resilienz öffentlicher und privater Einrichtungen.

Eine „Joint Cyber-Unit" – eine virtuelle und physische Plattform – soll die Zusammenarbeit der verschiedenen Cyber-Sicherheitsgemeinschaften in der Europäische Union stärken.

Die Cyber-Sicherheitsanforderungen werden mit NIS 2 ausgebaut. Der Anwendungsbereich wurde in dem Vorschlag angepasst. Die Begriffe wesentliche Dienste und Anbieter digitaler Dienste werden ersetzt durch die Begriffe *wesentliche* (besonders kritische) und *wichtige* Einrichtungen. Kleinst- und Kleineinrichtungen sollen, mit Ausnahmen, aus dem NIS-Anwendungsbereich ausgeschlossen sein. Wichtige Einrichtungen sollen einer weniger strengen Ex-post-Kontrolle bei Beibehaltung hoher Verpflichtungen zu Sicherheitsvorkehrungen unterzogen werden. Wesentliche Einrichtungen werden einer Ex-ante Kontrolle unterzogen. Die bisherigen Ermittlungen Betreiber wesentlicher Dienste entfallen. Durch diese Maßnahme soll der Aufwand für Behörden minimiert werden. Der Aufwand der Unternehmen für die Umsetzung von Sicherheitsmaßnahmen sollte gleichbleibend sein.

Der Vorschlag der Europäischen Kommission hat vor allem das Ziel, dass es ein hohes Ambitionsniveau im Bereich Cyber-Sicherheit gibt und die Maßnahmen in die Breite gehen. Die Kooperation und der Informationsaustausch zwischen den Mitgliedsstaaten soll erweitert werden. Die Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit wird ausgebaut, insbesondere durch die Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen.

Richtlinie über die Widerstandsfähigkeit. Zweitens hat die Europäische Kommission eine Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen vorgelegt. Diese muss als Gesamtpaket zusammen mit der NIS-2-Richtlinie gesehen werden. Das Ziel beider Richtlinien ist eine Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen zu erreichen. Die Ausrichtung soll weggehen von einer isolierten Betrachtung physischer und digitaler Risiken hin zu einer engen Abstimmung der Maßnahmen und der rechtlichen Grundlagen.

Konkret vorgeschlagene Maßnahmen in diesem Zusammenhang sind die Erweiterung der durch die Richtlinie erfassten Sektoren auf insgesamt zehn Sektoren. Die Mitgliedsstaaten müssen in Zukunft verpflichtend nationale Strategien für die Widerstandsfähigkeit kritischer Einrichtungen verfassen. Die Mitgliedsstaaten haben nunmehr die Pflicht, regelmäßige Risikobewertungen und die Identifikation von kritischen Einrichtungen in den Sektoren durchzuführen. Des Weiteren werden Verpflichtungen für kritische Einrichtungen in den Bereichen Risikoanalysen und Sicherheitsvorkehrungen sowie hinsichtlich Meldeverpflichtungen vorgesehen. Die autorisierte nationale Behörde kann die Einhaltung der Verpflichtungen überprüfen und bei Bedarf Sanktionen vorsehen.

Joint Cyber-Unit. Drittens wurden im Juni 2021 Details zu einer „Joint Cyber-Unit" bekannt. Sie soll eine virtuelle und physische Plattform zur Stärkung der Zusammenarbeit der verschiedenen Cyber-Sicherheitsgemeinschaften (wie Strafverfolgung, Diplomatie, Privatwirtschaft) führen. Die operative und technische Koordinierung soll verbessert werden. Insbesondere soll es die EU bestmöglich auf den Umgang und das Management von groß angelegten Cyber-Vorfällen und -krisen vorbereiten und auf diese reagieren. Die „Joint Cyber-Unit" soll die Mitgliedsstaaten und EU-Einrichtungen in die Lage versetzen, Strukturen, Ressourcen und Fähigkeiten in vollem Umfang zu nutzen und eine „Need-to-Share"-Mentalität fördern. Bis dato konnten die relevanten Akteure nicht das volle Potenzial der Zusammenarbeit ausschöpfen. Dies soll durch die „Joint Cyber-Unit" verbessert werden.

Die Umsetzung der beiden Richtlinien und Teilnahme an der „Joint Cyber-Unit" wird vom Bundesministerium für Inneres (BMI) als eine Chance gesehen, um die Resilienz in Österreich und der EU zu erhöhen. Das Cyber-Sicherheitspaket wird neue Aufgaben und Ressourcenbedarf für das BMI bedeuten, aber in Summe einen Mehrwert für die Sicherheit Österreichs haben.

Zur Begleitung der Verhandlungen der beiden Richtlinien sowie zu deren Umsetzung in österreichisches Recht in organisatorischer, personeller, rechtlicher und technischer Sicht wurde am 27. Mai 2021 ein Programm im BMI eingerichtet. Das Programm hat zum Inhalt, die Verhandlungen auf europäischer Ebene und die vollständige und ressourcenschonende innerstaatliche Umsetzung der beiden Richtlinien, als Grundlage für einen wirksamen und effizienten Aufgabenvollzug, zu steuern.

Wer Digitalisierung sagt, muss auch Cyber-Sicherheit sagen. Dieses Motto scheint die Europäische Kommission mit ihrem Cyber-Sicherheitspaket zu verfolgen. Wenn man an den plötzlichen Stillstand kritischer Einrichtungen wegen eines physischen oder digitalen Angriffs denkt, dann ist dies ein düsteres Bild. Es ist wichtig, bereits heute Vorkehrungen zum Schutz wesentlicher und wichtiger Dienste zu treffen und die Kooperation in der EU zu verstärken, um im Fall des Falles gut vorbereitet zu sein. Die Unterstützung und rasche nationale Umsetzung des Cyber-Sicherheitspakets ist daher wichtig.

Caroline Schmidt

FOTO: GORODENKOFF PRODUCTIONS OU/STOCK.ADOBE.COM