CYBERRESILIENZ IN DER ÖFFENTLICHEN VERWALTUNG

Autor: Benjamin Isak ***Redaktion: Diana Künstler***

➤ Nicht nur der massiv beschleunigte Übergang zum Homeoffice in den Jahren 2020 und 2021 stellte Kommunen und generell die öffentliche Verwaltung auf Bundes- und Landesebene vor enorme Herausforderungen. Auch die exorbitante Steigerung von Cyberangriffen sowie die verschärfte Bedrohungslage im Umfeld von Behörden und Ministerien trägt entscheidend dazu bei. Im Oktober des letzten Jahres, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2021“ über die aktuellen Bedrohungen im Cyberraum informiert und die Situation in Deutschland mit „angespannt bis kritisch“ eingeschätzt. Dabei spielen die Folgen für die veränderten Arbeitssituationen – wie mobiles Arbeiten, Homeoffice oder allgemein „work from anywhere“ – eine wichtige Rolle und es ergeben sich gänzlich neue Herausforderungen.

Bild: NCP Engineering

BENJAMIN ISAK,
Director Sales Public & Defence bei NCP Engineering

Kontinuierliche Bereitstellung von Bürgerservices

Die öffentliche Verwaltung besitzt naturgemäß eine essenzielle Verantwortung und muss zu jeder Zeit die bedeutenden Services für Land und Bevölkerung unterbrechungsfrei gewährleisten. Dabei steigt auch der Druck auf IT- und IT-Security-Teams, die für die Sicherstellung der Geschäftskontinuität federführend sind. Auch die pandemiebedingt beschleunigte Digitalisierung vergrößert naturgemäß die Angriffsfläche für Cyberangriffe. Diese können für kommunale Verwaltungen weitreichende Konsequenzen nach sich ziehen, etwa wenn Bürgerservices tagelang oder sogar über größere Zeiträume hinweg ausfallen. Die Auswirkungen sind dann bei Dienstleistungen wie der Beantragung einer Geburtsurkunde, dem Kauf einer Immobilie oder der Anmeldung eines Kraftfahrzeugs deutlich spürbar. Eine innovative und cybersicherheitsbewusste Verwaltung ist sich dieser Verantwortung und der Risiken bewusst.

Die vielzitierte Cyberresilienz spielt hier die Hauptrolle als Kernaspekt einer stark vernetzten IT-Infrastruktur. Sie bezeichnet die Widerstandsfähigkeit gegenüber negativen Einflüssen. In Bezug auf die IT-Sicherheit bezeichnet Cyberresilienz die Fähigkeit einer Organisation, sich gegen Angriffe auf ihre Informations- und Kommunikationstechnik zu wappnen. Im Fokus stehen hierbei die eigenen Systeme, aber auch Unternehmens- sowie Kundendaten. Der Grad der Widerstandsfähigkeit ermisst sich in der Gewährleistung von Vertraulichkeit, Integrität sowie der Verfügbarkeit von Daten und hoheitlichen Diensten, welche entsprechend bedeutsam sind.

Erfolgreiche Cyberangriffe können, neben den oben erwähnten Konsequenzen für die eigenen Prozesse und die Bevölkerung, auch erhebliche Auswirkungen auf Dienstleister, Kunden und Partner haben. Diese können nicht nur hohe Kosten nach sich ziehen, sondern auch den Ruf, das Image und den künftigen Geschäftserfolg massiv beschädigen.

Wie die Cyberresilienz erhöhen?

Um nicht Opfer eines Cyberangriffs zu werden, müssen sich die verantwortlichen Teams und Entscheider – stets unter Einbeziehung und Sensibilisierung der eigenen Mitarbeiter – optimal rüsten. Nur so kann rasch und flexibel auf sich verändernde gesellschaftliche oder arbeitstechnische Situationen reagiert werden. Ziel ist es dabei stets, den Geschäftsbetrieb robust, performant und vor allem sicher aufrechtzuerhalten. Was kann man also tun, um widerstandsfähig zu sein? Skalierbarkeit und Anpassungsfähigkeit gehen hier im besten Falle Hand in Hand und schaffen eine nahtlose, beständige und unterbrechungsfreie Geschäftskontinuität.

Leider sieht man sich fast immer einer Übermacht auf Seiten der Angreifer ausgesetzt. Demgegenüber steht die Verwaltung in der Rolle der Verteidigung, die in der Regel nicht genug Manpower und so gut wie nie genug Zeit hat.

Leider sieht man sich fast immer einer Übermacht auf Seiten der Angreifer ausgesetzt. Denn im Zweifel besitzen diese eine State-of-the-Art-Infrastruktur, halten alle Tools in ihrem „Werkzeugkasten“ parat und verfügen über beliebig viel Zeit sowie schier endlosen Nachschub an Angriffsobjekten. Demgegenüber steht die Verwaltung in der Rolle der Verteidigung, die in der Regel nicht genug Manpower und so gut wie nie genug Zeit hat (Privatunternehmen sind davon übrigens gleichermaßen betroffen). Da dies die Realität eins zu eins abbildet, muss man sich rüsten und im besten Falle mit einer anpassungsfähigen, flexiblen und harmonisierenden zentralen Lösung dagegenhalten. Dies gelingt einerseits durch spezialisierte Verteidigungsmechanismen, andererseits durch generische Maßnahmen, wie zum Beispiel einer starken Verschlüsselung und Authentifizierung. Und last but not least ist vor allem eine technisch automatisierte Compliance der entscheidende Schlüsselfaktor, weil immerhin 95 Prozent aller Cyberangriffe auf menschliche Fehler zurückzuführen sind.