Lösungen

Cybersicherheit stärken

[13.09.2024] Die NIS2-Richtlinie bietet die Chance, die IT-Sicherheit auf ein deutlich höheres Level zu heben, ist aber auch mit Herausforderungen verbunden. Kommunen benötigen zudem Lösungen, die speziellen IT-Sicherheitsanforderungen genügen.

Wir haben zwei Ransomware-Angriffe pro Monat in den Kommunen. Das ist besorgniserregend. So beschreibt Daniel Meltzian, Referatsleiter für Grundsatz, Cyber- und Informationssicherheit im BMI, die aktuelle Sicherheitslage. Laut dem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) gab es im Jahr 2023 mehr als 250.000 neue Schadprogramm-Varianten. Jeden Tag werden laut BSI rund 70 Sicherheitslücken in Softwareprodukten entdeckt. Diese Zahlen verdeutlichen: In Zeiten zunehmender digitaler Vernetzung und wachsender Bedrohungen entstehen enorme Herausforderungen für den Schutz sensibler Daten, auch – oder vielleicht sogar ganz besonders – für Kommunen in Deutschland. Trotz alarmierender Zahlen ist der Public Sector in Deutschland beim Thema IT-Sicherheit noch immer schlecht aufgestellt. Der Föderalismus sorgt dafür, dass alle Bundesländer verschiedene IT-Security-Vorschriften festlegen können. Eine Cyberzusammenarbeit über die Bundesländer hinweg fehlt hingegen komplett. **KI unterstützt Cyberkriminelle** Laut dem Lagebericht zur IT-Sicherheit des BSI liegt eine Ursache für die vermehrten Angriffe darin, dass die Cyberkriminellen immer professioneller agieren. Analog zur Realwirtschaft setzen auch die Angreifer zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg, heißt es in dem Bericht. Die fortschreitende Spezialisierung von Cyberangriffen führt also dazu, dass die Hacker ihre Ransomware gezielter einsetzen können. Dies geschieht beispielsweise durch Identitätsdiebstahl in Form von Phishing-Mails oder das Offenlegen von Schwachstellen innerhalb staatlicher Einrichtungen. Nicht zu vernachlässigen ist die zunehmende Unterstützung, von der die Angreifer profitieren: Die Rede ist hier von KI. Diese sorgt auch bei Cyberangriffen für Risiken, die auf der Hand liegen. Tools wie ChatGPT sind für jeden Nutzer einfach zu bedienen, auch für Kriminelle. Die Phishing-Mails werden dadurch immer ausgefeilter und glaubwürdiger. Darüber hinaus ermöglichen manipulierte Stimmen, Bilder und Videos eine verzerrte Faktenlage und erleichtern Desinformationskampagnen, die auch vor hochrangigen Politikern nicht Halt machen. **Neue An- und Herausforderungen** All diese Arten von Cyberkriminalität haben neben den finanziellen Schäden auch zur Folge, dass Unternehmen, Behörden und Kommunen zeitweise nicht mehr arbeiten können. Um derartige Szenarien künftig zu verhindern oder wenigstens abzuschwächen, hat die Europäische Union die NIS2-Richtlinie ins Leben gerufen. Diese soll grundsätzlich ein höheres Maß an Cybersicherheit gewährleisten und die Mindestanforderungen sicherstellen. Die Umsetzung dauert schon seit einigen Monaten an und bringt neue Herausforderungen und Anforderungen für den Public Sector mit sich. Viele Kommunen und Behörden, die bisher nicht als Betreiber Kritischer Infrastrukturen (KRITIS) galten, fallen nun unter die NIS2-Richtlinie. Zudem gibt es eine neue Meldepflicht für Sicherheitsvorfälle; und die Durchführung regelmäßiger Risikoanalysen soll verpflichtend werden. Dies hat zur Folge, dass vorhandene Prozesse und Technologien überdacht und gegebenenfalls aktualisiert werden müssen. Hinzu kommt ein Anstieg des personellen und finanziellen Aufwands: Die IT-Sicherheit muss fortlaufend überwacht, neue Sicherheitsmaßnahmen implementiert sowie Mitarbeitende geschult werden. Bei Nicht-Umsetzung drohen den Einrichtungen empfindliche Strafen. **Wenig Anbieter für speziellen IT-Schutz** Auf den ersten Blick wirkt die NIS2-Richtlinie für den Public Sector wie ein steiniger Weg. Die Umsetzung wird, wie beschrieben, einige Herausforderungen mit sich bringen. Doch noch viel

wichtiger ist, dass NIS2 eine riesige Chance bietet, die IT-Sicherheit in Europa auf ein deutlich höheres Level zu heben. Aufgrund der aktuellen Bedrohungslage ist dies überaus sinnvoll. Viele Verwaltungen arbeiten tagtäglich mit sensiblen Bürgerinformationen, die vom BSI mit dem Geheimhaltungsgrad VS-NfD (Verschlusssachen – Nur für den Dienstgebrauch) klassifiziert werden und damit einen speziellen IT-Security-Schutz beziehungsweise vom BSI-zugelassene Lösungen benötigen. Derartige IT-Lösungen werden nur von wenigen Anbietern zur Verfügung gestellt. Einer davon ist NCP aus Nürnberg.
Budgetschonende Lösung NCP hat speziell für sicheren Remote Access im Public-Sector die VS-GovNet-Lösungen entwickelt, die vom BSI für die Datenübertragung nach VS-NfD zugelassen sind. Die VPN-Security-Produkte von NCP sind zu 100 Prozent softwarebasiert, wodurch sie sowohl mit bestehender Hardware als auch mit aktuellen Cloud-Konzepten wie Zero Trust oder SASE kompatibel sind. Dadurch wird zudem sichergestellt, dass die Produkte sowohl im Rechenzentrum als auch vor Ort (On-Premises) betrieben werden können. Außerdem sind die VPN-Lösungen durch ihre Mandantenfähigkeit für Managed Security Service Provider wie Landesrechenzentren geeignet. Im Sinne der Nachhaltigkeit werden hierdurch Neuinvestitionen vermieden, da die NCP-Lösungen für Standard-Windows-Arbeitsplätze installiert und dadurch die ohnehin schon ausgereizten Kommunalbudgets geschont werden können.

()

https://www.ncp-e.com/de

Stichwörter: IT-Sicherheit, NCP, NIS2