IT-Sicherheit

Sicher arbeiten im Homeoffice

[29.08.2023] Cyber-Angriffe auf Behörden in Deutschland sind ein wachsendes Problem und erfordern ein Umdenken bei der IT-Sicherheit. Die Wahl einer geeigneten, BSI-zertifizierten Sicherheitslösung ist entscheidend, um die Verwaltung wirksam vor den Angriffen zu schützen.

Mittlerweile vergeht kaum eine Woche, in der man nicht von einem neuen Cyber-Angriff auf Behörden, städtische Verwaltungen oder Bürgerservices hört. Allein in Hessen gab es seit dem Jahr 2022 insgesamt 28 Cyber-Attacken auf Kommunen, wie das hessische Innenministerium zum jüngsten Cybersicherheitsgipfel in Wiesbaden mitteilte. Die Bedrohungslage ist durch die Konflikte und Krisen in den vergangenen Jahren so drastisch geworden, dass auch der Bund Alarm schlägt. „Ich finde es bedrohlich, dass die Kommunen besonders oft von Ransomware-Ausfällen betroffen sind“, äußerte sich zuletzt Gerhard Schabhüser, Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Eines ist angesichts der aktuellen Sicherheitslage klar: Lang anhaltende und hoch frequentierte Cyber-Angriffe erfordern bei der IT-Sicherheit im kommunalen Bereich ein Umdenken. Gleichzeitig müssen neue Anforderungen auch mit modernen Arbeitsweisen wie Homeoffice vereinbar sein. Doch wie sieht eine zukunftssichere Lösung für die neuen Cyber-Gefahren aus? Und mit welchen relevanten Sicherheitsstufen und Richtlinien müssen sie in Deutschland kompatibel sein?**Klassifizierungen für Behörden** Die meisten Behörden und auch Unternehmen stufen die Sensibilität ihrer zu verarbeitenden Daten völlig unterschiedlich ein. Eine derartige Klassifizierung von Daten hat direkte Auswirkungen auf die jeweils erforderliche Geheimhaltungsstufe. Folgende vier Geheimhaltungsgrade kommen häufig zum Einsatz: Öffentlich: Dabei handelt es sich um Informationen, die prinzipiell für jedermann zugänglich sein können. Ihre Veröffentlichung stellt kein Risiko dar, sondern ist in den meisten Fällen sogar ausdrücklich erwünscht. Intern: Diese Daten sind innerhalb der Behörde in der Regel frei verfügbar, sollen aber nicht nach außen dringen. Beispiele für interne Daten sind Handbücher für Mitarbeiter oder die innerbehördliche Kommunikation. Vertraulich: Diese Informationen gelten bereits als wesentlich sensibler und dürfen auch innerhalb der Behörde nur mit einer begrenzten Anzahl von Personen geteilt werden, die sie zur Erfüllung ihrer Aufgaben benötigen. Dazu zählen zum Beispiel Bürgerdaten, Personalinformationen und andere Arten von Geheimnissen. Streng vertraulich: Diese Daten haben höchste Wichtigkeit und benötigen maximalen Schutz. Der Zugang zu solchen Informationen ist deshalb stark eingeschränkt und muss protokolliert werden. Beispiele für diese Art von Informationen sind hochsensible personenbezogene Daten, kritische Geschäftsdaten oder vertrauliche Regierungsinformationen. Erst die Einstufung von Daten ermöglicht es Behörden, angemessene Sicherheitsmaßnahmen zu ergreifen. Diese stellen dann sicher, dass sensible Informationen nur diejenigen Personen einsehen können, die dazu berechtigt sind und diese Informationen zur Erfüllung ihrer Aufgaben auch benötigen. **Offizielle Geheimhaltungsgrade in Deutschland** In Deutschland enthält das Sicherheitsüberprüfungsgesetz (SÜG) in Paragraf 4 „Allgemeine Grundsätze zum Schutz von Verschlusssachen“, die für den Bund und seine nachgeordneten Behörden gelten. Sie geben in Absatz 2 wiederum vier Geheimhaltungsgrade vor. Diese lauten in aufsteigender Reihenfolge: VS-Nur für den Dienstgebrauch (VS-NfD), wenn die Kenntnisnahme durch Unbefugte den Interessen der Bundesrepublik Deutschland oder eines ihrer Länder Nachteile bereiten kann. VS-Vertraulich, wenn die Kenntnisnahme durch Unbefugte für die Interessen des Bundes oder seiner Länder schädlich sein kann. Geheim, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden

zufügen kann. Streng geheim, wenn ihre Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann. VS-NfD ist dabei der Geheimhaltungsgrad, der auf kommunaler Ebene am häufigsten zum Tragen kommt. Hier arbeiten Mitarbeiter in der öffentlichen Verwaltung mit vertraulichen Bürgerinformationen, die zu jedem Zeitpunkt sicher übertragen werden müssen. Das gilt nicht nur in der Behörde, sondern auch dann, wenn der entsprechende Sachbearbeiter aus dem Homeoffice heraus tätig ist. **Neue VS-NfD-Bestimmungen für Remote Work** Gerade das Thema Remote Work ist längst kein Grenzfall mehr. Auch in Behörden ist flexibles Arbeiten mittlerweile an der Tagesordnung. Die nötige Sicherheit darf darunter jedoch keinesfalls leiden. Wie wichtig entsprechende Schutzmechanismen sind, zeigen auch die jüngsten Beschlüsse des Bundes. Im Zuge der letzten Cyber-Angriffe auf kommunale Verwaltungen informiert das Bundesverwaltungsamt seit März alle Behörden, die mit dem Schengener Informationssystem (SIS) arbeiten, über erweiterte VS-NfD-Richtlinien. So sind betroffene Behörden künftig verpflichtet, für Remote-Work-Tätigkeiten im Umgang mit VS-NfD die entsprechenden technischen Anforderungen umzusetzen und eine BSI-zugelassene Lösung einzusetzen. Für viele Landratsämter und andere Behörden, die mit diesem System zur Personen- und Sachfahndung im Schengenraum arbeiten, beginnt damit eine Umstellung ihrer Remote-Work- und IT-Prozesse an die neuen Anforderungen. **Technische Anforderungen für VS-NfD** Um VS-NfD-konformes Arbeiten sicherzustellen, muss die IT-Infrastruktur der jeweiligen Behörden und Verwaltungen bestimmte technische Vorgaben erfüllen. Dafür gibt es seitens des Bundesministeriums für Wirtschaft und Energie (BMWi) genaue Bestimmungen und Anforderungen, die in einem Merkblatt festgehalten sind. In Kapitel II wird beispielsweise erläutert, welche Maßnahmen zum Schutz der Vertraulichkeit von elektronisch gespeicherten Verschlusssachen getroffen werden müssen: PCs mit E-Mail- und Internet-Anschluss müssen nicht nur mit aktuellen Betriebssystem- und Antiviren-Software-Versionen ausgestattet sein, sondern zusätzlich von einer Firewall und einem zugelassenen Application Gateway geschützt werden. Dabei muss mit verbindlichen Anwenderregelungen sichergestellt sein, dass nur entsprechend geschulte Mitarbeiter auf Verschlusssachen zugreifen dürfen. Die Übertragung von VS-NfD muss zudem verschlüsselt erfolgen (etwa über einen sicheren VPN-Tunnel), wobei für die Verschlüsselung nur vom BSI zugelassene Produkte eingesetzt werden dürfen. Behörden und Verwaltungen sind also dazu verpflichtet, ihre komplette IT-Infrastruktur und Datenkommunikation nach den Empfehlungen des BSI lückenlos mit entsprechend zertifizierten Lösungen abzusichern. **Die richtige Lösung finden** Was sich nach einem aufwendigen Unterfangen anhört, lässt sich mit etwas Planung jedoch geordnet umsetzen. Wichtig dabei ist vor allem die Wahl der richtigen IT-Security-Lösung, die alle Anforderungen des Gesetzgebers erfüllt und gleichzeitig einfach zu bedienen und zu managen ist. Hierbei ist die BSI-Zulassung nach VS-NfD für alle eingesetzten Komponenten zwingend notwendig. Außerdem sollten Application Gateway, Management Software und Endgeräte-Client möglichst von einem Hersteller stammen, um reibungslose Prozesse zu garantieren. Des Weiteren sollten Made-in-Germany-Produkte bevorzugt werden, um Backdoors zu vermeiden und die digitale Souveränität sicherzustellen. Zudem empfiehlt es sich, bei Software-Produkten auf hohe Kompatibilität achten, um vorhandene Hardware weiterverwenden zu können. Ferner sollten zentrale Management-Komponenten zum Einsatz kommen, über die Administratoren Updates und Firewall-Richtlinien ausspielen sowie Benutzer, Lizenzen und Zertifikate prüfen können. Schließlich bedarf es Endpoint Policy Checks, die Endgeräte auf Sicherheitslücken prüfen und gegebenenfalls vom Zugriff ausschließen. Deckt eine Lösung all diese Punkte ab, sind umsetzende Behörden bestens für die neuen VS-NfD-Anforderungen gerüstet und schützen ihre kommunale Verwaltung auch in Zukunft effektiv vor Cyber-Angriffen. Einen Anhaltspunkt für die Auswahl liefert die „Liste der zugelassenen IT-Sicherheitsprodukte und -systeme“ des BSI.

()

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

Stichwörter: IT-Sicherheit, NCP,