IT-Security

Sicher arbeiten im Homeoffice

[28.03.2022] Beim mobilen Arbeiten in der öffentlichen Verwaltung muss auch die IT-Sicherheit gewährleistet sein. Wie können Kommunen ihr Netzwerk, ihre Daten und Geräte so absichern, dass Cyber-Angriffe erschwert werden?

Die öffentliche Verwaltung besitzt eine essenzielle Verantwortung und muss zu jeder Zeit die bedeutenden Services für Land und Bevölkerung aufrechterhalten und unterbrechungsfrei sicherstellen. Dabei steigt der Druck auf IT-(Security)-Teams, die für die Gewährleistung der Geschäftskontinuität bei gleichzeitiger Sicherheit zuständig sind. Cyber-Attacken auf kommunale Verwaltungen können weitreichende Konsequenzen haben. Um gar nicht erst Opfer eines Angriffs zu werden, müssen sich die verantwortlichen Teams und Entscheider Gedanken darüber machen, was präventiv getan werden kann. Als größtes bekanntes Risiko stehen vor allem die eigenen Mitarbeiter und deren Information und Sensibilisierung in IT-Sicherheitsbelangen im Mittelpunkt. Auch aktuelle Themen wie Zero Trust und Cloud spielen eine Rolle, wenn sich Verwaltungen nicht nur für die Gegenwart, sondern auch zukunftssicher aufstellen möchten. Hierbei ist eine ganzheitliche Betrachtung entscheidend. Die richtigen Überlegungen drehen sich also um die Fragestellungen, wie man sein Netzwerk, die Mitarbeitenden (User), Daten, Zugriffe und Geräte so absichert, dass die Kommune in Gänze geschützt ist. Benutzerverwaltung: Ein sehr guter und sicherer Weg ist die Kopplung einer IT-Sicherheitslösung mit dem favorisierten, im Einsatz befindlichen Verzeichnisdienst – wie beispielsweise dem Active Directory (AD). So wird auf einfache Weise ein automatisiertes und synchrones User-/Gruppen- und Rechte-Konzept etabliert. Das bedeutet, dass für jeden einzelnen User, für Gruppen oder gesamte Organisationseinheiten wie Referate oder Fachabteilungen dedizierte Zugriffsrechte und Attribute zentral vererbbar und automatisiert vergeben werden können. Besonders wichtig wird dies, wenn beispielsweise Mitarbeiter die Verwaltung verlassen sollten. Sobald der User im AD gelöscht wird, verschwinden auch sämtliche Zugriffsrechte im Netzwerk automatisch und werden gesperrt. Dadurch wird eine Kompromittierung durch einen alten Account verhindert und Angriffsszenarien eines so genannten „kalten“ Accounts von vornherein ausgeschlossen. Authentifizierung: Bei allen Themen rund um Authentifizierung müssen User und Geräte gleichermaßen betrachtet werden. Für Mitarbeiter im Homeoffice sollte beispielsweise mindestens eine Zwei-Faktor- oder besser eine Multi-Faktor-Authentifizierung eingesetzt werden. Nach der Regel „wissen und besitzen“ ist so ein höheres Security-Level erreichbar. Eine mobile Mitarbeiterin beispielsweise meldet sich mit Benutzernamen und Passwort an und muss als zweiten Faktor zusätzlich einen sicheren, zeitbasierten Token eingeben. Somit kann sich ein Angreifer mit einem erbeuteten Passwort ohne den zusätzlichen Token nicht verbinden und erlangt keinen Zugriff. Darüber hinaus können Geräte wie Laptops über dedizierte Maschinenzertifikate entsprechend identifiziert werden. Damit ist für die IT zu jeder Zeit sichergestellt, dass es sich auch beim verwendeten Gerät um ein bekanntes und sicheres handelt. **Haben ist besser als brauchen** Endpoint Security: Gerade bei Remote-Zugriffen ist es besonders wichtig, höchstmögliche Sicherheit zu gewährleisten. Neben dem User muss auch das Endgerät unter die Lupe genommen werden, mit dem auf Daten zugegriffen wird. Hierfür gibt es adäquate Technologien und Features, die bereits beim Aufbau eines verschlüsselten Tunnels eine Vielzahl von sicherheitsrelevanten Parametern überprüfen. Hierbei können das aktuelle Patch-Level des Betriebssystems, Zertifikatsgültigkeiten, aktuelle Viren- oder laufende Dienstinformationen auf dem Endgerät geprüft werden. Sogar technisch vollautomatisierte Compliance ist so einfach realisierbar. Ein besonderes Augenmerk sollte bei diesem so genannten Endpoint Policy Enforcement auf eigene Anpassbarkeit

(Customizability) gelegt werden, um in der Lage zu sein, individuelle Policies zu definieren, die automatisch bei allen Usern und Gruppen Anwendung finden. Network-Filtering: Um die Hoheit über die eigene Infrastruktur und das Netzwerk inklusive aller Assets zu sichern und zu behalten, sind detailliert definierte Filter für die User ausschlaggebend. Hierbei sollte granular konfiguriert werden, welche Netzwerk-Assets, -Ressourcen, -Daten, -Anwendungen und -Bereiche für die User/Gruppen zugänglich sein sollen und welche nicht. Durch solch ein professionelles Vorgehen hat die IT alle Fäden zentral in der Hand und kann sich zu jeder Zeit sicher sein, dass es keine unbefugten Zugriffe oder kein fehlerhaftes Nutzerverhalten gibt. Netzwerksegmentierung: Damit ein User nur auf relevante Assets im Netzwerk zugreifen kann, ermöglicht man bei der Segmentierung des eigenen Netzwerks und insbesondere bei der Mikrosegmentierung die Zugriffe folgendermaßen: Im Incident-Fall, also im Falle eines erfolgreichen Angriffs wie beispielsweise einer Ransomware-Attacke, muss der Angriff absolut isoliert bleiben, damit er sich nicht im Netzwerk ausbreitet. Durch dieses Vorgehen wird der Schaden wesentlich verringert und Auswirkungen sind schneller behoben, weil man sich nur um einen kleinen Teilbereich kümmern muss. Diese und andere Aspekte sind immens wichtig, um den Bedrohungen und Herausforderungen im Cyber-Raum Rechnung zu tragen. Wie bei Versicherungen aller Art gilt auch für Maßnahmen der IT-Sicherheit des mobilen Arbeitens der Grundsatz: Haben ist besser als brauchen.

()

BSI-Liste der zugelassenen IT-Sicherheitsprodukte und -systeme

Stichwörter: IT-Infrastruktur, NCP, Datenschutz, Homeoffice, IT-Sicherheit, mobiles Arbeiten