VPN-Software

Immer einen Schritt voraus

[20.10.2023] Angriffe auf die IT-Infrastrukturen von Unternehmen und Behörden ereignen sich mittlerweile tagtäglich. Die stark gestiegene Bedrohungslage erfordert ein Umdenken im kommunalen Bereich.

Mitte Juni 2023 ging in der Verwaltung von Hülben plötzlich gar nichts mehr. Angreifer hatten sich unbefugten Zugang zu den Servern der schwäbischen Gemeinde verschafft, die IT-Systeme der Verwaltung mussten heruntergefahren werden. Die Folge: Mitarbeiter konnten nicht mehr auf das kommunale Netz zugreifen, Telefon- und E-Mail-Systeme waren offline, online gebuchte Termine mussten abgesagt werden. Ob auch Daten von Bürgern abgeflossen sind, ist unklar. Die forensische Aufarbeitung des Falls dauert noch an. Was vor einigen Jahren noch ein Einzelfall gewesen wäre, reiht sich nun in eine lange Liste von Behörden und öffentlichen Einrichtungen ein, die in den vergangenen Monaten Opfer von Cyber-Attacken geworden sind. Selbst das Bundeskriminalamt schlägt angesichts der hohen Fallzahlen Alarm. „Diese Angriffe können massive Auswirkungen haben, wenn etwa Verwaltungen über Wochen nicht arbeitsfähig sind“, warnt BKA-Chef Holger Münch. „Wenn dann noch die technischen Hürden vergleichsweise niedrig sind, wird es für Kriminelle schnell attraktiv und damit lukrativ.“**IT-Sicherheitslevel steigern** Spätestens seit der Corona-Pandemie ist die Verwaltung in vielen Bereichen digitaler geworden. Gleichzeitig muss das IT-Sicherheitslevel angesichts zunehmender Cyber-Angriffe stetig steigen; und es dürfen durch die veränderten Arbeitsweisen keine neuen Sicherheitslücken entstehen. Was nach einer großen Aufgabe klingt, ist nicht unmöglich, wie das Beispiel der Stadt Baden-Baden zeigt. Matthias Götz, IT-Leiter der Stadtverwaltung, stand bereits Ende 2019 vor dieser Herausforderung. 60 Außenstellen, zwei Rechenzentren und 1.200 Mitarbeiter sollten nicht nur vernetzt, sondern auch für die Anforderungen von Remote Work fit gemacht werden. Gleichzeitig sollte das allgemeine IT-Sicherheitsniveau der Verwaltung erhöht und der bisher hohe Administrations- und Kostenaufwand reduziert werden. Nach einer intensiver Planungs- und Projektphase gelang dies mit der VPN-Lösung des Herstellers NCP, die einen komplett abgesicherten Datentransfer von den Mitarbeitenden zu den Servern der Stadtverwaltung ermöglicht. Wirtschaftlich sinnvoll integriert wurde die Lösung mit einem flexiblen Pay-per-Use-Kostenmodell, bei dem Baden-Baden alle benötigten VPN-Lizenzen zur Verfügung stehen, die Stadt am Ende des Monats aber nur die tatsächlich genutzten Zugänge bezahlt. Damit waren die primären Ziele der Umstellung erfüllt, doch die kommunalen IT-Verantwortlichen bemerkten durch den Wechsel auf das neue System noch weitere Vorteile. So bot die neue VPN-Software umfassende zentrale Konfigurationsmöglichkeiten, die den Administratoren die Verwaltung der Laptops und Mobilgeräte der Beschäftigten deutlich erleichterte. Zudem spürten auch die Mitarbeitenden selbst die Vorteile: Nach dem Start des Rechners genügte ein Mausklick, um die vorkonfigurierte Verbindung sicher und standortunabhängig herzustellen. Die Entscheidung, die eigene IT-Security-Lösung grundlegend zu überdenken, hat sich für Matthias Götz rückblickend gelohnt: „Ich würde raten, nicht abzuwarten, sondern die technischen und organisatorischen Veränderungen sofort anzugehen.“ **Hürden überwinden** Häufig haben kommunale Verwaltungen oder Dienstleister bei der Modernisierung ihrer IT-Infrastruktur spezielle Hürden zu überwinden. So benötigen viele Kommunen eine VPN-Lösung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) speziell für die Geheimhaltungsstufe VS-NfD (Verschlusssachen – Nur für den Dienstgebrauch) zugelassen ist. Doch gerade in diesem Punkt zieht der Bund derzeit die Zügel an. So hat das Bundesverwaltungsamt in den vergangenen Wochen alle Behörden, die mit dem Schengener Informationssystem (SIS) arbeiten, darüber informiert, dass für Remote-Work-Tätigkeiten im Umgang mit

VS-NfD zukünftig die entsprechenden technischen Anforderungen umgesetzt werden müssten und der Einsatz einer BSI-zugelassenen Lösung verpflichtend sei. Zweifellos steht bei bei der Suche nach einer geeigneten IT-Security-Lösung die Einhaltung aller Richtlinien zu VS-NfD-konformer Datenübertragung im Vordergrund. Auf dem Weg zu wirklich zukunftstauglichen IT-Umgebungen muss eine solche Lösung aber auch ein anwenderfreundliches Arbeiten ermöglichen, um die Produktivität der Nutzer nicht einzuschränken. Es gibt bereits entsprechende Software-Produkte, die es den Anwendern ermöglichen, mit handelsüblichen Windows-Laptops von jedem Standort aus auf das Datennetz ihrer Behörde zuzugreifen und dabei alle VS-NfD-Anforderungen zu erfüllen. Der Anwender selbst stellt die Verbindung mit wenigen Klicks her, alle sicherheitsrelevanten Prozesse laufen für ihn unsichtbar im Hintergrund ab. Dazu zählt beispielsweise ein Integritätsdienst, über den Administratoren alle Funktionalitäten des Betriebssystems im Hintergrund überwachen und auswerten. Mithilfe granularer Firewall-Regelungen können zudem alle Zugriffe auf das Netzwerk selbstbestimmt und über eine Management-Konsole Updates zentral an alle Benutzer ausgespielt werden. Der Umstieg auf eine moderne IT-Security-Lösung wie die von NCP kann sich also in vielerlei Hinsicht lohnen. Behörden werden sich immer gegen Angreifer wehren müssen – daher bleibt den Verantwortlichen nur der Weg nach vorne. Moderne IT-Security-Software-Produkte ermöglichen es, den Kriminellen immer einen Schritt voraus zu sein.

()

Dieser Beitrag ist in der Ausgabe Oktober 2023 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, NCP, mobiles Arbeiten, VPN, VS-NfD