Dell Technologies

Cyber-Resilienz ist mehr als Technik

[28.06.2023] Zunehmend rückt die öffentliche Verwaltung ins Visier von Cyber-Kriminellen. Um die Arbeitsfähigkeit zu gewährleisten, braucht es moderne Strategien für Cyber-Resilienz. Diese umfassen die gesamte Organisation: Neben der Technik müssen auch Menschen und Prozesse einbezogen werden.

Neue digitale Behördendienste und Homeoffice-Möglichkeiten für die Mitarbeiter haben die Angriffsfläche der öffentlichen Verwaltung in den vergangenen Jahren deutlich erhöht. Die Einrichtungen von Bund, Ländern und Kommunen stellen für Cyber-Kriminelle attraktive Ziele dar. Schließlich arbeiten solche Einrichtungen nicht nur mit den sensiblen Daten vieler Menschen und Unternehmen, sondern sind wichtig für das Funktionieren der Gesellschaft und Wirtschaft – daher bieten sie ein hohes Erpressungspotenzial. Dementsprechend häufen sich Angriffe mittels Ransomware, die den Zugriff auf Daten und Systeme durch Verschlüsselung verhindert und Behörden zur Zahlung eines Lösegelds zwingen soll.
Wie weitreichend die Folgen eines erfolgreichen Angriffs sind, ließ sich besonders eindrucksvoll am Beispiel des Landkreises Anhalt-Bitterfeld beobachten, der im Sommer 2021 nach einer Ransomware-Attacke den Katastrophenfall ausrufen musste und nach einem Jahr noch immer mit den Folgen zu kämpfen hatte. Auch andernorts konnten Verwaltungen ihren Aufgaben teilweise über Wochen und Monate nur eingeschränkt nachkommen, weil ihre IT-Systeme verschlüsselt wurden oder sie diese sicherheitshalber abgeschaltet hatten, um größere Schäden zu verhindern.
Dass die Wiederaufnahme des normalen Geschäftsbetriebs oft sehr lange dauert, liegt vor allem daran, dass sich Behörden meist auf die Abwehr von Cyber-Bedrohungen konzentrieren und ihre Cyber-Resilienz vernachlässigen. Ihnen fehlt nicht nur die Fähigkeit, nach einem erfolgreichen Angriff umgehend die richtigen Maßnahmen einzuleiten, um den Angriff zu stoppen und seine Auswirkungen zu minimieren. Es existieren häufig auch keine nutzbaren Datensicherungen mehr, da diese ebenso wie die Produktivsysteme durch den Angriff unbrauchbar gemacht wurden und nichts zur Wiederherstellung vorhanden ist.

Cyber-Resilienz ist eine umfassende Strategie

Wollen Behörden resilienter werden, müssen sie zunächst akzeptieren, dass selbst die besten Abwehrmaßnahmen keinen hundertprozentigen Schutz garantieren und sich Sicherheitsvorfälle nie vollständig vermeiden lassen. Zudem brauchen sie das Verständnis, dass Cyber-Resilienz kein Produkt ist, das sie einfach einkaufen können – stattdessen handelt es sich um eine Strategie, die Menschen, Prozesse und Technologien umfasst. Der erste Schritt zu mehr Cyber-Resilienz ist oft die Schulung der Mitarbeitenden, um deren Verantwortungsbewusstsein im Umgang mit IT zu erhöhen und Verhaltensweisen wie das sorglose Anklicken von Dateianhängen und Links in Mails mit zweifelhafter Herkunft auszuräumen.
Behörden sollten sich aber nicht allein auf Awareness-Trainings verlassen. Viele sicherheitsrelevante Entscheidungen können sie ihren Mitarbeitern abnehmen – etwa, indem sie USB-Ports am Arbeitsrechner sperren oder eigenmächtige Software-Installationen unterbinden. Damit ist der Einstieg in Zero Trust bereits geschafft. Dieses moderne Sicherheitskonzept reduziert Cyber-Risiken erheblich, indem es auf eine stärkere Netzwerksegmentierung, minimale Rechtevergabe und die konsequente Verifizierung aller Zugriffe setzt. Sollten Cyber-Kriminelle dann ein Passwort für ein System oder eine Anwendung erbeuten, können sie nur wenig damit anfangen: Der leichte Zugriff auf weitere Systeme oder Anwendungen

innerhalb der Behörde ist versperrt.

Offene Fehlerkultur als wichtiger Baustein

Häufig wird unterschätzt, welche Effekte eine positive Organisationskultur auf die Cyber-Resilienz hat. Sie erlaubt es Mitarbeitern, offen über Fehler zu sprechen, sodass die Organisation als Ganzes daraus lernen und im Ernstfall schnell handeln kann. Sie motiviert außerdem die Mitarbeiter, sich aktiv um Verbesserungen zu bemühen. Auch den Verwaltungen – und anderen Organisationen – insgesamt fällt es so leichter, eingefahrene Prozesse zu verändern oder völlig neue Prozesse zu etablieren.
Zu solchen neuen Prozessen zählen beispielsweise die Ausarbeitung von Notfallplänen und die Durchführung von Notfalltests. Solche Pläne stellen sicher, dass bei einem Cyber-Vorfall alle Abläufe und Verantwortlichkeiten geklärt sind – jeder weiß, was zu tun ist und wer Entscheidungen fällt. Das ist wichtig, damit die Maßnahmen, bei denen oft jede Minute zählt, nicht durch lange Abstimmungsprozesse und die Suche nach den Zuständigen ausgebremst werden. Durch regelmäßige Tests mit wechselnden Herausforderungen sammeln die Mitarbeiter dann praxisnahe Erfahrungen, damit im Ernstfall eine gewisse Routine herrscht und ein Rädchen tatsächlich perfekt ins andere greift. Zugleich sind solche Tests ein guter Realitätscheck, ob die Pläne den Anforderungen noch gerecht werden – schließlich verändern sich IT-Infrastrukturen kontinuierlich, wodurch auch die Notfallpläne angepasst werden müssen.

Ein Blick von außen kann helfen

Die notwendigen Veränderungsprozesse innerhalb der Organisation, die Auswahl geeigneter Lösungen, die Entwicklung von Notfallplänen und deren Test – all das kann vor allem die Verwaltungen kleinerer Kommunen schnell überfordern. Allein schon die Entscheidung, welche Systeme nach einem Komplettausfall der IT als erste wieder einsatzbereit gemacht werden müssen, ist gar nicht so leicht: die mit den für das Tagesgeschäft wichtigen Verwaltungsanwendungen oder doch eher die Back-up-Server und das Active Directory? Ein IT-Dienstleister mit Erfahrung und technischer Expertise kann hier unterstützen. Er weiß, wie Infrastrukturen und Prozesse aussehen müssen, damit sie resilient sind, und wo Stolperfallen lauern.
Ohne den Blick von außen neigen Behörden ebenso wie Unternehmen dazu, an einer bestehenden IT-Umgebung und alten Abläufen festzuhalten. Der Versuch diese zu erhalten und lediglich zu verändern, führt oft zu einem Sammelsurium aus Speziallösungen, die an die vorhandenen Systeme angehängt werden. Dadurch können Aufwand und Kosten für die Administration erhöht werden ebenso wie die Ausfallzeit, wenn tatsächlich ein Cyber-Angriff eintritt. Oft ist es besser, einen Strich zu ziehen und optimale Infrastrukturen und Prozesse ganz neu zu erarbeiten. Erst im Anschluss kann man Wege suchen, um dieses Ziel zu erreichen und dabei auch prüfen, welche bestehenden Systeme und Abläufe angepasst werden können. Dabei können IT-Dienstleister mit einem breiten Portfolio an Lösungen für Security und Data Protection sinnvoll unterstützen.

Klassische Ansätze reichen nicht mehr aus

Der technologische Kern einer Resilienzstrategie ist eine moderne Data Protection, die sicherstellt, dass sich Daten auch nach einer schwerwiegenden Ransomware-Attacke wiederherstellen lassen. Klassische Back-up-Ansätze und Disaster-Recovery-Strategien können das nicht leisten, weil Schadprogramme inzwischen gezielt Datensicherungen und an Remote-Standorte replizierte Daten verschlüsseln. Benötigt werden Back-up-Speicher mit einem so genannten Retention Lock oder Datentresore. Ein Retention Lock verhindert, dass hinterlegte Daten vor Ablauf einer definierten Aufbewahrungsfrist gelöscht oder verändert werden. Die Daten sind dann nicht nur vor Ransomware, sondern auch vor menschlichen Fehlern sicher.

Datentresore wiederum schotten wertvolle Daten ab, indem sie sie unbefugten Zugriffen entziehen. Solche Tresore sind nur kurzzeitig im Netzwerk erreichbar, um eine Datenkopie aufzunehmen, Manipulationen erkennen sie mittels einer intelligenten Forensik. Solche Speichersysteme können die wertvollsten Daten, größere Back-ups oder auch eine komplette Ersatzinfrastruktur für den Ernstfall aufnehmen – letztlich ist es eine Frage der Kosten sowie der Datenverluste und Ausfallzeiten, die eine öffentliche Verwaltung hinnehmen kann.
Man sieht: Cyber-Resilienz ist ein durchaus komplexes Thema, das sich sicher nicht nebenbei bearbeiten lässt und Investitionen erfordert – sowohl in das Personal als auch in die Technik. Die neuen Aufgaben und Verantwortungen sollten nicht einfach in die Hände von IT-Administratoren gelegt werden, sondern erfordern Spezialisten wie einen dedizierten Chief Information Security Officer (CISO) als Gesamtverantwortlichen für die IT-Sicherheit.

()

Stichwörter: IT-Sicherheit,