Serie Cyber-Sicherheit

Schwachstellen minimieren

[28.11.2022] Viele Maßnahmen zur Erhöhung der Cyber-Sicherheit sind organisatorischer Natur und oft auch ohne IT-Fachkenntnisse realisierbar. In Teil 2 unserer Serie geben wir sieben Einsteiger-Tipps, die es Angreifern erschweren, Schaden zu verursachen.

Ein nicht abgewehrter Cyber-Angriff ist für jede Kommunalverwaltung ein potenzielles Desaster. Trotz der Gefahren können insbesondere kleine und mittlere Kommunen viele der empfohlenen Maßnahmen zur Steigerung der Cyber-Sicherheit nicht umsetzen, weil Personal und Mittel fehlen. In jedem Fall sollten die folgenden sieben Einsteiger-Tipps beachtet werden.

Rechteverwaltung: In den gängigen Betriebssystemen gibt es die Möglichkeit, Benutzerkonten einzurichten. Diesen Konten können unterschiedliche Rechte zugewiesen werden. Hierzu gehören Zugriffsrechte auf Dateien, Ordner und Bereiche, Lese- und Schreibzugriffe sowie die Berechtigung, Software zu installieren. Verschafft sich ein Cyber-Krimineller Zugang zu einem Benutzerkonto, hat er zunächst die Rechte dieses Benutzers. Die Rechte sollten rollenbasiert an die Mitarbeiterinnen und Mitarbeiter vergeben werden. Jeder erhält nur die für seine Arbeit unbedingt notwendigen Rechte. Konten mit Administratorenrechten werden ausschließlich für Administrationsaufgaben genutzt – auch von den Administratoren selbst. Diese Maßnahme bietet zwar keinen Schutz vor Vollverschlüsselung oder Kriminellen, die wissen, wie sie Berechtigungen erweitern können – eine strenge Rechtevergabe kann es Angreifern jedoch erschweren, Schaden zu verursachen.

Regelmäßige Schulungen: Cyber-Sicherheit ist in hohem Maße von den Kenntnissen und der Wachsamkeit der Mitarbeitenden abhängig. Sie sind es, die suspekte E-Mails, Anrufe und SMS-Nachrichten erkennen und richtig handeln müssen. Doch die Strategien der Cyber-Kriminellen sind stetig im Wandel. Regelmäßige Schulungen zu Angriffsarten sowie zur Cyber- und IT-Sicherheit sind daher essenziell. Es gibt inzwischen zahlreiche Anbieter von Awareness-Schulungen, die teilweise im Selbststudium durchgeführt werden können (siehe Kasten Link-Tipps). Neben regelmäßigen Schulungen sollten Führungskräfte eine positive Fehlerkultur etablieren. Schäden lassen sich verhindern, wenn Beschäftigte sich trauen, den Klick auf eine dubiose Anlage oder das merkwürdige Verhalten ihres Rechners zu melden. Cyber-Kriminelle manipulieren ihre Opfer, indem sie Stress und Angst erzeugen. Das geschieht durch Angriffe zu Zeiten mit hoher Arbeitsbelastung, die Themenwahl oder suggerierter Dringlichkeit der Nachricht. Der Angreifer möchte dem Opfer keine Zeit zum Nachdenken lassen – Führungskräfte können mit einer positiven Fehlerkultur dagegenhalten.

Passwörter: Es sollten starke Passwörter vergeben und pro Anwendung oder Zugang ein eigenes Passwort verwendet werden. Starke Passwörter sind möglichst lang und komplex. Im Idealfall besteht ein Passwort aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen. Die Länge der Passwörter ist dabei wichtiger als die Komplexität. Einfache Passwörter wie Namen oder Begriffe können durch eine Brute-Force-Attacke in weniger als einer Sekunde geknackt werden. Hierbei werden Passwörter automatisiert mit Wörterbüchern abgeglichen. Das Knacken von langen Passwörtern, die Groß- und Kleinbuchstaben sowie Sonderzeichen und Zahlen enthalten, dauert deutlich länger. Passwörter sollten regelmäßig geändert werden. Dadurch werden gestohlene Passwörter wertlos. Auch das neue Passwort muss natürlich lang und komplex sein. Muster wie das Durchnummerieren von Passwörtern sollten vermieden

werden. Um sich all diese Passwörter merken zu können, ist ein Passwort-Manager empfehlenswert. Merken muss man sich dann nur noch das Master-Passwort.

Gestohlene Nutzerdaten: Einer der häufigsten Angriffsvektoren sind gestohlene Nutzerdaten. Cyber-Kriminelle können diese verwenden, um sich im System anzumelden, sich auf Dienste der Kommune aufzuschalten oder gar Phishing-E-Mails mit der Kommune als vermeintlichen Absender zu verschicken. Ob E-Mail-Adressen und weitere Daten gestohlen wurden, lässt sich beispielsweise mit dem HPI Identity Leak Checker überprüfen. Für mittlere und große Kommunen bietet das HPI zentralisierte Lösungen an. Das Hessen CyberCompetenceCenter (Hessen3C) stellt hessischen Kommunen zur Unterstützung der IT-Sicherheit den Hessen Leak Checker zur Verfügung.

Patch Management: Jede Soft- und Hardware kann Sicherheitslücken aufweisen. Sobald diese Schwachstellen öffentlich bekannt werden, beginnt ein Rennen gegen die Zeit. Auf der einen Seite die Cyber-Kriminellen, die Sicherheitslücken immer schneller auszunutzen wissen – auf der anderen Seite die Hersteller und Systemadministratoren, die schnellstmöglich Sicherheitsupdates, so genannte Patches, erstellen, veröffentlichen und installieren müssen. Kommunen sollten eine Übersicht der von ihnen verwendeten Soft- und Hardware erstellen und die Websites der Hersteller regelmäßig auf Sicherheitsupdates überprüfen. Auch auf Warnungen in der Fachpresse sollte geachtet werden. Ist eine Schwachstelle bekannt, für die noch kein Sicherheitsupdate veröffentlicht wurde, kann es notwendig sein, das Programm vorübergehend für die Benutzung zu sperren. Häufig sind hiervon Browser wie Chrome, Firefox und Edge betroffen. Für den Fall einer Sperrung sollten Alternativen zur Verfügung stehen.

Datensicherungsstrategie: Ein Muss sind regelmäßige Back-ups, also Sicherungskopien aller Daten. Dabei ist zu prüfen, ob alle wichtigen Daten gesichert werden, die Back-ups funktionieren und der Sicherungsturnus zum tolerierbaren Datenverlust passt. Ein Verschlüsselungsangriff kann eine Kommune so nur um einen gewissen Zeitraum zurückwerfen. Wichtig ist, dass auch Offline-Sicherungen der Back-ups zur Verfügung stehen. Die Back-ups sollten nicht dauerhaft mit dem System verbunden sein, da sie sonst mitverschlüsselt werden könnten. Manchmal halten sich Hacker über längere Zeiträume in Systemen auf. Es ist daher hilfreich, auch ältere Back-ups zu besitzen, um im Notfall den älteren, aber schadsoftwarefreien Stand wiederherzustellen.

Krisen-Management: Die Wahrscheinlichkeit, Opfer eines Cyber-Angriffs zu werden, war noch nie so groß wie heute. Kommunalverwaltungen sollten daher vorab festlegen, wer in einer Krise für was zuständig ist. Wer ist wie von wem zu alarmieren? Liegen die aktuellen Kontaktdaten aller krisenwichtigen Beschäftigten auch in Papierform vor? Je genauer Abläufe festgelegt, dokumentiert und kommuniziert werden, desto besser kann im Ernstfall reagiert werden. Sinnvoll ist es, schon vorab nach Einrichtungen zu suchen, die im Notfall Unterstützung leisten können, etwa Nachbarkommunen, die übergangsweise Rechner zur Verfügung stellen, damit wichtige Services schnell wieder angeboten werden können.

()

Kurs „Tatort Internet“ des Hasso-Plattner-Instituts
BSI-Online-Kurs zum IT-Grundschutz
Online-Kurs zum IT-Grundschutz (PDF, 6 MB)

Stichwörter: IT-Sicherheit, Cyber-Sicherheit