Cybersicherheit

Die Angriffsflächen minimieren

Cyberkriminelle nehmen, was sie kriegen können, ob beim Angriff auf einen Großkonzern oder auf das Rathaus. In der öffentlichen Verwaltung muss daher die IT-Sicherheit oben auf der Agenda stehen. Es geht um technische Hackerabwehr, aber auch darum, die Mitarbeiter zu sensibilisieren.

Mögen Unternehmen und Behörden in ihren Aufgaben noch so unterschiedlich sein – in einem Punkt trennt sie nichts: der Gefahr, ins Visier von Cyberkriminellen zu geraten. Sie alle sind den gleichen Gefahren ausgesetzt – von Advanced Persistent Threats, Malware oder Botnets über Trojaner, Viren und Ransomware bis hin zu Drive-by-Downloads, Phishing sowie Zero-Day-Attacken, sagt Michael Haas. Er ist IT-Sicherheitsexperte bei Watchguard Technologies und besitzt spezifische Erfahrungen mit den Anliegen von Kunden im Umfeld öffentlicher Verwaltungen.

Gerade die Vielzahl der Bedrohungen und ihre zunehmende Komplexität erfordert ein erhöhtes Bewusstsein und passgenaue Lösungen zum Schutz der Netzwerke und Daten. Eines der größten Probleme derzeit ist Phishing, also der Versuch, über gefälschte E-Mails oder Webseiten an persönliche Daten des Nutzers zu gelangen oder Schadsoftware zu verbreiten. Anschaulich zeigt dies der Trojaner Emotet. Selbst ohne Infektion wurde vielerorts das Tagesgeschäft beeinflusst. So sperrte etwa das Landratsamt Oberallgäu – wie andere Behörden auch – vorsorglich den Empfang von Office-Dokumenten.

Gerade hinsichtlich der Bürgerdaten obliegt öffentlichen Verwaltungen eine besondere Verantwortung. „In dem Zusammenhang kann man nicht wirklich zwischen der Sicherheit der kommunalen IT-Systeme und Daten trennen. Cybersicherheit ist viel mehr als nur ein IT-Thema, es geht um die öffentliche Sicherheit“, betont Haas. Er selbst macht ganz unterschiedliche Erfahrungen, wie in Rathäusern mit dem Thema IT-Sicherheit umgegangen wird. Manche Gemeinden seien in dem Bereich sehr fortschrittlich und hätten die Sicherheit ihrer Systeme weit oben auf ihrer Agenda stehen mit klaren Vorstellungen.

Wie stark sich einzelne Auftraggeber mit dem Thema auseinandergesetzt haben, spiegeln nicht zuletzt die Ausschreibungen. Daher ist vor allem auf Seiten der Hersteller und IT-Partner Aufklärungs- und Beratungskompetenz gefragt. Zudem werden Lösungen benötigt, die komplexe Bedrohungen abwehren können und gleichzeitig einfach zu handhaben sind.

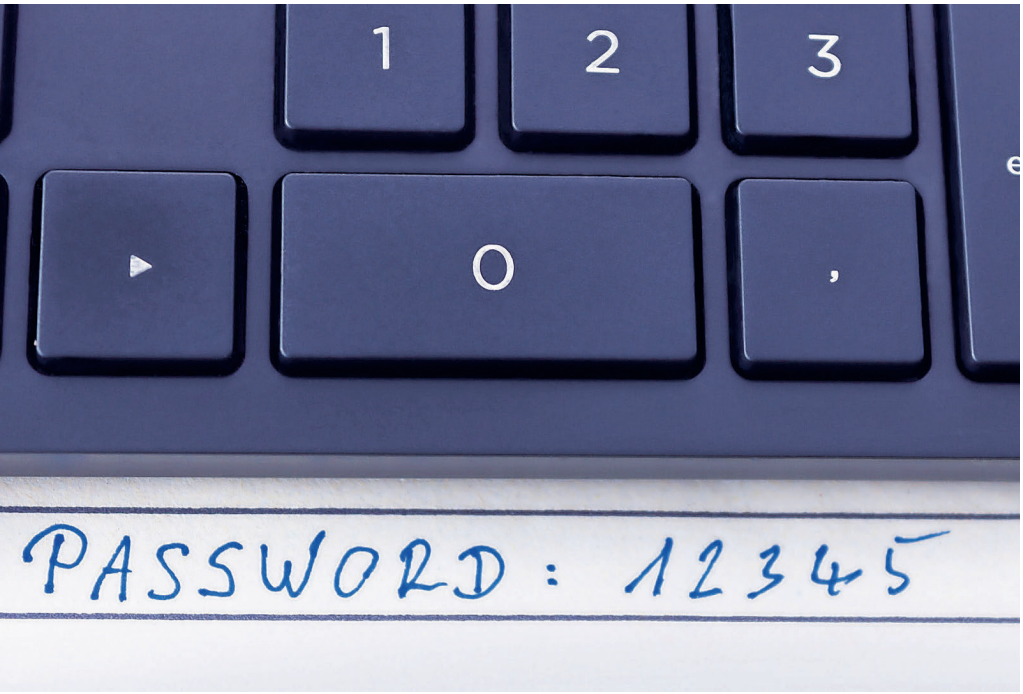

Foto: Echelon IMG/Adobe Stock

Passwort ohne Wert: Beim Thema IT-Sicherheit müssen die Mitarbeiter ins Boot geholt und über die Gefahren sorglosen Handelns informiert und entsprechend geschult werden.

ANTIVIRUS-DIENST AUF DIE NEUE ART

Denn es geht in erster Linie darum, mit den immer ausgefeilteren Angriffsmethoden Schritt zu halten. Die Bedrohungslandschaft entwickelt sich stetig weiter. Systeme, die vor zwei Jahren noch auf dem neuesten Stand der Technik waren, können heute funktionale Lücken aufweisen, die Hacker gezielt ausnutzen. „Entsprechend müssen die Abwehrstrategien regelmäßig hinsichtlich ihrer Wirksamkeit hinterfragt werden. Zur Aufdeckung von Angriffen reicht ein klassischer, signaturbasierter Antivirus-Dienst zum Beispiel kaum noch aus“, sagt Haas.

Sein Unternehmen hat einen Service entwickelt, mithilfe dessen Malware unter Einsatz künstlicher Intelligenz erkannt wird. Andere Funktionsbausteine rücken dem Phishing zu Leibe: Wird ein angeklickter Link als gefährlich eingestuft, blockiert ihn das System automatisch.

Innovative Erkennungs- und Abwehrtechniken sind nur die eine Hälfte der Cybersicherheit – es müssen auch die Mitarbeiter ins Boot geholt werden. Sie sind über Gefahren zu informieren und entsprechend zu schulen, beispielsweise hinsichtlich des Umgangs mit Passwörtern. Haas: „Nur über die Kombination von fortschrittlichen Sicherheitstechnologien und aufmerksamen Mitarbeitern lässt sich die Angriffsfläche auf ein Minimum eingrenzen.“ *Wolfram Markus*