PwC Deutschland

IT-Sicherheit für die öffentliche Verwaltung

[20.12.2021] Die Wirtschaftsprüfungs- und Beratungsgesellschaft PricewaterhouseCoopers (PwC) gibt vor dem Hintergrund häufiger Cyber-Attacken grundlegende Tipps, wie Behörden und Ämter ihre Daten und Systeme vor solchen Angriffen schützen können.

Um ihre Daten und Infrastrukturen vor Cyber-Attacken zu schützen, müssen Ämter und Behörden auch 2022 ihre IT-Sicherheit weiter stärken. Darauf weist die Wirtschaftsprüfungs- und Beratungsgesellschaft PricewaterhouseCoopers (PwC) hin. Immer öfter würden kommunale Verwaltungen zum Ziel schlagkräftiger Cyber-Attacken. PwC verweist auf eine Umfrage von Zeit Online und dem Bayerischen Rundfunk, der zufolge in den vergangenen sechs Jahren insgesamt mindestens 100 Ämter und Behörden von Cyber-Attacken betroffen waren. Wie gravierend die Folgen solcher Attacken ausfallen können, zeige der Landkreis Anhalt-Bitterfeld. Dort hatten Unbekannte die Daten der Verwaltung verschlüsselt und damit für Wochen die gesamte IT lahmgelegt. Auch aktuelle Zahlen des Bundesamts für Sicherheit in der Informationstechnik (BSI) bestätigten, dass Ämter und Behörden einem solchen Worst-Case-Szenario oft nur knapp entgingen, berichtet PwC. Von Juni 2020 bis Mai 2021 habe das BSI jeden Monat rund 44.000 E-Mails mit Schadprogrammen in den Regierungsnetzen abgefangen. Aufgrund der komplexen Organisationsstrukturen und knappen Ressourcen in der öffentlichen Verwaltung würden die Fachkräfte in den Behörden unter erschwerten Rahmenbedingungen gegen diese Gefahren kämpfen. Daher sei es von entscheidender Bedeutung, „gewisse Grundlagen“ beim Schutz der IT-Infrastrukturen zu beherzigen, so PwC. Der PwC-Experte für Cyber-Sicherheit im öffentlichen Sektor bei PwC Deutschland, André Glenzer, nennt fünf wichtigste Maßnahmen, die zu einer sichereren IT in der öffentlichen Verwaltung beitragen können.

Für den Worst Case gewappnet

Um alle sicherheitsrelevanten Parameter lückenlos abzustecken, sei es für Organisationen aus der öffentlichen Verwaltung wichtig, ein Management-System für die Informationssicherheit (ISMS) aufzustellen. Damit seien alle notwendigen Maßnahmen, Vorgaben und Hilfsmittel definiert, um die Informationssicherheit innerhalb der Organisation zu garantieren. So könnten verpflichtende Standards für sämtliche Mitarbeitende durchgesetzt und etwaige Verstöße und Sicherheitsrisiken frühzeitig erkannt werden. Für den öffentlichen Sektor biete sich dazu der IT-Grundschutz des BSI an (wir berichteten). Anknüpfend an das ISMS seien Behörden auch gut beraten, einen konkreten Notfallplan (Cyber Incident Response Plan) aufzustellen. Ein solcher Leitfaden definiere für den Fall eines Angriffs sämtliche Abläufe und Maßnahmen zur Begrenzung des Schadens. Wenn alle Notfallmaßnahmen richtig ineinandergriffen, könnten Behörden bei der Abwehr eines Angriffs wertvolle Zeit gewinnen und den Schaden eingrenzen. Ein solcher Notfallplan müsse regelmäßig geübt und die Übungen ausgewertet werden. Neben kriminellen Angreifenden können auch die eigenen Angestellten – ohne böse Absicht – ein Sicherheitsrisiko für die IT-Sicherheit darstellen. Dies zeige sich in verschiedenen Untersuchungen. So seien raffinierte Phishing- oder Social-Engineering-Kampagnen für ungeschulte Personen nur schwer zu identifizieren. Daher sei es wichtig, die gesamte Belegschaft regelmäßig hinsichtlich der Bedrohungsszenarien zu schulen. Alle Schulungen sollten ebenfalls dokumentiert werden.

Schwachstellen schließen

Wenn Mittel wie Phishing oder Social Engineering nicht greifen, suchen sich Kriminelle gerne andere Hintertüren, um an die Daten von Ämtern und Behörden zu gelangen. Sogar Stellenausschreibungen können potenziellen Angreifenden Hinweise auf leichte Ziele geben, berichtet PwC. Suche eine Einrichtung beispielsweise nach Administratoren mit Kenntnissen für veraltete Systeme wie Windows 7 oder Windows Server 2008 R2, können Kriminelle davon ausgehen, dass die IT-Infrastruktur vor Ort nicht auf dem neuesten Stand und somit verwundbar sei. Es sei wichtig, den Angreifenden zuvorzukommen. Zunächst einmal bestehe die Möglichkeit, Anwendungen und Netzwerke mit einem Schwachstellen-Scanner automatisiert auf Sicherheitslücken zu überprüfen. Für tiefergreifende Analysen seien jedoch externe Fachleute erforderlich – so genannte Penetration Tester, die aus Angreiferperspektive versuchen, in die Kundensysteme einzudringen. Der PwC-Experte Glenzer weist darauf hin, dass einmalige Schwachstellen-Tests meist wirkungslos verpuffen. Es gelte also, diese langfristig zu planen und in Abhängigkeit des ermittelten Schutzbedarfs entsprechend zu wiederholen.
Behördliche Informationssicherheitsbeauftragte sollten sich auch nicht allein auf den Perimeterschutz etwa durch eine Firewall verlassen. Dieser Schutz könne jedoch bei Wartungsarbeiten oder durch Unachtsamkeit ausgehebelt werden – in einem solchen Moment könnten Angreifende umgehend in die Systeme eindringen. Daher sei es innerhalb des Risiko-Managements wichtig, IT-Systeme und Anwendungen grundsätzlich so zu behandeln, als wären diese jederzeit frei über das Internet erreichbar. Als Maßnahmen, um auch innerhalb geschlossener Netze das Sicherheitsniveau zu erhöhen, nennt PwC das Einsetzen eines Security Information and Event Managements (SIEM), Verschlüsselungsmaßnahmen und ein stringentes Patchmanagement. In Kombination könnten solche Maßnahmen die Auswirkungen neuer Schwachstellen wie jüngst Log4Shell deutlich mindern.

(sib)

Stichwörter: IT-Sicherheit, PwC, Log4Shell