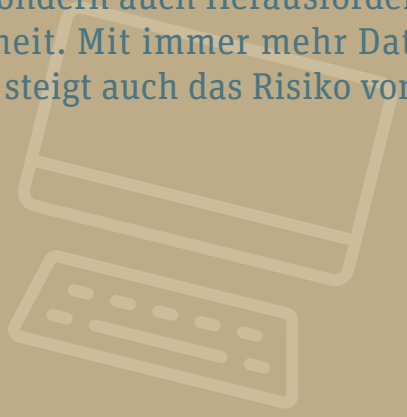
Cybersecurity
Neue Technologien erhöhen die Sicherheit und den Datenschutz der öffentlichen Verwaltung

Digitale Transformation bedeutet für die öffentliche Verwaltung nicht nur Möglichkeiten, sondern auch Herausforderungen – insbesondere in Bezug auf die Cybersicherheit. Mit immer mehr Daten, die digital erfasst und verarbeitet werden, steigt auch das Risiko von Cyberangriffen.



Die jüngsten Angriffe auf kommunale Verwaltungen und Infrastrukturen haben die Gefahren von Ransomware und Supply-Chain-Attacken, bei denen die Angreifer Schadcode über Bibliotheken und Softwareprodukte von Partnerunternehmen oder Open-Source-Projekten einschleusen, in den Vordergrund gerückt. Diese zwei Beispiele für unmittelbare Bedrohungen können lähmend wirken, wenn nicht die richtigen Sicherheitsmassnahmen ergriffen werden.

Sicherheitszertifikate als Vertrauensbasis

Zertifizierungen der IT-Sicherheit, z. B. nach ISO 27000 oder mit dem Schweizerischen Cyber-Safe-Label, tragen dazu bei, das Vertrauen in digitale Lösungen der öffentlichen Verwaltung zu stärken. Grundlage hierfür ist ein robustes Informationssicherheitsmanagementsystem (ISMS), das einen systematischen Ansatz für das Management von Cybersicherheitsrisiken gewährleistet.

Allerdings muss die Verwaltung sicherstellen, dass Geräte und Daten auch ausserhalb des eigenen Perimeters sicher sind. Die Zunahme an Remote-Arbeitsmodellen (Homeoffice) und die Integration über Behördengrenzen hinweg fordert Sicherheit über Systemgrenzen hinweg. Mechanismen wie Remote Attestation, d. h. dem sicheren Nachweis, dass vertrauenswürdige Software auf Geräten ausserhalb unserer direkten Kontrolle ausgeführt wird, können dabei helfen, neue Anwendungsszenarien sicher auszugestalten (z. B. Remote-Arbeit an vertraulichen Daten oder verteilte Online-Prüfungen).

Datenschutz und Anonymisierung

Sicherheit ist auch eine Voraussetzung für Datenschutz – ohne einen starken Schutzmechanismus können Daten nicht anonymisiert und somit nicht rechtskonform für KI-Zwecke genutzt werden (vgl. «KI im öffentlichen Sektor», S. 50). Zur Nutzung von KI in der Verwaltung muss der Zweck der Datenerfassung genau definiert sein. Es muss garantiert sein, dass die Daten angemessen geschützt sind. Zudem stellt Anonymisierung von Daten eine grosse Herausforderung dar, weil immer mehr Datensätze zusammengeführt werden, was dazu führen kann, dass Profile von Einzelpersonen «berechnet» werden können. Beim Einsatz von Technologien, beispielsweise im Bereich der «Smart Cities» in einem städtischen Umfeld, muss dem Datenschutz deswegen besondere Beachtung geschenkt werden (vgl. «Smart City», S. 30).

Insgesamt ist die Cybersicherheit in der öffentlichen Verwaltung nicht nur eine technische, sondern auch eine organisatorische und kulturelle Herausforderung. Nicht zuletzt ist die Schulung der Mitarbeitenden punkto Cybersicherheit und Datenschutz unerlässlich. Schliesslich kann die beste Technologie nicht vor menschlichen Fehlern schützen. Grundlage hierfür ist die Förderung der Sicherheitskultur innerhalb der Organisation. Alle Mitarbeitenden sollen Sicherheit und Datenschutz als gemeinsame Verantwortung wahrnehmen und proaktiv zur Verbesserung der Cybersicherheit beitragen. Cybersicherheit ist eine kontinuierliche Aufgabe aller Beteiligten, die ständige Wachsamkeit und Anpassung erfordert.

Unsere Empfehlungen

1. Investieren in Cyberschulungen
Alle Mitarbeitenden sollten die Grundlagen der Cybersicherheit in ihren Verantwortungsbereichen kennen und anwenden können.

2. Den Datenschutz überdenken
Datenschutz beginnt mit Cybersicherheit. Verwaltungen sollten sicherstellen, dass ihre Daten durch solide Sicherheitspraktiken geschützt sind.

3. Auf Technologie setzen
Fortschrittliche Mechanismen wie Remote Attestation und Zertifizierungen erhöhen das Sicherheitsniveau der digitalen Ressourcen in der Verwaltung.

Mehr Informationen

Kontaktmöglichkeiten und weitere Informationen zu Cybersecurity im öffentlichen Sektor:
bfh.ch/ipst/cyber-security

Kontakt

Prof. Dr. Sebastian Höhn
Dozent

sebastian.hoehn@bfh.ch
T +41 31 848 44 26