Erfolgsfaktor Informationssicherheit

Sichere Lösungen für die Digitalisierung der Behörden

Dieses Whitepaper stellt die zentralen Handlungsfelder in Sachen Informationssicherheit vor und zeigt konkrete Lösungsansätze auf.

Herausforderung Informationssicherheit

Die Digitalisierung beschäftigt Schweizer Behörden und öffentliche Verwaltungen. Dabei rücken neben Chancen vermehrt auch Risiken ins Bewusstsein: Cyberangriffe sind an der Tagesordnung und gleichzeitig intensiviert sich der digitale Datenaustausch.

Studien zeigen: Schweizerinnen und Schweizer wollen ihre Behördengeschäfte schnell und unkompliziert erledigen. Diesem Wunsch kommen Behörden auf allen Staatsebenen nach und bauen ihr E-Government-Angebot laufend in Richtung «Digital First» aus.

Der Ausbau des Onlineangebots geht aber auch mit zusätzlicher Verantwortung einher, denn digitale Behördendienstleistungen müssen eine hohe Sicherheit aufweisen. Die Behörden stehen demnach in der Pflicht, für umfassenden Cyberschutz zu sorgen.

Dieser Verantwortung sind sich die Entscheidungstragenden in der öffentlichen Verwaltung bewusst. Gemäss «Trendradar 2022: Handlungsansätze für die öffentliche Verwaltung», einer Studie des Beratungsunternehmens PwC und der Universität St. Gallen, stufen 99 Prozent der Befragten die Stärkung der Cyber- und Informationssicherheit als «sehr relevant» ein.

« Informationssicherheit ist in der DNA der Post. »

Marcel Zumbühl, Chief Information Security Officer Post

Digitalisierung braucht Vertrauen

Die Vorteile von E-Government liegen auf der Hand: Behörden profitieren von höherer Prozesseffizienz, Nutzerinnen und Nutzer erhalten mehr Flexibilität. Gleichzeitig bestehen Bedenken betreffend Datenschutz.

Grundsätzlich hat die Schweizer Bevölkerung ein hohes Vertrauen in die Behörden, wenn es um die Behandlung vertraulicher Daten geht. In der Studie «Datenschutz in der Schweiz» der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) stimmten 74 Prozent der Befragten der Aussage, dass Behörden personenbezogene Daten ordnungsgemäss und vertraulich behandeln, eher oder vollständig zu. Diese hohe Zustimmung ist eine gute Grundlage, um Bedenken zum Datenschutz bei der Nutzung digitaler Kanäle aus dem Weg zu räumen.

Der Datenschutz regelt das Recht jeder und jedes Einzelnen, über die Verwendung und Weitergabe der eigenen personenbezogenen Daten zu bestimmen. Der Datenschutz soll die Privatsphäre schützen und Datenmissbrauch von Dritten unterbinden. Das Datenschutzgesetz legt fest, wie Daten erhoben, verarbeitet, genutzt oder gelagert werden. Um alle gesetzlichen Anforderungen an den Datenschutz bei E-Government-Services zu erfüllen, ist die Informationssicherheit von entscheidender Bedeutung. Sie umfasst Massnahmen und Technologien zur Verhinderung von Missbrauch, Verfälschung und Verlust von Daten und stellt Vertraulichkeit sicher.

Datenschutz und Informationssicherheit sind zentrale Elemente, um die Akzeptanz digitaler Lösungen weiter zu steigern und das Vertrauen in E-Government zu stärken. Das gilt für Einwohnerinnen und Einwohner ebenso wie behördenintern. Angesichts der zunehmenden Gefährdung von Daten durch Cyberangriffe muss der Informationssicherheit höchste Priorität eingeräumt werden. Das schafft Vertrauen in digitale Angebote.

Weitere Informationen zum neuen DSG:
https://digital-solutions.post.ch/de/datenschutz-incamail

« Die eigenen Risiken zu kennen, ist in der Cyber Security zentral. »

Marcel Zumbühl, Chief Information Security Officer Post (CISO)

Fünf Herausforderungen mit Blick auf die Informationssicherheit

Behörden benötigen sichere Verfahren zur Identifikation, Übermittlung und Speicherung von Daten, um ihre Cyber- und Informationssicherheit zu stärken. Dabei sollten sie ihr Augenmerk aktuell auf folgende fünf Herausforderungen legen:

1

Neues Datenschutzgesetz: höhere Anforderungen an die Compliance
Am 1. September 2023 tritt das neue Schweizer Datenschutzgesetz (DSG) in Kraft. Damit gelten verschärfte Regeln zur Bearbeitung von Personendaten.

Eine zentrale datenschutzrechtliche Vorgabe des DSG ist Informationssicherheit. Für die gesetzeskonforme Umsetzung sind eine Bestandsaufnahme über die Bearbeitung von Personendaten und eine Risikobewertung erforderlich, um die Anforderungen an die Datenschutz-Compliance zu bestimmen.

Auch gilt es, Mitarbeitende zu sensibilisieren und ein IT-Sicherheitskonzept zu entwickeln, das ausreichend Schutz gegen Schadsoftware, Datendiebstahl oder -verlust bietet.

2

Aktuelle Bedrohungslage: ganzheitliches Risikomanagement
Cyberangriffe sind an der Tagesordnung. Bis ein Vorfall registriert wird, vergehen im Durchschnitt 100 Tage. Seit Jahresbeginn hat das Nationale Zentrum für Cybersicherheit (NCSC) 10 000 Meldungen erhalten (Stand Ende April).

Die Bedrohungslage hat sich massiv verschärft und die Angreiferinnen und Angreifer gehen immer raffinierter vor: Ransomware as a Service (RaaS), Supply-Chain-Angriffe oder neue Social-Engineering-Taktiken gehören gemäss Angaben des NCSC aktuell zu den häufigsten Bedrohungen.

Die hohe Dynamik im Bereich Cybergefahren erfordert ein ganzheitliches Risikomanagement. Um mit der Entwicklung Schritt zu halten, sind regelmässige Updates von Hard- und Software unerlässlich.

3

Remote-Arbeit:
Informationssicherheit auch im Homeoffice
Auch im Behördenumfeld haben sich hybride Arbeitsformen etabliert. Damit geht mit der Bearbeitung der teils sensiblen Daten ein erhöhtes Risiko einher. Denn die Daten sind stärker fragmentiert, wodurch die Schwachstellen zunehmen. Deshalb braucht es Lösungen, um die Daten auch in Homeoffice-Umgebungen effektiv zu schützen.

4

Bewusstsein schaffen:
Schulung und Sensibilisierung der Mitarbeitenden
Technische Massnahmen allein bieten keinen Schutz vor Cyberangriffen. In der Sicherheitsarchitektur von Behörden muss der Mensch eine zentrale Rolle spielen, denn Mitarbeitende tragen wesentlich zu einer sicheren Lösung bei. Dieses Bewusstsein gilt es mit Schulungen und Sensibilisierungskampagnen zu stärken. Präventive Massnahmen betreffen die verschiedensten Bereiche. Das kann der Umgang mit Passwörtern und Zugangsberechtigungen sein. Es gehören aber auch Kenntnisse über aktuell relevante Gefährdungen dazu. Denn das rasche Erkennen und richtige Verhalten in Zusammenhang mit einem Cyberangriff oder einem Social-Engineering-Versuch können erheblichen Schaden verhindern.

5

Fachkräftemangel:
Cybersecurity-Partner mit Expertise
Die Risiken von Cyberangriffen sind hoch. Gleichzeitig mangelt es an gut ausgebildetem Personal. Der Security-Branche fehlen die Fachkräfte. «Wir kämpfen um knappe Ressourcen auf diesem Markt», sagt Marcel Zumbühl, CISO der Schweizerischen Post. Der Fachkräftemangel sei eine der ganz grossen Herausforderungen. Entsprechend wichtig sind Partner, die über die notwendige Cyber-Expertise verfügen.

Informationssicherheit gewinnt angesichts zunehmender Cyberangriffe an Bedeutung. Welche Massnahmen die Schweizerische Post umsetzt, erklärt **Marcel Zumbühl**.

Marcel Zumbühl ist Chief Information Security Officer (CISO) der Schweizerischen Post.

«Vertraulicher Datentransport gehört zu unserer Kernkompetenz – auch im digitalen Zeitalter»

Herr Zumbühl, wie stark bedroht ist die Post durch Cyberangriffe?

Wir registrieren 10 000 Viren pro Tag und 10 Millionen Spam-Mails im Monat. Wie alle grossen Unternehmen steht die Post im Fadenkreuz von Cyberkriminellen. Aktiv attackiert werden wir rund 100-mal monatlich.

Wie stellt die Post die Cyber Security sicher?

Bei uns sind etwa 80 Security-Spezialistinnen und -Spezialisten beschäftigt, von 1200 IT-Fachkräften insgesamt. Sie stellen die Sicherheitsüberwachung aus mehreren Cyber Security Centers heraus sicher – rund um die Uhr, an sieben Tagen die Woche. Dabei setzen wir auf partizipative Sicherheit.

Was bedeutet partizipative Sicherheit?

Der partizipative Ansatz definiert Sicherheit als Kette. Diese Kette besteht aus allen Beteiligten – Mitarbeitende, Kundinnen und Kunden sowie Lieferanten. Sie tauschen sich regelmässig in verschiedenen Communities aus und stärken so gemeinsam die Cyber Security. Zudem setzen wir auf «Bug Bounty».

«Bug Bounty» – was heisst das?

Ethische Hackerinnen und Hacker können uns angreifen und werden finanziell entschädigt, wenn sie uns einen Bug, also eine Schwachstelle, melden. Auch simulieren wir laufend künstliche Angriffe und unterziehen unsere Produkte jährlich rund 100 gezielten Tests. Das zeigt: Cyber Security ist ein Prozess, der nie stillsteht. Die Post bietet auch Behördendienstleistungen im Bereich der geschützten Übermittlung von sensiblen Daten an, Beispiel E-Voting.

Warum ist die Post eine vertrauensvolle Partnerin?

Der vertrauliche und sichere Transport von sensiblen, schützenswerten Daten gehört zur DNA der Post – das bleibt auch im digitalen Zeitalter so. Dabei bieten wir unseren Kundinnen und Kunden Transparenz. Beim E-Voting zum Beispiel haben wir den Code zum Download veröffentlicht. Damit ermöglichen wir die erwähnte «partizipative Sicherheit», die eine stetige Verbesserung des Systems ermöglicht. Das E-Voting-System gewährleistet den Schutz der Daten zudem mit modernsten kryptografischen Verfahren.

Welche Security-Themen der Zukunft beschäftigen Sie derzeit?

Heute schützen wir Daten, morgen Algorithmen. Deshalb befassen wir uns intensiv damit, wie sich künstliche Intelligenz schützen lässt. Auch bereiten wir uns auf Quantencomputer vor. Diese werden Verschlüsselungsverfahren sehr viel schneller brechen können als konventionelle Computer. Als Drittes forschen wir im Bereich Smart City. Als zweitgrösstes Personentransportunternehmen der Schweiz wollen wir natürlich bereit sein, wenn sich Verkehrsmittel wie beispielsweise Postautos mit der Infrastruktur vernetzen können.

Massnahmen zur Erhöhung der Cybersicherheit

Bei Digitalisierungsprojekten gilt es grundlegende Sicherheitsaspekte zu beachten. Die Schweizerische Post gehört zusammen mit der Swisscom, Microsoft und anderen Unternehmen zur Trägerschaft der Swiss Cyber Defense DNA. Diese empfiehlt in ihrem Leitfaden sechs Massnahmen auf den Ebenen Organisation und Technologie:

1 Massnahme: Aktuelle unveränderbare Datensicherung / schreibgeschütztes Backup

- Eine Person für die Umsetzung und Überprüfung definieren
- Externe Speicherung des Backups sicherstellen

- Automatisierter, schreibgeschützter Back-up-Prozess inkl. Verschlüsselung
- Wenn nicht möglich: Backup-Medium vom Netzwerk trennen und offline lagern

2 Massnahme: Umfassender und aktueller Schutz vor Schadsoftware

- Sensibilisierung und Schulung von Mitarbeitenden im Umgang mit E-Mails, Webseiten, Passwörtern etc.

- Umfassender, flächendeckender Malware-Schutz von Endgeräten, Servern, Cloud- und E-Mail Services
- Makroausführung einschränken; Internet- und Spamfilter installieren

3 Massnahme: Netzwerke und Fernzugriffe absichern

- Schulung der Mitarbeitenden und Lieferanten für Fernzugriff

- Netzwerke mittels Firewall in Zonen aufteilen, damit wichtige Geschäftsbereiche voneinander abgeschottet sind
- Fernzugriff mittels 2-Faktoren-Authentifizierung zusätzlich absichern (z. B. SMS Code)

4 Massnahme: Hardware und Software aktuell halten

- Eine Person definieren, die für die Verwaltung und periodische Überprüfung der Lizenzen/Updates verantwortlich ist und Lieferanten für Fernzugriff

- Gemäss Risikobeurteilung veraltete Systeme ablösen und bestehende physisch schützen (z. B. Zutritt zum Server)
- Nur aktuelle Betriebssysteme und Applikationen einsetzen

5 Massnahme: Mitarbeitende und deren Rollen

- In einem Rollenkonzept definieren, welche Rechte pro Mitarbeiterin bzw. Mitarbeiter notwendig sind
- Zugriffsrechte der Geschäftsleitung ebenfalls prüfen und einschränken

- Passwortregeln für Mitarbeitende erstellen
- Definierte Rollen mit den Zugriffsrechten koppeln und einschränken

6 Massnahme: Notfallprozesse definieren

- Notfallorganisation bestimmen, Prozesse definieren und alle Mitarbeitenden informieren
- Rollen und Abläufe regelmässig überprüfen und Datenrückführung testen

- Unabhängige Technologie nutzen, um auch im Notfall auf die Dokumente zugreifen zu können (z. B. Notfallzettel, Ordner, Cloud oder Mobile Lösung)

Informationssicherheit braucht vertrauenswürdige Partner

Die Schweizer Behörden und öffentlichen Verwaltungen treiben die Digitalisierung ihrer Dienstleistungen vorwärts. Ein Erfolgsfaktor dabei ist die Informationssicherheit. Sie bildet die Grundlage für den vertrauensvollen Datenaustausch zwischen Einwohnerinnen und Einwohnern und der öffentlichen Hand.

E-Government-Angebote müssen einfach und sicher sein, damit sie breit genutzt werden. Dies wird erreicht, wenn die Bedürfnisse der Nutzerinnen und Nutzer konsequent in den Mittelpunkt gestellt werden.

Dazu gehörten unter anderem:

Datensouveränität: Einwohnerinnen und Einwohner wissen, welche Daten erhoben und gespeichert werden, wer sie nutzt und weiterverarbeitet.

Informationssicherheit: Dank sicherer Authentifizierung können ausschliesslich berechtigte Personen auf persönliche Daten zugreifen. Für den Austausch stehen Bevölkerung und Behörden sichere Kanäle zur Verfügung.

Cyber Security: Anlagen und Systeme der Behörden sind vor folgenschweren Angriffen geschützt und werden regelmässig auf Cyberangriffe überwacht.

Digitale Befähigung: Dienstleistungen sind so intuitiv gestaltet, dass alle sie nutzen oder die notwendigen Kompetenzen leicht erlernen können.

Die Schweizerische Post als Partnerin

Vertrauen ist bei E-Government-Projekten ein zentraler Erfolgsfaktor. Die Post ist mit ihrem Netzwerk eine vertrauenswürdige Partnerin. Sei es für die digitale Abwicklung einzelner Prozesse, für den Schutz der gesamten digitalen Infrastruktur oder den Austausch sensibler Daten – wir verfügen über sichere, einfache und pragmatische Lösungen. Dabei setzen wir uns für eine Digitalisierung ein, die alle mitnimmt: dank intuitiven Onlineservices und Mitarbeitenden an der Front, die eine Brücke zwischen digital und analog schlagen.

Mehr erfahren
E-Government | Die Post

Immer auf dem Laufenden sein
Die Post | E-Government: Beiträge | LinkedIn