La sécurité de l’information: un facteur de succès

Des solutions sûres pour la numérisation des autorités

Le présent livre blanc expose les principaux champs d'action en matière de sécurité de l'information et propose des solutions concrètes.

Le défi de la sécurité de l'information

La numérisation occupe les autorités et les administrations publiques suisses. Outre les opportunités, les risques sont de plus en présents dans les esprits: les cyberattaques sont monnaie courante et l'échange de données numériques s'intensifie.

Des études montrent que la population suisse veut régler ses affaires administratives rapidement et simplement. Les autorités à tous les niveaux de l'État répondent à ce souhait et développent en permanence leur offre d'e-government dans le sens du «Digital First».

Cela étant, étendre l'offre en ligne s'accompagne aussi de responsabilités supplémentaires. En effet, les prestations administratives numériques doivent afficher un niveau élevé de sécurité. Les autorités sont donc tenues d'assurer une cyberprotection complète.

Les décideurs de l'administration publique sont conscients de cette responsabilité. D'après l'étude «Radar des tendances 2022 – Pistes d'action pour le secteur public», réalisée par l'entreprise de conseil PwC en collaboration avec l'Université de Saint-Gall, 99% des personnes interrogées indiquent comme «très pertinent» le renforcement de la cybersécurité et de la sécurité de l'information.

« La sécurité de l'information est dans l'ADN de la Poste. »

Marcel Zumbühl, Chief Information Security Officer de la Poste

La numérisation nécessite de la confiance

Les avantages de l'e-government sont évidents: les autorités bénéficient d'une plus grande efficacité des processus et les utilisateurs d'une plus grande flexibilité. Mais en parallèle, il existe des inquiétudes quant à la protection des données.

En principe, la population suisse a une grande confiance dans les autorités concernant le traitement de données confidentielles. Dans l'étude «La protection des données en Suisse» de la Haute école zurichoise de sciences appliquées (ZHAW), 74% des personnes interrogées sont plutôt ou totalement d'accord avec l'affirmation selon laquelle les autorités traitent les données personnelles de manière appropriée et confidentielle. Ce pourcentage d'approbation élevé constitue une bonne base pour répondre aux préoccupations concernant la protection des données lors de l'utilisation des canaux numériques.

La protection des données règle le droit de chaque personne de décider de l'utilisation et de la communication de ses données personnelles. La protection des données vise à protéger la vie privée et à empêcher l'utilisation abusive des données par des tiers. La loi fédérale sur la protection des données fixe la façon dont les données sont collectées, traitées, utilisées ou stockées. Pour satisfaire à l'ensemble des exigences légales en matière de protection des données dans les services d'e-government, la sécurité de l'information est primordiale. Elle comprend des mesures et des technologies visant à empêcher l'utilisation abusive, la falsification et la perte de données, et à garantir la confidentialité.

La protection des données et la sécurité de l'information sont des éléments clés pour renforcer l'adoption des solutions numériques et la confiance dans l'e-government. Un constat qui vaut aussi bien pour la population que pour les autorités. Face à la vulnérabilité croissante des données aux cyberattaques, la sécurité de l'information doit être une priorité absolue. Cela permet d'instaurer la confiance dans les offres numériques.

Informations complémentaires sur la LPD:
https://digital-solutions.post.ch/fr/protection-des-donnees-incamail

« Cinq défis en lien avec la sécurité de l'information. »

Marcel Zumbühl, Chief Information Security Officer (CISO) de la Poste

Cinq défis en lien avec la sécurité de l'information

Les autorités ont besoin de procédures sécurisées pour l'identification, la transmission et le stockage des données afin de renforcer leur cybersécurité et la sécurité de l'information. Dans ce cadre, elles doivent se consacrer aux cinq défis suivants:

1

Nouvelle loi fédérale sur la protection des données: des exigences de compliance plus strictes

La nouvelle LPD suisse entrera en vigueur le 1er septembre 2023. Des règles plus strictes s'appliqueront ainsi au traitement des données personnelles.

La sécurité de l'information est une exigence centrale de la LPD. Pour une mise en œuvre conforme à la loi, il est nécessaire de dresser un état des lieux du traitement des données personnelles et de procéder à une évaluation des risques afin de déterminer les exigences en matière de conformité à la protection des données.

Il faut en outre sensibiliser les collaborateurs et développer un concept de sécurité informatique qui offre une protection suffisante contre les logiciels malveillants, le vol ou la perte de données.

2

Menaces actuelles: gestion globale des risques

Les cyberattaques sont monnaie courante. En moyenne, il s'écoule 100 jours avant que l'incident se déclare. Depuis le début de l'année, le Centre national pour la cybersécurité (NCSC) a reçu 10 000 signalements (état à la fin du mois d'avril).

Les menaces se sont considérablement aggravées et les pirates redoublent d'ingéniosité: Ransomware as a Service (RaaS), attaques de chaîne d'approvisionnement, tactiques de social engineering comptent, selon les informations du NCSC, parmi les dangers les plus fréquents actuellement.

La forte dynamique de croissance de ces risques nécessite une gestion des risques globale. Afin de tenir le rythme de l'évolution des menaces, des mises à jour régulières du matériel comme des logiciels sont indispensables.

3

Télétravail:
la sécurité de l'information à la maison également
Les modèles de travail hybride ont aussi gagné les administrations publiques. Cela s'accompagne d'un risque accru concernant le traitement des données dont certaines sont sensibles. En effet, les données sont davantage fragmentées, ce qui multiplie le nombre de failles. C'est pourquoi il faut des solutions pour protéger efficacement les données également dans les environnements informatiques en télétravail.

4

Améliorer la prise de conscience:
former et sensibiliser les collaborateurs
Seules, les mesures techniques n'offrent pas de protection contre les cyberattaques. L'humain doit jouer un rôle central dans l'architecture de sécurité des autorités. En effet, les collaborateurs sont cruciaux pour assurer la sécurité de la solution. Il faut renforcer cette prise de conscience par des formations et des campagnes de sensibilisation. Les mesures préventives concernent des secteurs extrêmement variés. Cela peut par exemple être la gestion des mots de passe et des droits d'accès. Mais il faut assortir cela de la connaissance des dangers actuels. En effet, identifier rapidement une cyberattaque ou une tentative de social engineering et adopter le bon comportement permet d'éviter des dommages considérables.

5

Pénurie de main-d'œuvre spécialisée:
des partenaires experts en cybersécurité
Les risques de cyberattaque sont élevés. En parallèle, il existe une pénurie de personnel suffisamment formé. Le personnel fait défaut dans le secteur de sécurité. «C'est un marché où nous luttons pour acquérir des ressources qui sont rares», indique Marcel Zumbühl, CISO de la Poste. La pénurie de main-d'œuvre qualifiée est l'un des plus grands défis à relever. Les partenaires qui disposent de la cyber-expertise nécessaire sont donc d'autant plus importants.

Eu égard à la multiplications des cyber-attaques, la sécurité de l'information gagne en importance. **Marcel Zumbühl** nous explique quelles mesures déploie le géant jaune.

Marcel Zumbühl est Chief Information Security Officer de la Poste.

«Le transport confidentiel de données fait partie de nos compétences clés, à l'ère numérique également»

M. Zumbühl, dans quelle mesure la Poste est-elle exposée aux cyberattaques?

Chaque jour, nous recensons 10 000 virus, et 10 millions de pourriels par mois. Comme toutes les grandes entreprises, la Poste est dans le collimateur des cybercriminels. Nous sommes attaqués de manière active environ 100 fois par mois.

Qui assure la cybersécurité de la Poste?

Nous employons quelque 80 spécialistes de la sécurité, sur 1200 membres du personnel IT. Ils assurent la surveillance depuis plusieurs centres de cybersécurité, 7 jours sur 7, 24 heures sur 24. Dans ce cadre, nous misons sur la sécurité participative.

Qu'est-ce que cela signifie?

L'approche participative définit la sécurité comme une chaîne, composée de tous les acteurs – personnel, clientèle et fournisseurs. Ils échangent régulièrement au sein de différentes communautés et renforcent ainsi ensemble la cybersécurité. De plus, nous nous appuyons sur le «bug bounty».

«Bug bounty» – qu'est-ce que c'est concrètement?

Les pirates éthiques peuvent nous attaquer et sont rétribués financièrement s'ils nous signalent un bug, c'est-à-dire une faille. Nous simulons également en permanence des attaques artificielles et soumettons nos produits à une centaine de tests ciblés chaque année. Cela montre que la cybersécurité est un processus qui ne s'arrête jamais. La Poste propose également des prestations pour les autorités dans le domaine de la transmission protégée de données sensibles, par exemple le vote électronique.

Pourquoi la Poste est-elle un partenaire fiable?

Le transport sécurisé et en toute confidentialité de données sensibles est inscrit dans l'ADN de la Poste, et l'ère numérique n'y change rien. Dans ce cadre, nous sommes transparents à 100% vis-à-vis de notre clientèle. Concernant le vote électronique, par exemple, nous avons publié le code sous forme téléchargeable. Nous rendons ainsi possible la «sécurité participative» mentionnée plus haut, qui permet une amélioration constante du système. Le système de vote électronique garantit en outre la protection des données grâce à des procédés cryptographiques de pointe.

Quels sont les thèmes de sécurité du futur sur lesquels vous travaillez actuellement?

Aujourd'hui, nous protégeons des données, demain, des algorithmes. C'est pourquoi nous nous intéressons de près à la manière dont protéger l'intelligence artificielle. Nous nous préparons également à l'informatique quantique. Les ordinateurs de cette génération pourront déjouer les procédures de cryptage beaucoup plus rapidement que les conventionnels. Troisièmement, nous menons des recherches dans le domaine de la ville intelligente. En tant que deuxième plus grande entreprise de transport de personnes en Suisse, nous voulons bien sûr être prêts lorsque les moyens de transport, comme les cars postaux par exemple, pourront se connecter à l'infrastructure.

Mesures de renforcement de la cybersécurité

Les projets de numérisation doivent tenir compte d'aspects fondamentaux en matière de sécurité. La Poste fait partie, avec Swisscom, Microsoft et d'autres entreprises, de l'organisme responsable de Swiss Cyber Defence DNA. Dans son guide, ce groupement recommande six mesures aux niveaux organisationnel et technologique:

1 Sauvegarde actualisée et non modifiable des données / Sauvegarde en lecture seule

- Désigner une personne pour la mise en œuvre et le contrôle
- Assurer le stockage externe de la sauvegarde

- Processus de sauvegarde automatisé en lecture seule, chiffrage compris
- Si ce n'est pas possible, déconnecter le support de sauvegarde du réseau et le stocker hors ligne

2 Protection complète et actualisée contre les logiciels malveillants

- Sensibilisation et formation des collaborateurs à l'utilisation de la messagerie électronique, des sites web, mots de passe, etc.

- Protection complète des terminaux, serveurs, services cloud et messagerie électronique contre les logiciels malveillants dans l'entreprise
- Restreindre l'exécution de macros; installer des filtres Internet et antispam

3 Réseaux et accès à distance sécurisés

- Formation des collaborateurs et des fournisseurs en matière d'accès à distance

- Fragmenter les réseaux en plusieurs zones au moyen de pare-feux, afin de séparer les domaines d'activités critiques
- Augmenter encore la sécurité de l'accès à distance via une authentification à deux facteurs (code SMS par ex.)

4 Mises à jour du matériel et des logiciels

- Désigner une personne responsable de l'administration et du contrôle périodique des licences/mises à jour, et des fournisseurs pour l'accès à distance

- Remplacer les systèmes obsolètes en fonction de l'évaluation des risques et protéger physiquement les systèmes existants (par ex. accès au serveur)
- N'utiliser que des systèmes d'exploitation et applications à jour

5 Collaborateurs et rôles respectifs

- Définir dans un concept de rôles les droits nécessaires à chaque membre du personnel
- Vérifier et limiter également les droits d'accès de la direction

- Définir des règles relatives aux mots de passe pour les collaborateurs
- Associer et restreindre les rôles définis aux droits d'accès

6 Définir les procédures d'urgence

- Déterminer l'organisation d'urgence, définir les processus et informer tous les collaborateurs
- Vérifier régulièrement les rôles et les processus, tester la restauration des données

- Utiliser une technologie indépendante pour accéder aux documents en cas d'urgence (liste avec informations utiles, répertoire, solution cloud ou mobile, etc.)

Des partenaires dignes de confiance sont une clé de la sécurité de l'information

Les autorités et les administrations publiques suisses font progresser la numérisation de leurs services. La sécurité de l'information est un facteur de succès à cet égard. Elle constitue la base d'un échange de données en toute confiance entre la population et les pouvoirs publics.

Les offres d'e-government doivent être simples et sûres afin d'assurer une large utilisation. Pour parvenir à cet objectif, il faut que les besoins des utilisateurs soient systématiquement placés au centre du développement.

En voici quelques-uns:

Souveraineté des données: la population sait quelles données sont collectées et enregistrées, qui les utilise et les traite par la suite.

Sécurité de l'information: grâce à une authentification forte, seules les personnes autorisées peuvent accéder aux données personnelles. Des canaux sécurisés pour les échanges entre la population et les autorités existent.

Cybersécurité: les installations et systèmes des autorités sont protégés des attaques aux conséquences graves et font l'objet d'une surveillance régulière des cyberattaques.

Facilitation numérique: les services sont conçus de manière si intuitive que tout un chacun peut les utiliser ou acquérir facilement les compétences nécessaires à leur utilisation.

La Poste, votre partenaire

La confiance est un facteur clé de la réussite des projets d'e-government. Avec son réseau, la Poste est un partenaire fiable. Que ce soit pour le traitement numérique de processus individuels, pour la protection de l'ensemble de l'infrastructure numérique, pour l'échange sécurisé de données sensibles, nous disposons de solutions numériques simples et pratiques. Dans ce cadre, nous nous engageons pour une numérisation qui profite à toutes et à tous: grâce à des services en ligne intuitifs et à du personnel de première ligne qui fait le lien entre l'analogique et le numérique.

En savoir plus
E-government | La Poste

Être toujours à la page
La Poste | E-Government: Posts | LinkedIn