La sicurezza delle informazioni come fattore di successo

Soluzioni sicure per la digitalizzazione dei servizi amministrativi

Questo white paper individua i principali settori d'intervento sul fronte della sicurezza delle informazioni e presenta possibili soluzioni concrete.

La sfida della sicurezza delle informazioni

Man mano che le autorità svizzere e le amministrazioni pubbliche promuovono la digitalizzazione, aumenta sempre più la consapevolezza non solo delle opportunità, ma anche dei rischi che questa comporta: gli attacchi informatici sono all'ordine del giorno e allo stesso tempo lo scambio di dati si intensifica.

Gli studi dimostrano che le cittadine e i cittadini svizzeri vogliono sbrigare le questioni amministrative in modo rapido e semplice. Per soddisfare quest'esigenza, le autorità a tutti i livelli statali stanno ampliando costantemente la loro offerta e-government secondo il principio «digital first».

L'ampliamento dell'offerta online si accompagna tuttavia a responsabilità ulteriori, poiché le prestazioni amministrative digitali devono garantire la massima sicurezza. Le autorità hanno dunque il dovere di provvedere a una protezione informatica completa.

Chi prende le decisioni nell'amministrazione pubblica è consapevole di tale responsabilità. In base a uno studio della società di consulenza PwC e dell'Università di San Gallo sulle tendenze 2022 negli approcci operativi dell'amministrazione pubblica («Trendradar 2022: Handlungsansätze für die öffentliche Verwaltung»), il 99% delle persone intervistate reputa «molto rilevante» il rafforzamento della sicurezza cibernetica e delle informazioni.

« La sicurezza delle informazioni è nel DNA della Posta. »

Marcel Zumbühl, Chief Information Security Officer della Posta

La digitalizzazione richiede fiducia

I vantaggi dell'e-government sono evidenti: le autorità beneficiano di una maggiore efficienza dei processi, l'utenza di una maggiore flessibilità. Non mancano però i timori per la protezione dei dati.

In linea di massima le cittadine e i cittadini svizzeri hanno fiducia nel fatto che le autorità gestiscano i loro dati sensibili con la dovuta confidenzialità. In uno studio condotto sulla protezione dei dati in Svizzera dall'Università di Scienze applicate di Zurigo («Datenschutz in der Schweiz»), il 74% delle persone intervistate si è detto abbastanza o pienamente d'accordo con l'affermazione secondo cui le autorità gestiscono i dati personali in maniera corretta e confidenziale. Questo consenso elevato rappresenta una buona base per mettere da parte i timori per la protezione dei dati nell'utilizzo dei canali digitali.

La protezione dei dati disciplina il diritto di ogni individuo a decidere in merito all'utilizzo e alla trasmissione dei propri dati personali. Il suo intento è quello di proteggere la sfera privata e impedire l'uso improprio dei dati da parte di terzi, pertanto stabilisce il modo in cui i dati possono essere rilevati, elaborati, utilizzati o conservati. La sicurezza delle informazioni riveste un'importanza fondamentale per il soddisfacimento di tutti i requisiti giuridici sulla protezione dei dati nei servizi e-government. Essa comprende le misure e le tecnologie per la prevenzione degli abusi, delle falsificazioni e della perdita di dati, e garantisce la riservatezza.

La protezione dei dati e la sicurezza delle informazioni sono elementi cruciali per aumentare l'accettazione delle soluzioni digitali e rafforzare la fiducia nell'e-government, non solo tra la popolazione ma anche all'interno delle istituzioni. Anche a causa del crescente pericolo di attacchi informatici a cui sono esposti i dati, la sicurezza delle informazioni deve considerata della massima priorità. Questo creerà fiducia nelle offerte digitali.

Per ulteriori informazioni sulla nuova LPD:
https://digital-solutions.post.ch/it/protezione-dei-dati-incamail

« Conoscere i rischi che si corrono è fondamentale nella cibersicurezza. »

Marcel Zumbühl, Chief Information Security Officer della Posta

Cinque sfide legate alla sicurezza delle informazioni

Le autorità hanno bisogno di procedure sicure per l'identificazione, la trasmissione e la conservazione dei dati, al fine di rafforzare la loro sicurezza cibernetica e delle informazioni. La loro attenzione dovrebbe perciò concentrarsi sulle cinque sfide seguenti:

1

Nuova Legge sulla protezione dei dati: requisiti di conformità più severi

Il 1º settembre 2023 entra in vigore la nuova Legge federale sulla protezione dei dati, insieme a norme più severe per il trattamento dei dati personali.

Una disposizione fondamentale per la protezione dei dati nella LPD riguarda la sicurezza delle informazioni. Per un'attuazione conforme alla legge è necessario svolgere una valutazione del rischio e fare il punto della situazione sul trattamento di dati personali, così da determinare i requisiti di conformità in materia di protezione dei dati.

Altrettanto importante è sensibilizzare il personale e sviluppare un piano di sicurezza informatica che protegga a sufficienza dai software dannosi, dal furto o dalla perdita di dati.

2

Attuali minacce per la sicurezza: una gestione del rischio globale

Gli attacchi informatici sono ormai all'ordine del giorno. In media viene registrato un caso ogni 100 giorni. Dall'inizio dell'anno il Centro nazionale per la cibersicurezza (NCSC) ha ricevuto 10 000 segnalazioni (dati di fine aprile).

La situazione di pericolo si è fortemente inasprita e chi perpetra gli attacchi lo fa in modo sempre più raffinato: secondo i dati dell'NCSC le minacce più frequenti attualmente arrivano sotto forma di Ransomware as a Service (RaaS), attacchi alla supply chain o nuove tattiche di social engineering.

L'elevato dinamismo dei pericoli informatici richiede una gestione del rischio globale. Per rimanere al passo con lo sviluppo è indispensabile aggiornare regolarmente hardware e software.

3

Lavoro da remoto: sicurezza delle informazioni anche in modalità home office

Poiché anche presso le autorità pubbliche si sono affermate modalità di lavoro ibride, il trattamento dei dati, sensibili e non, comporta rischi maggiori. Se i dati infatti sono maggiormente frammentati, le lacune nella sicurezza aumentano. Per questo servono soluzioni per proteggere efficacemente i dati anche negli ambienti dell'home office.

4

Creare consapevolezza: formazione e sensibilizzazione del personale

Le misure tecnologiche da sole non bastano a proteggere dagli attacchi informatici. Nell'architettura di sicurezza delle autorità, l'individuo deve ricoprire un ruolo da protagonista, poiché il personale contribuisce in misura fondamentale alla sicurezza di una soluzione. Questa consapevolezza va rafforzata mediante sessioni di formazione e campagne di sensibilizzazione. Le misure preventive interessano i campi più svariati: si passa dalla gestione delle password e delle autorizzazioni di accesso alle conoscenze sui pericoli più rilevanti nell'attualità. Perché riconoscere rapidamente un attacco informatico o un tentativo di social engineering e comportarsi nel modo giusto al riguardo può prevenire danni considerevoli.

5

Mancanza di forza lavoro specializzata: partner di cibersicurezza competenti

Il rischio di attacchi informatici è elevato e al contempo manca personale adeguatamente formato. Il ramo della sicurezza sta sperimentando una carenza di figure specializzate. «Su questo mercato ci contendiamo risorse già scarse», afferma Marcel Zumbühl, CISO della Posta, secondo il quale la carenza di personale specializzato è una delle principali sfide da affrontare. Per questo è importante farsi affiancare da partner che dispongano delle competenze informatiche necessarie.

Alla luce dell'incremento degli attacchi informatici, la sicurezza delle informazioni acquista sempre più importanza. **Marcel Zumbühl** spiega quali misure adotta l'azienda al riguardo.

Marcel Zumbühl è Chief Information Security Officer (CISO) della Posta.

«Il trasferimento di dati confidenziali è una delle nostre competenze chiave, anche nell'era digitale»

Signor Zumbühl, quanto è forte la minaccia di attacchi informatici per la Posta?

Registriamo 10 000 virus al giorno e 10 milioni di e-mail di spam al mese. Come tutte le altre grandi aziende, la Posta è nel mirino dei criminali informatici. Veniamo attaccati attivamente circa 100 volte al mese.

Come viene garantita la sicurezza informatica dalla Posta?

Su un totale di 1200 specialisti IT impieghiamo circa 80 specialisti della sicurezza, che assicurano la sorveglianza 24 ore su 24, 7 giorni su 7, da diversi centri di cibersicurezza. Puntiamo quindi sulla sicurezza partecipativa.

Cosa si intende con sicurezza partecipativa?

Secondo l'approccio partecipativo, la sicurezza è come una catena i cui anelli sono rappresentati da tutte le parti coinvolte: il personale, la clientela e i fornitori. Mantenendo scambi regolari sulle diverse community, queste parti rafforzano collettivamente la cibersicurezza. Un'altra misura a cui ricorriamo è il «bug bounty».

Che cosa significa «bug bounty»?

Lasciamo che gli hacker etici ci attacchino e diamo loro un compenso quando scoprono un bug, cioè una lacuna nella sicurezza. Inoltre, simuliamo costantemente attacchi con l'intelligenza artificiale e sottoponiamo ogni anno i nostri prodotti a un centinaio di test mirati. È evidente che cibersicurezza significa non stare mai fermi. La Posta offre anche prestazioni amministrative nel campo della trasmissione protetta di dati sensibili, come nel caso del voto elettronico.

Cosa fa della Posta un partner affidabile?

La trasmissione confidenziale e sicura di dati sensibili, che richiedono una particolare protezione, è nel DNA della Posta. Ed è così anche nell'era digitale. Alla nostra clientela offriamo trasparenza; per esempio, nel caso del voto elettronico abbiamo messo a disposizione il codice da scaricare, così da consentire la sicurezza partecipativa di cui parlavo e apportare continui miglioramenti al sistema. Inoltre, il sistema di voto elettronico garantisce la protezione dei dati attraverso le più moderne procedure crittografiche.

Di quali tematiche legate alla sicurezza si sta occupando al momento?

Oggi proteggiamo i dati, domani proteggeremo gli algoritmi. Per questo stiamo lavorando sodo per capire come è possibile difendere l'intelligenza artificiale. Ci stiamo occupando anche di computer quantistici, che saranno in grado di infrangere le procedure crittografiche molto più rapidamente rispetto ai computer convenzionali. In terzo luogo stiamo conducendo ricerche sulle smart city. Come seconda azienda di trasporto di persone della Svizzera, naturalmente vogliamo arrivare pronti al momento in cui i mezzi di trasporto, come gli autopostali, potranno essere interconnessi all'infrastruttura.

Misure per il rafforzamento della cibersicurezza

Nei progetti di digitalizzazione ci sono aspetti di sicurezza fondamentali di cui tenere conto. Insieme a Swisscom, Microsoft e altre aziende, la Posta è ente promotore dell'iniziativa Swiss Cyber Defense DNA, le cui linee guida racchiudono sei misure raccomandate sul piano organizzativo e tecnologico:

1 Protezione dei dati aggiornata e non modificabile / backup in sola lettura

- Definire una persona responsabile dell'attuazione e della verifica
- Assicurare il salvataggio esterno del backup

- Processo di backup automatizzato e in sola lettura, cifratura inclusa
- Se quanto sopra non è possibile: separare il medium di backup dalla rete ed effettuare il salvataggio offline

2 Protezione globale e aggiornata dai software dannosi

- Sensibilizzare e formare il personale nella gestione di e-mail, siti web, password ecc.

- Proteggere in modo globale e capillare dai malware apparecchi terminali, server, servizi cloud e e-mail
- Limitare l'esecuzione delle macro; installare filtri internet e antispam

3 Proteggere le reti e gli accessi da remoto

- Formare il personale e i fornitori per l'accesso da remoto

- Suddividere le reti in zone mediante il firewall, in modo da isolare importanti settori aziendali
- Proteggere ulteriormente l'accesso da remoto mediante l'autenticazione a due fattori (ad es. codice SMS)

4 Mantenere sempre aggiornati hardware e software

- Definire una persona responsabile per la gestione e la verifica periodica delle licenze / degli aggiornamenti e fornitori per l'accesso da remoto

- Sostituire i sistemi obsoleti conformemente all'analisi dei rischi e proteggere fisicamente i sistemi attuali (ad es. accesso al server)
- Utilizzare soltanto applicazioni e sistemi operativi aggiornati

5 Collaboratrici e collaboratori e i rispettivi ruoli

- Definire in un piano dei ruoli le autorizzazioni necessarie a ogni collaboratrice e collaboratore
- Verificare e delimitare anche i diritti d'accesso della direzione

- Stabilire le regole relative alle password per collaboratrici e collaboratori
- Abbinare i ruoli definiti con i diritti d'accesso e delimitarli

6 Definire i processi d'emergenza

- Stabilire un'organizzazione d'emergenza e i relativi processi; informare tutto il personale
- Verificare regolarmente ruoli e processi e testare il feedback dei dati

- Utilizzare tecnologie indipendenti, per poter accedere ai documenti anche nei casi d'emergenza (ad es. istruzioni in caso d'emergenza, cartelle, cloud o soluzione mobile)

La sicurezza delle informazioni richiede partner affidabili

Le autorità svizzere e le amministrazioni pubbliche promuovono la digitalizzazione dei loro servizi e la sicurezza delle informazioni è un fattore determinante per il successo dell'operazione, in quanto costituisce la base per uno scambio di dati affidabile tra la popolazione e la pubblica amministrazione.

Perché possano godere di ampio utilizzo, le offerte di e-government devono essere semplici e sicure. Ciò è possibile se le esigenze dell'utenza vengono messe coerentemente al centro dell'attenzione.

Tra le altre cose, questo significa:

Sovranità dei dati: cittadine e cittadini sanno quali dati vengono rilevati e memorizzati, chi li utilizza e chi ne esegue il trattamento successivo.

Sicurezza delle informazioni: grazie all'autenticazione sicura possono accedere ai dati soltanto le persone aventi diritto. La popolazione e le autorità hanno a disposizione canali sicuri per lo scambio di dati.

Cibersicurezza: gli impianti e i sistemi delle autorità sono sorvegliati costantemente e protetti da attacchi informatici dalle conseguenze gravi.

Promozione delle competenze digitali: i servizi sono configurati in modo così intuitivo da consentire a chiunque di utilizzarli o di acquisire facilmente le competenze necessarie.

La Posta in veste di partner

La fiducia è un fattore di successo chiave nell'ambito dei progetti di e-government. Grazie alla sua rete, la Posta è un partner affidabile. Che si tratti della gestione digitale di singoli processi, della protezione dell'intera infrastruttura digitale o dello scambio di dati sensibili, disponiamo di soluzioni semplici, sicure e pragmatiche. Promuoviamo con convinzione una digitalizzazione che coinvolga tutti, creando un ponte tra la dimensione analogica e quella digitale grazie a servizi online intuitivi e al nostro personale in prima linea.

Scoprire di più
E-Government | La Posta

Restare sempre al passo con le novità
La Posta | Contributi a tema e-government LinkedIn