Prevenire la cybercriminalità

Guida per i Comuni

Indice

Liste di controllo

1 Cosa ha a che fare la criminalità informatica con il vostro Comune

Maggior vicinanza al cittadino, miglior promozione del turismo e dell'economia, servizi rapidi multimediali: la digitalizzazione offre ai Comuni molte nuove opportunità. Allo stesso tempo per funzionare vengono richiesti nuovi processi che portano ad una maggior dipendenza da una tecnologia dell'informazione e della comunicazione (TIC) e dalle imprese di servizio ad essa associate. I criminali approfittano proprio di queste interconnessioni e dipendenze.

Nel suo rapporto sulla situazione nel 2019[1], il Servizio delle attività informative della Confederazione constata che anche l'Amministrazione pubblica è nel mirino degli attacchi informatici. Dall'amministrazione comunale all'approvvigionamento elettrico – nessuno è al sicuro. Può ad esempio essere oscurato il sito web, ma anche essere colpita l'intera rete. Oltre ai danni finanziari che ne scaturiscono, in alcuni casi dati sensibili finiscono nelle mani sbagliate. Con gravissime conseguenze come ad esempio: perdita di dati, blocco dei sistemi, richieste di risarcimento per responsabilità civile a causa di una violazione della protezione dei dati o danni alla reputazione.

Gli attacchi informatici possono danneggiare in modo permanente la fiducia della popolazione nell'amministrazione.

Con il presente materiale informativo forniamo ai Comuni di piccole e medie dimensioni delle raccomandazioni concrete per proteggersi dalla cybercriminalità e illustriamo come reagire dopo un attacco. In tal modo intendiamo inoltre fornire un contributo all'attuazione delle misure iscritte nella «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018-2022», che mira a garantire la protezione della Svizzera dai minacce cibernetiche intesa come compito comune a tutti i livelli statali e agli altri partner.[2]

Desideriamo inoltre incoraggiarvi a segnalare alla Polizia i casi rilevanti. Soltanto attraverso la collaborazione fra le autorità di perseguimento penale e le persone prese di mira, si possono scoprire e condannare i colpevoli e combattere così la cybercriminalità in modo duraturo.

1 Servizio delle attività informative della Confederazione (2019). La Sicurezza della Svizzera 2019. Rapporto sulla situazione del Servizio delle attività informative della Confederazione. www.vbs.admin.ch

2 Consiglio federale (2018). Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018-2022 www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html

2 Come possono i criminali arrecare danni al vostro Comune

Con la minaccia ai Comuni di pubblicare dati sensibili o di paralizzare i servizi, in particolare nel settore della sicurezza dell'approvvigionamento, i criminali informatici ricattano e derubano i Comuni.

2.1 Metodi utilizzati dai truffatori

Attraverso l'inganno, gli autori dei reati riescono ad indurre la persona presa di mira a compiere una determinata azione contro la sua volontà. Nella maggior parte dei casi si tratta di indurre l'obbiettivo ad aprire l'allegato di una email, cliccare su di un link, comunicare dati personali come ad esempio una password od effettuare un versamento.

Uno dei metodi comunemente utilizzati si chiama social engineering. In genere gli autori dei reati si informano anticipatamente sulla struttura dell'amministrazione, dell'organizzazione o dell'impresa. Ciò avviene attraverso la consultazione d'informazioni liberamente accessibili, per esempio sul sito dell'amministrazione comunale o sui social network. Dopodiché prendono di mira una persona idonea e la coinvolgono in uno scenario creato appositamente. Cercano per esempio di procurarsi il nome utente e la password, facendosi passare al telefono per un collaboratore di un'impresa di software. Con il pretesto dell'esistenza di gravi problemi informatici o facendo credere di essere in possesso di determinate informazioni sull'azienda, i criminali disorientano la vittima, rendendola sempre più insicura, finché comunica le informazioni richieste. Nelle loro email o telefonate, i criminali a volte utilizzano in modo abusivo anche i nomi di unità amministrative, ad esempio l'Amministrazione delle contribuzioni, o di aziende elettriche.

Modalità di manipolazione	
Gerarchia	I truffatori si servono della struttura gerarchica dell'organizzazione e creano una certa pressione ad agire. Di solito simulano un'altra identità e a nome di un superiore esortano un collaboratore a comunicargli informazioni sensibili o a effettuare un pagamento.
Urgenza	Alle vittime viene fatto credere di dover agire sotto forte pressione di tempo.
Avidità/curiosità	Alla vittima viene promessa una vincita o una sorpresa se apre il file o clicca sul link inviato.
Paura/collera	Si minacciano ripercussioni, se non si dà seguito alla richiesta. Oppure si rilasciano dichiarazioni manifestamente false, che possono essere corrette cliccando sul link malevolo.
Partecipazione	L'argomento presentato coinvolge la vittima sul piano emotivo, esortandola ad esempio ad agire per eliminare delle ingiustizie.

2.2 Varianti di ricatto e furto

I criminali si procurano l'accesso alla rete del comune attraverso i dati di accesso sottratti, malware o sistemi protetti in modo insufficiente. Se i criminali trovano dati preziosi, li criptano o minacciano di renderli pubblici o di cancellarli se non viene pagato il riscatto. A volte i dati vengono copiati o venduti a terzi oppure utilizzati per effettuare pagamenti tramite e-banking.

Metodi frequenti

Ransomware	Si inviano in massa file nocivi, per esempio via email. Le potenziali vittime individuate con questo metodo vengono poi spiate in modo mirato per raccogliere informazioni. Se i truffatori hanno successo, assumono il controllo e iniziano a cifrare i dati. In certi casi i dati vengono anche sottratti. Gli autori esigono il pagamento di un riscatto (ransom) per decodificare/recuperare i dati.
Trojan nell'e-banking	Oltre al ricatto, i cybercriminali puntano spesso sulla manipolazione di ordini di pagamento. A questo scopo si servono di cosiddetti trojan e-banking. Si tratta di programmi che permettono all'autore di accedere al conto e-banking della vittima. Spesso i trojan sono inviati per email (p.es. camuffati da fattura o da candidatura).
Phishing	Alle potenziali vittime viene comunicato per email, sito web, telefonia via Internet o SMS che determinati dati di accesso non sono più sicuri o non sono aggiornati. Nel contempo vengono invitate a modificarli seguendo il link inviato, il quale, tuttavia, porta ad un sito web contraffatto. Se la vittima accede al sito web inserendo le proprie credenziali, i truffatori ottengono i dati di accesso, p.es. le indicazioni relative a carte di credito o password per l'email o per un altro account.
DDoS (attacco per sovraccarico)	DDoS significa Distributed Denial of Services. Con un attacco di questo tipo i servizi, p.es. il sito Internet, il servizio email o l'impianto di telefonia digitale sono inondati da un enorme numero di richieste. Questo sovraccarico manda in tilt i sistemi e l'amministrazione o l'impresa, che non possono più adempiere ai propri compiti. Per sospendere gli attacchi è richiesto il pagamento di un riscatto. I criminali usano gli attacchi DDoS in parte anche per distogliere l'attenzione dall'attacco digitale vero e proprio eseguito con dati di accesso rubati in precedenza.
Remote Access (accesso remoto)	L'accesso remoto serve ad accedere a un computer o ad una rete dall'esterno, per esempio in home office oppure permettendo a collaboratori del supporto di effettuare operazioni di manutenzione. I criminali si servono di questo accesso remoto anche per accedere alle reti di amministrazioni o imprese, per esempio attraverso tentativi di phishing o attacchi alle password o alle componenti di rete non protette o obsolete.

3 Come potete proteggere il vostro Comune

Per proteggersi contro gli attacchi informatici servono varie misure tecniche e organizzative. Alcune possono essere attuate autonomamente dai responsabili comunali, altre devono essere discusse con i responsabili TIC interni o esterni. Nella lista di controllo alla fine del presente documento trovate una sintesi delle misure di protezione descritte.

3.1 Misure di protezione organizzative

> **Definire le responsabilità**
Bisogna designare delle persone responsabili all'adempimento dei vari compiti legati alla sicurezza dei sistemi TIC all'interno della vostra amministrazione. Definite anche il ruolo e le responsabilità in merito all'organizzazione in caso di emergenza o di crisi, nonché le relative competenze. Le interfacce con i partner devono essere identificate preventivamente e i processi devono essere coordinati. Definite con il responsabile informatico i casi di attacco alla sicurezza sui quali volete imperativamente essere informati. Ciò vale per tutti gli eventi che interessano sia la vostra infrastruttura, sia quella del fornitore di servizi informatici e di telecomunicazione.

> **Conoscere il proprio ambiente TIC**
Documentate la vostra infrastruttura TIC in un inventario il più dettagliato possibile. Solo se conoscete la vostra infrastruttura, i vostri servizi, i computer, gli utenti, ecc., potete sapere cosa occorre proteggere e sorvegliare.

> **Prevenire**
Una buona strategia contro gli attacchi informatici viene prima dell'attacco vero e proprio: processi collaudati e percorsi di «escalation» sono indispensabili per mantenere il controllo.

Definite quali sono i log file (protocolli eventi) da salvare e per quanto tempo tenerli. Si raccomanda di farlo in una struttura centralizzata. Log file estesi aiutano a individuare l'origine dell'attacco, a ottenere informazioni relative a sistemi infetti nella propria rete e ad attuare le contromisure adeguate. Per via dell'importanza che rivestono, si raccomanda di non trascurare l'aspetto della protezione dei dati dei log file. Chiarite le questioni relative ai log file e all'identificazione degli attacchi con il responsabile TIC.

Strategia preventiva in caso di emergenza

> Concetto di comunicazione e di crisi adeguato alla dimensione del Comune e concordato con il fornitore di servizi.

> Liste di contatto (organi interni e esterni, fornitore di servizi).

> Considerazioni
  > relative alla perdita totale dell'infrastruttura TIC (recupero, riavvio dell'esercizio, perdita di dati, ecc.).
  > relative ai mezzi di comunicazione sostitutivi quando i sistemi informatici e telematici non sono più disponibili.

> Scenari di emergenza, esercitazioni e verifica della vulnerabilità dell'infrastruttura.

> **Disciplinate la gestione delle informazioni e dei dati sensibili**
Allestite un inventario dei dati e delle informazioni e definite gli elementi che necessitano di una protezione particolare. Elaborate un piano di protezione per questi elementi. In merito alle direttive cantonali e comunali sulla protezione dei dati consultate anche i siti Internet del Cantone e dell'associazione dei Comuni (v. anche 4: «Procuratevi l'aiuto necessario»).

Considerate bene quali informazioni volete pubblicare sul vostro sito web o sui social media, perché questi dati vengono raccolti dai delinquenti. Non dovrebbe figurare sul sito web in particolare il nominativo della persona responsabile delle questioni finanziarie che ha accesso all'e-banking in seno all'amministrazione. In linea di massima non si dovrebbero comunicare informazioni e dati confidenziali attraverso canali impersonali, quali telefono o email. Le informazioni confidenziali da inoltrare a esterni dovrebbero sempre essere inviate in forma cifrata o per posta.

Utilizzate con cautela i servizi cloud. Questi servizi sono usati da molti programmi. Valutate quali dati vanno salvati a livello locale e quali nel cloud. Non caricate mai nel cloud dati sensibili non cifrati. Leggete le condizioni generali (CG) dell'azienda che offre i servizi di cloud storage e prestate attenzione alle disposizioni sulla protezione dei dati. I dati non devono essere inoltrati a terzi, per esempio per scopi economici. Informatevi presso il vostro addetto alla protezione dei dati. Sul sito della Conferenza degli incaricati svizzeri per la protezione dei dati (privatim) trovate consigli relativi alla protezione dei dati nonché l'elenco dei sorveglianti: www.privatim.ch

> **Utilizzate password sicure**
Definite regole vincolanti per le password e imponetene il rispetto anche ai collaboratori. La lunghezza minima della password dovrebbe essere di dodici caratteri e comprendere lettere minuscole e maiuscole, cifre e caratteri speciali. Idealmente la password è generata casualmente e non ha riferimento ad informazioni personali, quali nomi o data di nascita. L'autenticazione a due fattori offre una protezione addizionale. Evitate assolutamente l'utilizzo della stessa password per più servizi! Se risulta difficile memorizzare più password utilizzate un password manager.

Se ci si attiene a queste regole, non è per forza necessario cambiare le password periodicamente. In ogni modo, le password devono essere cambiate immediatamente se esiste la possibilità che terzi ne siano a conoscenza o se un collaboratore non lavora più presso il Comune.

> **Sensibilizzate i collaboratori fissi e di milizia**[3]
In caso di un attacco informatico, i responsabili del Comune sono chiamati in causa. Fra i loro compiti si annovera anche la sensibilizzazione dei collaboratori. I segretari comunali assumono un ruolo di grande responsabilità nell'amministrazione comunale e sempre più spesso sono chiamati a prendere decisioni anche in merito alle TIC. Si raccomanda di offrire loro una formazione specialistica in merito a questo ambito e in generale di investire nel Security Awareness Training dei collaboratori fissi e di milizia. Organizzatevi con altri Comuni o le associazioni cantonali dei Comuni. In tal modo potrete probabilmente ridurre costi e oneri. Nella lista di controllo «Suggerimenti per i collaboratori dei Comuni» troverete informazioni utili per i dipendenti.

3 Politici, esterni, ecc.

> **Attenzione alla gestione delle email**
Spesso i malware arrivano nei computer attraverso allegati di email, camuffati da fatture o candidature. Bloccate la ricezione di allegati pericolosi. Una lista esaustiva ed aggiornata di allegati pericolosi è disponibile sul sito web di GovCERT[4]. Assicuratevi che nessuna macro di dubbia provenienza possa essere eseguita dai programmi Office. Discutete dell'argomento con il responsabile TIC del Comune. Definite processi di comunicazione, in modo che i dipendenti sappiano come procedere per notificare eventi sospetti (email, computer, telefonate, ecc.), e se necessario attivate una funzione per la segnalazione di email dubbie.

Comunicate accuratamente anche con i cittadini. Inviate le vostre email solo in formato di testo e utilizzate gli allegati con parsimonia. Evitate di utilizzare documenti Office con macro e utilizzate piuttosto documenti in formato PDF. Presentate i link in modo trasparente, evitando i link verso siti web che richiedano l'inserimento di nome utente, password o altri dati. Le email fraudolente di solito arrivano ancora in modo anonimo; per quanto possibile rivolgetevi ai cittadini con nome e cognome.

Chi conosce le porte di accesso può mantenerle chiuse ai cybercriminali.

> **Proteggete il vostro conto di online banking**
Utilizzate per i vostri pagamenti un computer separato, che non va utilizzato per navigare in Internet o per ricevere email. Discutete con il responsabile TIC del Comune della possibilità di effettuare i pagamenti online in un'area separata dalle altre applicazioni (sandboxing) o in un sistema dedicato, virtualizzato e particolarmente protetto.

Verificate tutti i processi che interessano il traffico dei pagamenti. I collaboratori devono sempre attenersi a queste procedure. Per esempio attraverso il principio del doppio controllo (quattro occhi) e/o con firma collettiva: prima di sbloccare il pagamento è così richiesta la validazione da parte di un altro utente dell'e-banking. Ciò vale in particolare se vi sono più dipendenti con diritto di effettuare i pagamenti. Discutete possibili misure di sicurezza con la vostra banca.

4 www.govcert.ch/downloads/blocked-filetypes.txt

3.2 Misure di protezione tecniche

> **Proteggete i vostri dati**
Definite una procedura che regoli periodicamente il salvataggio dei dati (backup) e seguitela rigorosamente. Considerate quante giornate di perdita dati potreste sopportare e conservate una copia addizionale del vostro backup separatamente (offline) e fuori sede (offsite). Esercitatevi di tanto in tanto nel ripristino del backup e esortate il vostro supplente a fare altrettanto, di modo che in caso di necessità abbiate già dimestichezza con la procedura. Custodite i backup precedenti per vari mesi.

> **Eseguite gli update di sicurezza**
Un software antiquato è una porta spalancata per i malware. Accertatevi che i vostri sistemi siano sempre aggiornati. Ciò vale anche per il Content Management System (CMS), vale a dire per il sistema di gestione del sito Internet. La maggior parte dei CMS dispone di una funzione di aggiornamento automatico semplice da attivare.

> **Installate un antivirus**
Accertatevi che su ogni computer sia installato un antivirus e sia attivata la protezione in tempo reale. Provvedete affinché l'antivirus si aggiorni regolarmente e effettuate quotidianamente una scansione completa del sistema.

> **Proteggete il vostro accesso remoto**
Non limitatevi a proteggere il vostro accesso remoto alla rete attraverso un'autenticazione semplice (nome utente e password). Utilizzate almeno un'autenticazione a due fattori oppure accedete tramite una rete privata virtuale (VPN). Ciò vale anche per l'accesso da parte dei responsabili TIC esterni.

4 Che cosa si deve osservare in caso di esternalizzazione delle prestazioni TIC

Se la vostra infrastruttura TIC è gestita in esterno e se la vostra TIC è gestita da una o più aziende esterne, ecco alcune dritte. Nella lista di controllo «Quanto è protetto il vostro Comune dagli attacchi informatici?» trovate altri requisiti che dovrebbero essere soddisfatti nel catalogo delle prestazioni di servizio e nel contratto con l'impresa di servizio TIC. Tenete presente che la responsabilità non può essere esternalizzata o delegata a terzi. In caso di evento, il Comune può ritrovarsi ad essere l'ultimo anello della catena della responsabilità.

La responsabilità è dei responsabili comunali.

- **Attenetevi ai requisiti minimi**
  Già al momento della presa in consegna dei sistemi TIC devono essere eseguite delle verifiche di sicurezza. Informatevi presso il responsabile del servizio cantonale di informatica o l'associazione dei Comuni in merito alle condizioni generali e alle direttive da osservare nell'utilizzo dei servizi di informatica. Queste prescrizioni dovrebbero essere parte integrante del contratto fra il Comune e il fornitore di servizi. Gli obblighi legali in materia di segretezza per la manutenzione e la cura di sistemi TIC da parte di terzi devono essere disciplinati; non va consentito un accesso non necessario a dati personali degni di particolare protezione. Vanno eseguiti e concordati accertamenti e accordi anche con l'impresa incaricata del salvataggio dei dati (impresa di servizi cloud).

- **Scegliete un'impresa di servizi TIC qualificata**
  Le certificazioni secondo standard di protezione dei dati e di sicurezza dell'informazione riconosciuti oppure rapporti di controllo di terzi indipendenti possono essere utili nella scelta dell'azienda (v. lista di controllo «Standard e linee guida raccomandati nel settore TIC»). Tuttavia, non è obbligatorio scegliere un'azienda certificata. È consigliabile scegliere fornitori di servizi TIC in grado di dimostrare di poter soddisfare i requisiti definiti e che possano garantire la disponibilità e la sicurezza di cui si ha bisogno. Chiedete a un ente indipendente di certificare o verificare questi fattori.

- **Eseguite audit di sicurezza**
  L'attuazione delle prestazioni specificate nel contratto deve essere verificata periodicamente mediante standard di auditing riconosciuti, per esempio COBIT (Control Objectives for Information and Related Technology) della ISACA (Information Systems Audit and Control Association). Avvaletevi dei servizi di centri di controllo indipendenti. Il fornitore di servizi TIC può chiedere che sia realizzato un cosiddetto ISAE 3402 Type 2 (International Standard on Assurance Engagements) – noto anche come Rapporto SOC-2 (Service Organization Control). L'organismo di controllo valuta anche la sicurezza, la disponibilità, l'integrità e la riservatezza.

- **Unitevi ad altri Comuni**
  Se il vostro Comune non si trova in condizioni finanziarie tali da acquisire servizi ampliati di un fornitore di TIC, unitevi ad altri Comuni interessati. In tal modo potrete approfittare di condizioni di acquisto più vantaggiose e di una procedura semplificata. Un'altra opzione può essere l'esternalizzazione di questo compito ad un Comune più grande.

- **Procuratevi l'aiuto necessario**
  Diversi enti pubblici, associazioni e organizzazioni offrono informazioni importanti sull'esternalizzazione di prestazioni IT e vari ausili, quali linee guida, promemoria e modelli di contratto per la collaborazione con i fornitori di IT.

Ecco alcuni esempi di enti pubblici, associazioni e organizzazioni:

Tecnologia dell'informazione e della comunicazione (TIC)

- I servizi cantonali TIC dispongono di linee guida e ausili, per esempio l'Amt für Informatik und Organisation del Cantone di Berna (KAIO), www.be.ch/kaio
- Anche le associazioni dei Comuni possono offrire assistenza. Sul sito www.chgemeinden.ch trova un elenco delle associazioni dei Comuni.
- Sul sito dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) troverà standard minimi per le TIC: www.bwl.admin.ch.
- Il Centro nazionale per la cibersicurezza[5] (NCSC), www.ncsc.ch, dispone di informazioni provenienti da servizi di attività informative e di conoscenze ottenute attraverso i Computer Emergency Response Teams (CERT) di altri Paesi, nonché di misure di prevenzione. Se il vostro fornitore di prestazioni TIC non è ancora affiliato, vogliate rivolgervi a outreach@ncsc.ch
- Le condizioni generali di contratto della Conferenza Svizzera per l'Informatica (CSI) si prestano per le TIC e il loro impiego nell'amministrazione pubblica. Per le CG della CSI esistono anche modelli di contratto: https://sik.swiss
- Il label cyber-safe.ch è stato sviluppato dall'Associazione svizzera per il label di cybersicurezza. Il label definisce i requisiti minimi specifici per i Comuni e le PMI. Le minacce cibernetiche di Comuni e PMI possono essere individuati mediante un questionario online: www.cyber-safe.ch

Acquisti

- I siti web di eGovernment Svizzera, www.egovernment.ch e dell'associazione simap.ch, www.simap.ch, offrono una panoramica dei servizi di acquisto delle amministrazioni federali, cantonali e delle maggiori città.

Protezione dei dati

- Sul sito della Conferenza degli incaricati svizzeri per la protezione dei dati (privatim) si trovano ausili relativi alla protezione dei dati nonché l'elenco corrispondente: www.privatim.ch
- L'incaricato federale della protezione dei dati e della trasparenza (IFPDT) è responsabile del trattamento di dati da parte di privati e da parte degli organi federali, www.edoeb.admin.ch

5 Dal 1° gennaio 2020 diversi compiti della Confederazione relative al cyberspazio sono riuniti sotto il cappello del Centro nazionale per la cibersicurezza. Ciò vale anche per la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

5 Che cosa si deve fare in caso di attacco

Aiuto di emergenza in caso di attacco informatico

Isolare
> Scollegate immediatamente tutti i sistemi dalla rete. Non dimenticate di spegnere la WLAN.

Contattare
> Contattate i responsabili TIC nonché tutti gli interlocutori dell'organizzazione di cui avete bisogno per gestire la situazione.
> Valutate se contattare la polizia e sporgere denuncia. Per il reboot dei sistemi aspettate che la polizia abbia rilevato le tracce. I collaboratori specializzati della polizia vi assistono con consulenza e supporto su come procedere, rilevano le tracce e conducono l'indagine. Su www.suisse-epolice.ch trovate il numero telefonico del posto di polizia più vicino.

Notificare
> Segnalate l'attacco anche al NCSC, www.ncsc.ch. Anche la vostra associazione dei Comuni dovrebbe essere messa al corrente dell'evento, visto che eventualmente possono essere interessati altri Comuni.
> Osservate gli obblighi di notifica, per esempio in merito alla protezione dei dati.

I responsabili TIC o altri esperti vi aiutano a riparare l'infrastruttura e eventualmente a ripristinarla.

Prima che avvenga il prossimo attacco integrate le conoscenze acquisite nel perfezionamento della qualità, nei processi interni, nelle documentazioni, negli esercizi nonché nella gestione e nella cultura aziendale.

6 Come potete contribuire all'identificazione degli autori del reato

6.1 Non temere di sporgere denuncia

L'esperienza ci insegna che molti reati nel cyberspazio sono correlati e presentano delle similitudini. Ogni denuncia e ogni segnalazione può fornire l'indizio determinante per individuare gli autori.

La polizia non è interessata a conoscere i segreti della vostra amministrazione comunale e non influisce sulla vostra infrastruttura. In caso di attacco cerca solo informazioni e tracce rilevanti per risolvere il caso. L'indagine è coperta dal segreto d'ufficio. Inoltre, le disposizioni sulla protezione dei dati vanno osservate anche nelle indagini. I timori di ripercussioni negative in caso di denuncia, come ad esempio il sequestro di computer per un periodo di tempo prolungato oppure la pubblicazione di informazioni sul caso, sono infondati. La polizia vi prenderà sul serio e di regola prima di agire discuterà con voi le misure che verranno intraprese. In ogni momento potrete anche consultare il vostro consulente legale. Nella maggior parte dei casi sarà possibile trovare una procedura che soddisfi entrambe le parti.

Un intervento tempestivo in caso di attacchi informatici può ridurre i danni

6.2 Segnalare l'accaduto immediatamente

Notificate gli avvenimenti rilevanti dal punto di vista penale, quali ad esempio l'intrusione in un sistema di elaborazione dati, il più presto possibile alla polizia o al pubblico ministero, in particolare in caso di danno. Più temporeggiate e maggiore sarà la probabilità che vengano cancellate preziose tracce. Inoltre, ogni interferenza può portare all'inutilizzabilità delle tracce o alla loro cancellazione. La denuncia può essere sporta presso qualsiasi posto di polizia. Su (www.suisse-epolice.ch) trovate il numero telefonico del posto di polizia più vicino.

Considerate inoltre di segnalare volontariamente alle autorità inquirenti o al NCSC anche nei casi in cui non è stato causato alcun danno o l'attacco è stato sventato prima di essere commesso. Le notifiche al NCSC non possono però essere utilizzate per una querela o in un procedimento penale.

Suggerimenti ai responsabili comunali per proteggersi da attacchi informatici

Un attacco informatico può colpire ogni Comune. Con alcuni accorgimenti, tuttavia, potrete proteggere meglio il vostro Comune.

Chiarite le responsabilità e attuate delle misure di prevenzione

> Definite le responsabilità in materia di sicurezza informatica, come pure le interfacce con i vostri partner. Processi collaudati e percorsi di «escalation» sono indispensabili per mantenere il controllo.

Proteggete i vostri dati

> Disciplinate la gestione delle informazioni e dei dati sensibili. I canali privati non devono essere utilizzati per l'inoltro di informazioni confidenziali.
> Utilizzate i servizi cloud con cautela. Leggete le condizioni generali dell'azienda che offre i servizi di cloud e prestate attenzione alle disposizioni sulla protezione dei dati. I dati sensibili non devono mai essere salvati nel cloud se prima non sono stati cifrati.
> Definite una procedura che disciplini il salvataggio periodico (backup) dei dati. Conservate una copia addizionale del backup separatamente (offline) e fuori sede (offsite).

Utilizzate password sicure

> La lunghezza minima di una password dovrebbe essere di dodici caratteri, composti da lettere minuscole e maiuscole, cifre e caratteri speciali. L'autenticazione a due fattori offre una protezione addizionale. Evitate assolutamente l'utilizzo della stessa password per più servizi. Utilizzate piuttosto un password manager e generate una password specifica per ogni applicazione.

Sensibilizzate i collaboratori fissi e di milizia (politici e/o collaboratori esterni)

> I segretari comunali assumono un ruolo di grande responsabilità nell'amministrazione comunale e sempre più spesso sono chiamati a prendere decisioni anche in merito alle TIC. Si raccomanda di offrire loro una formazione specialistica in merito a questi argomenti e in generale di investire nella Security Awareness Training (allenamento nella consapevolezza della sicurezza) dei collaboratori fissi e di milizia.

Attenzione alla gestione delle email

> Bloccate la ricezione di allegati email pericolosi e assicuratevi che nessuna macro di dubbia provenienza possa essere eseguita da programmi Office. Definite canali di comunicazione attraverso i quali i collaboratori possano segnalare avvenimenti sospetti (email, computer, telefonate, ecc.). Se possibile, attivate una funzione per la segnalazione delle email sospette.

Mantenetevi sempre aggiornati

> Implementate software antivirus e assicuratevi che tutti i computer e i server nella vostra rete eseguano automaticamente gli aggiornamenti di sicurezza.

Proteggete il vostro accesso remoto

> Proteggete gli accessi remoti sulla vostra rete con un'autenticazione a due fattori. L'ideale è utilizzare un collegamento sicuro attraverso una rete virtuale privata (VPN).

Prestate attenzione alla sicurezza dell'online banking

> Proteggete il vostro conto bancario online con un computer separato, un'area distinta (sandboxing) o un sistema dedicato, virtualizzato e particolarmente protetto. Regolate i processi di pagamento, per esempio con un principio di doppio controllo o con la firma collettiva.

Suggerimenti ai collaboratori dei Comuni per prevenire gli attacchi informatici

In caso di un attacco informatico, i responsabili comunali sono chiamati in causa. Fra i loro compiti si annovera anche la sensibilizzazione dei collaboratori. Le seguenti misure dovrebbero essere attuate quotidianamente dai vostri collaboratori.

Cautela nella gestione delle email

> Trattate con diffidenza i link o gli allegati in email di mittenti che non conoscete. È richiesta particolare prudenza se aprite documenti in Office; non attivate mai la macro. Non esitate a chiedere di persona, se una mail vi sembra sospetta. Ciò vale anche per i mittenti che conoscete! Siate prudenti anche con l'uso del pulsante «Rispondi». Verificate che la mail vada veramente alla persona giusta. L'ideale sarebbe di digitare l'indirizzo email ex novo.

Utilizzate password sicure

> La lunghezza minima di una password dovrebbe essere di dodici caratteri, composti da lettere minuscole e maiuscole, cifre e caratteri speciali. Non comunicate mai password, dati di accesso o informazioni relative al conto per telefono, per mail o attraverso formulari web aperti seguendo un link.
> Evitate assolutamente l'utilizzo ripetuto della stessa password per più servizi.

Prestate attenzione ai dati da proteggere

> Pensate attentamente a quali informazioni volete rendere pubbliche, come ad esempio nel sito web e nei social network, divulgare o discutere nella corrispondenza con il pubblico.
> Le informazioni confidenziali da inoltrare a esterni dovrebbero essere sempre inviate in forma cifrata o per posta.

Quanto è protetto il vostro Comune dagli attacchi informatici?

Quanto è protetta la vostra amministrazione comunale dagli attacchi informatici e in quale modo è pronta a contrastarli? Questa lista di controllo vi aiuterà a confrontarvi con le questioni più importanti relative ad una protezione minima nel cyberspazio. Informatevi bene su ogni punto al quale rispondete «non so» o «no». Tenete presente le considerazioni seguenti: le misure per la protezione del cyberspazio non possono essere delegate ai collaboratori, ma devono essere affrontate e coordinate dai responsabili comunali.

Se avete già esternalizzato le tecnologie dell'informazione e della comunicazione (TIC), appurate che i seguenti punti siano inclusi nel contratto con il fornitore di servizi.

	Sì	No	Non so
Compiti, competenze, responsabilità			
Nel vostro Comune è stata definita la persona responsabile della cybersicurezza?	○	○	○
La persona responsabile dispone delle conoscenze e delle abilità necessarie per gestire la cybersicurezza e si aggiorna regolarmente?	○	○	○
La persona responsabile occupa la posizione gerarchica corrispondente e dispone delle competenze necessarie per attuare misure di cybersicurezza?	○	○	○
Esistono direttive per l'uso sicuro di dispositivi TIC e per la gestione dei dati?	○	○	○
Queste direttive e misure di cybersicurezza sono attuate sistematicamente e verificate regolarmente?	○	○	○
Sensibilizzare i collaboratori fissi e di milizia			
Esistono direttive sulla gestione sicura di mail, dati digitali e Internet per i collaboratori?	○	○	○
I collaboratori conoscono queste direttive e le capiscono?	○	○	○
I collaboratori applicano le direttive in modo coerente e corretto?	○	○	○
I collaboratori sono formati e sensibilizzati regolarmente sulla cybersicurezza, per esempio per quanto riguarda la gestione corretta delle email?	○	○	○
Direttive sulla protezione dei dati			
I dati sui vostri sistemi (archivi e memorie, terminali e server) sono cifrati?	○	○	○
Siete a conoscenza delle disposizioni di legge relative al salvataggio e al trattamento dei dati?	○	○	○
Conoscete i vostri obblighi relativi alle disposizioni legali sui dati personali?	○	○	○
Le disposizioni in vigore sulla protezione dei dati sono applicate in modo coerente e corretto nell'amministrazione del vostro Comune?	○	○	○
Nell'amministrazione del vostro Comune l'accesso fisico all'infrastruttura informatica (computer, server e rete) è adeguatamente protetto dall'accesso di terzi?	○	○	○
Direttive sulle password e sull'amministrazione degli utenti			
Nell'amministrazione del vostro Comune esistono direttive sull'utilizzo di password?	○	○	○
Vi sono direttive che definiscono quali collaboratori hanno accesso a quali dati?	○	○	○
Queste direttive sono applicate in modo coerente e corretto?	○	○	○
Protezione aggiornata da malware			
I vostri dispositivi sono protetti da malware (programmi antivirus)?	○	○	○
Firewall configurati e aggiornati			
La vostra rete e i vostri sistemi TIC sono protetti da firewall?	○	○	○
Sono state definite regole firewall specifiche (p.es. restrizioni geografiche)?	○	○	○
Il vostro firewall è aggiornato regolarmente?	○	○	○

	Sì	No	Non so
Segmentazione della rete			
I vari settori della vostra amministrazione comunale, per esempio personale e contabilità, sono separati?			
Utilizzate un computer separato o un sistema separato per l'online banking?			
Accesso remoto			
Nell'amministrazione comunale l'accesso esterno all'infrastruttura (computer, server e rete) è protetto (VPN, autenticazione a due fattori)?			
Mantenere aggiornati gli apparecchi e i sistemi connessi a Internet			
Vi avvalete della possibilità dell'aggiornamento automatico del software?			
Il software di apparecchi e sistemi non aggiornato automaticamente viene aggiornato regolarmente per esempio dal produttore?			
I dispositivi mobili utilizzati nel contesto dell'amministrazione comunale sono aggiornati regolarmente?			
Il Content Management System per il vostro sito web corrisponde agli standard più recenti?			
Rete WLAN protetta e cifrata			
La vostra WLAN è protette e cifrata?			
Esiste una WLAN separata per collaboratori e ospiti?			
Backup			
Utilizzate un processo di backup dati?			
Controllate regolarmente la funzionalità e la leggibilità del backup?			
Conservate una copia addizionale del backup separatamente (offline) e fuori sede (offsite)?			
Precauzioni minime in caso di emergenza			
Sono definite le misure di emergenza in caso di evento TIC?			
In caso di evento TIC (p.es. in caso di malfunzionamento, attacco o simili) sono definiti e reperibili i responsabili e le persone di contatto?			
Esistono piani operativi di reazione e di riavvio?			
Sapete come funziona il monitoraggio dei sistemi e dei processi di «escalation»?			
Vi è la possibilità di indagini forensi proprie? In caso negativo: queste indagini sono assicurate da esterni?			
L'accesso fisico ai sistemi è garantito (per l'equipe di indagini forensi)?			
Sono disponibili supporti dati in misura sufficiente per salvare le prove?			
È disciplinato l'obbligo di documentazione di tutti i sistemi rilevanti (p.es. in un Configuration Management Database, CMDB)?			
Contratto con il fornitore di servizi TIC			
I punti menzionati sopra sono coperti dal contratto stipulato con il fornitore di servizi?			
La responsabilità civile in caso di danno e l'esclusione di obbligo di prestazione (p.es. per forza maggiore) sono disciplinate dal contratto?			
I livelli di servizio per l'esercizio regolare e di emergenza sono definiti in modo chiaro (servizi previsti negli obiettivi di sicurezza necessari, p.es. disponibilità, riservatezza o integrità)? Sono definiti concetti quali esercizi di emergenza o per eventi critici?			
Si è riflettuto sulla strategia di exit ed è stata definita nel contratto, in particolare per le soluzioni di cloud?			

La lista di controllo si basa sul test rapido di cybersicurezza per le PMI di ICTswitzerland e di altri partner:
www.cybersecurity-check.ch

Standard e linee guida raccomandati nel settore TIC

Le certificazioni di conformità agli standard di protezione di dati e sicurezza dell'informazione o rapporti di controllo di terzi indipendenti possono essere d'aiuto nella scelta del fornitore di servizi TIC. Tuttavia, non è obbligatorio scegliere un'azienda certificata. È consigliabile scegliere fornitori di servizi TIC in grado di dimostrare di soddisfare i requisiti definiti e di garantire la disponibilità e la sicurezza di cui si ha bisogno. Chiedete a un ente indipendente di certificare o verificare questi fattori.

Esiste un'ampia varietà di standard e linee guida. I fornitori di TIC dovrebbero conoscere gli standard ISO 27001, ISO 22301, ISO 9001 e ISO 14001 ed essere conformi a quanto stabiliscono. Se gli standard utilizzati sono altri, l'azienda deve presentare un compliance-mapping. Se le vostre esigenze di protezione sono maggiori, dovete formulare voi stessi requisiti più severi.

Esempi di standard e linee guida:

Gestione di crisi, Business Continuity, Disaster Recovery
- ISO 22301, Business Continuity Management System
- ISO 27031, IT Service Continuity Management System
- BS 11200, Sistema di gestione di crisi

Sicurezza dei dati e dell'informazione
- ISO 27001, Sicurezza dell'informazione
- ISO 27701, Estensione di ISO 27001 alla protezione dei dati
- ISO 30141 Internet of Things (IoT) – Reference Architecture, in particolare per la riservatezza dei dati elaborati
- Conformità con il Regolamento dell'UE 2016/679 sulla protezione dei dati (GDPR)
- NIST Cyber Security Framework

Guide tecniche
- EN 50173, Cablaggio strutturato
- EN 50600, Data center
- ANSI/TIA-942, Data center

Altri (in particolare fornitori di hardware)
- ISO 9001, Gestione della qualità
- ISO 14001, Gestione ambientale

Linee guida per i committenti
- ISO 22300, Norma Sicurezza e resilienza, vocabolario
- ISO 22318, Supply Chain Continuity
- ISO 27036, Sicurezza dell'informazione nella gestione dei fornitori
- ISO 31010, Gestione dei rischi

Note editoriali

Polizia cantonale di Berna, Centro nazionale per la cibersicurezza (NCSC) e Rete integrata Svizzera per la sicurezza (RSS) per la Rete nazionale di sostegno alle indagini nella lotta contro la criminalità informatica (NEDIK)

Con la partecipazione di: Amt für Informatik und Organisation des Kantons Bern (KAIO), Verband Bernischer Gemeinden (VBG), Associazione dei Comuni Svizzeri (ACS)

Contatto: Polizia cantonale di Zurigo, NEDIK, cyc_nedik@kapo.zh.ch

Immagini: iStock

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali