

Prevenzione della criminalità informatica

Guida per le piccole e medie imprese

**Sapete quanto è protetta
la vostra azienda?**

Verificatelo utilizzando la lista di controllo
alla fine di questo opuscolo!

Indice

1_Cybersecurity nelle aziende come aspetto esistenziale	3
2_Ecco come agiscono i criminali	4
3_Come proteggere la vostra azienda	6
4_Cosa sarebbe da considerare nel caso di esternalizzazione dei servizi TIC	11
5_Come superare gli attacchi informatici	12
6_Cercate supporto	13
7_Allegati	14

1_Cybersecurity nelle aziende come aspetto esistenziale

La digitalizzazione apre nuove opportunità di crescita e di occupazione per l'economia.

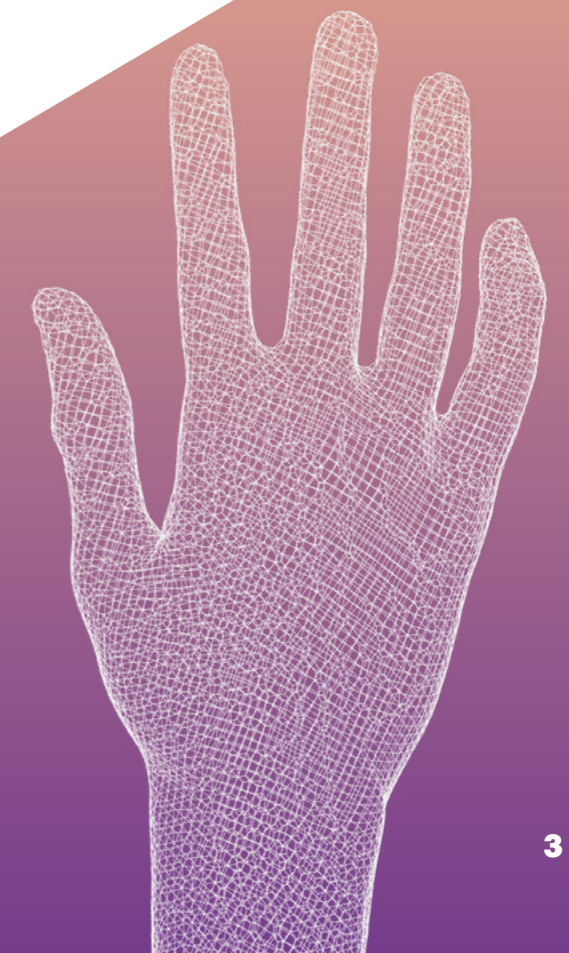
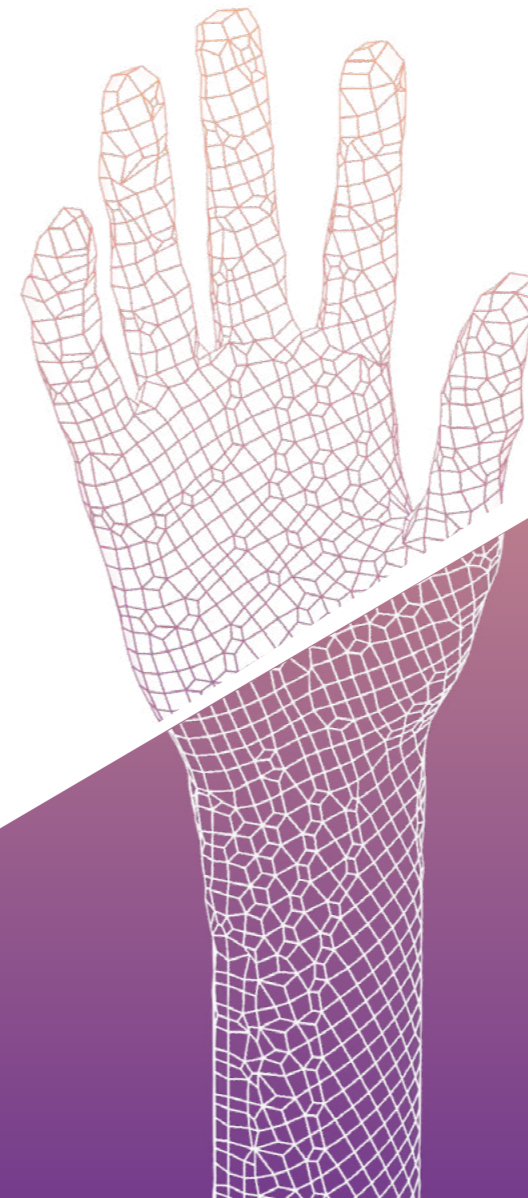
Allo stesso tempo, richiede nuovi processi e comporta una maggiore dipendenza dal funzionamento delle tecnologie dell'informazione e della comunicazione (TIC). Anche i criminali sfruttano queste dipendenze.

I criminali utilizzano metodi sempre più sofisticati per accedere alle reti, rubare dati o paralizzare interi sistemi. Dalle piccole imprese artigianali alle grandi aziende: un attacco informatico può rappresentare una minaccia

esistenziale per le imprese.

Con questo materiale informativo, la polizia fornisce ai dirigenti delle piccole e medie imprese raccomandazioni di base su come proteggersi dalla criminalità informatica. I contenuti si basano, tra l'altro, sull'esperienza delle indagini di polizia.

La guida mostra anche cosa fare dopo un attacco e perché vale la pena rivolgersi alla polizia.



2_Come agiscono i criminali

Gli attacchi di solito iniziano con la raccolta di informazioni sull'azienda da parte dei criminali. Sulla base delle informazioni presenti sul sito Web dell'azienda o sui social media, vengono identificate le vulnerabilità nell'ambiente aziendale, vengono individuati le possibili porte d'entrata nella rete aziendale e viene sviluppato uno scenario di attacco adeguato.

2.1 Tipiche porte d'entrata

Manipolazioni

I criminali sfruttano la disponibilità, la buona fede o l'insicurezza dei dipendenti per ottenere da loro informazioni rilevanti per la sicurezza o per accedere alle reti aziendali ("social engineering"). Contattando le persone via e-mail ("phishing") o per telefono, gli autori tentano di convincerle a consegnare dati sensibili. Inviando allegati infetti in messaggi fraudolenti o link a siti web infetti, i criminali riescono a infiltrarsi nei dispositivi con malware e quindi ad accedere alle reti aziendali.

Lo "spear phishing" è una forma di manipolazione particolarmente insidiosa e diffusa. Le vittime prese di mira sono indotte a credere di comunicare con persone, organizzazioni o aziende fidate. Poiché la fonte dei messaggi sembra essere nota e le informazioni sembrano plausibili, anche le persone più attente possono non riconoscere la manipolazione.

Accesso da remoto (Remote Access)

L'accesso da remoto viene utilizzato per accedere a un computer o a una rete dall'esterno, ad esempio per lavorare da casa o per la manutenzione a distanza da parte del personale di supporto. Anche i criminali utilizzano questo accesso da remoto per accedere alle reti aziendali. Ciò avviene soprattutto se l'accesso da remoto non è protetto in modo adeguato.

Vulnerabilità nelle applicazioni

Anche lo sfruttamento delle vulnerabilità nelle applicazioni è un approccio comune negli attacchi informatici. Può trattarsi di vulnerabilità del software, di vulnerabilità di progettazione o di parametri di protezione mal configurati, come ad esempio password deboli.

2.2 Possibili scenari di attacco



Crittografia, furto o corruzione dei dati

I dati vengono crittografati durante un attacco e rilasciati solo dietro pagamento di un riscatto ("ransomware"), rubati e rivenduti a scopo di lucro, ad esempio sul darknet ("data leakage"), oppure vengono utilizzati per ricattare aziende terze colpite. L'accesso non autorizzato a un sistema di elaborazione dati può anche avere come obiettivo la distruzione dei dati, ad esempio per ottenere un vantaggio sulla concorrenza o per bloccare un'attività in corso. Gli attacchi possono provenire sia dall'esterno che dall'interno dell'azienda: Anche i dipendenti possono manipolare o distruggere dati aziendali riservati o trasmetterli a persone non autorizzate.



La truffa del CEO

Di solito si tratta di un attacco personalizzato che utilizza informazioni sull'azienda raccolte in precedenza. La frode è spesso realizzata attraverso false e-mail inviate dalla direzione dell'azienda o dai presidenti delle società all'ufficio finanze o a persone con funzioni di cassiere. Una storia credibile viene utilizzata per convincere la persona contattata a effettuare pagamenti presumibilmente urgenti.



Frode con manipolazione di fatture

Gli autori inviano nuovamente fatture già spedite con un numero IBAN diverso o istruiscono le vittime a utilizzare un conto destinatario diverso per i pagamenti futuri. Si fa riferimento a una comunicazione e-mail esistente contenente un'istruzione di pagamento o una fattura. Ciò significa che i criminali hanno precedentemente avuto accesso all'account e-mail del mittente o del destinatario.



Attacco di sovraccarico

In un attacco DDoS ("Distributed Denial of Services"), i sistemi o le reti di un'azienda vengono completamente sovraccaricati in modo da renderli temporaneamente non disponibili. L'attacco viene mantenuto fino al pagamento di un riscatto. Le aziende che hanno un negozio online, ad esempio, devono aspettarsi una notevole perdita di profitti o di ordini in caso di attacco DDoS. Questo tipo di attacco non richiede un accesso preventivo alla rete della vittima.



Attacco fisico

Anche l'infrastruttura TIC fisica di un'azienda può essere attaccata, ad esempio sabotando le linee dati o manipolando i dispositivi elettronici e i supporti dati.



Ulteriori informazioni sulle attuali minacce informatiche sono disponibili all'indirizzo

www.ncsc.admin.ch

3_Come proteggere la vostra azienda

La protezione contro la criminalità informatica dovrebbe far parte di un concetto di sicurezza olistico e completo. Questo è orientato sia alla tecnologia che all'organizzazione.

3.1 Chiarite le responsabilità

Definite chiaramente ruoli e responsabilità nell'ambito della sicurezza informatica. Se avete affidato la TIC a terzi, regolate le responsabilità per contratto. Tuttavia, la responsabilità della sicurezza informatica della vostra azienda rimane a voi. I dipendenti devono anche sapere chi contattare in caso di domande sulla sicurezza informatica, ad esempio se ricevono un'e-mail sospetta o chi informare in caso di incidente.

3.2 Regolamentate l'accesso ai sistemi

Autorizzazioni e regole

Definite quali dati della vostra azienda sono considerati particolarmente degni di protezione. Create un concetto di protezione specifico per questi elementi. Ciò include la definizione dei diritti d'uso e delle autorizzazioni di accesso ai dati e ai sistemi e la regolamentazione dell'uso dei dispositivi privati utilizzati per le attività aziendali.

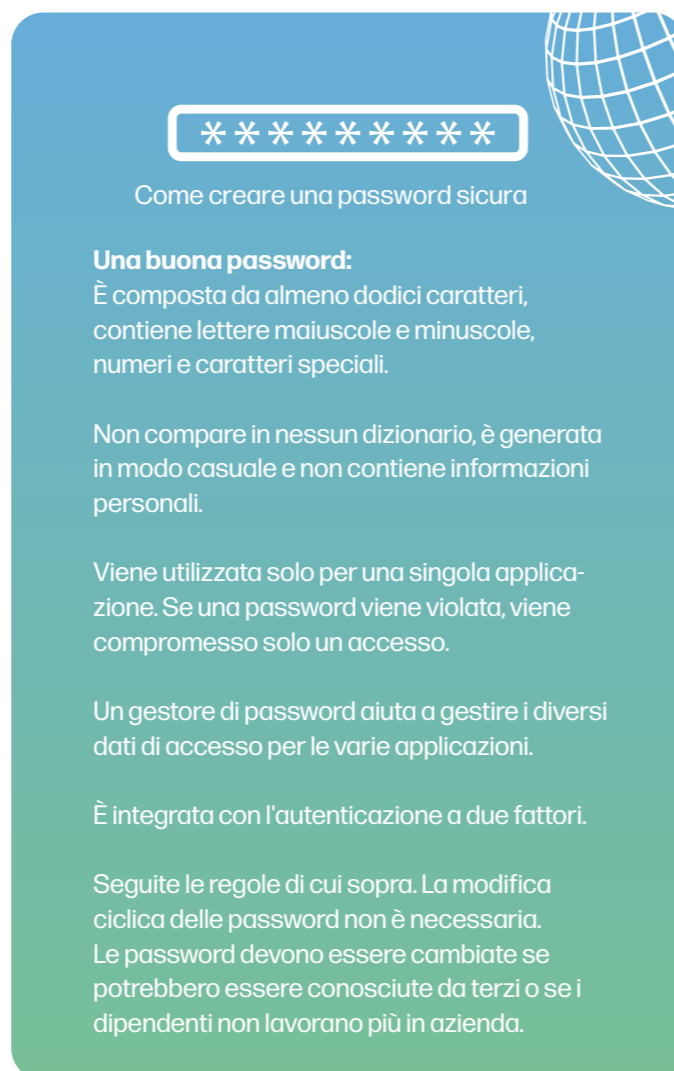
I dipendenti non devono avere diritti di amministratore. Ai dipendenti devono essere concessi solo i diritti necessari per svolgere il lavoro loro assegnato (principio della necessità di sapere).

Limitare i diritti di sistema in modo che i dipendenti non possano installare o aggiornare il software da soli.

Gli amministratori devono lavorare con un account di amministratore specifico configurato per questa attività e separato dall'account dei dipendenti.

Definite per le password regole vincolanti di elevata complessità e lunghezza e applicatele in modo coerente ai dipendenti. Impostate l'autenticazione a più fattori per l'accesso alla rete aziendale. Questo vale in particolare per gli amministratori o altri account privilegiati.

Riflettete attentamente sulle informazioni - anche quelle apparentemente innocue - che divulgate sul sito web aziendale o sui social media, poiché vengono raccolte dai criminali e possono essere utilizzate per attacchi mirati.



***** ** ***

Come creare una password sicura

Una buona password:
È composta da almeno dodici caratteri, contiene lettere maiuscole e minuscole, numeri e caratteri speciali.

Non compare in nessun dizionario, è generata in modo casuale e non contiene informazioni personali.

Viene utilizzata solo per una singola applicazione. Se una password viene violata, viene compromesso solo un accesso.

Un gestore di password aiuta a gestire i diversi dati di accesso per le varie applicazioni.

È integrata con l'autenticazione a due fattori.

Seguite le regole di cui sopra. La modifica ciclica delle password non è necessaria. Le password devono essere cambiate se potrebbero essere conosciute da terzi o se i dipendenti non lavorano più in azienda.

Infrastruttura TIC protetta e documentata

L'infrastruttura di rete, i dispositivi per ufficio e mobili e le attrezzature speciali devono essere protetti da accessi non autorizzati, perdita, furto o distruzione. Integrate le considerazioni sulla sicurezza nel processo di acquisto dell'infrastruttura TIC. Considerate non solo i requisiti per la messa in funzione, ma anche per l'intero ciclo di vita di un sistema, compresa la manutenzione e lo smaltimento. Informatevi, ad esempio, su quanto tempo saranno disponibili gli aggiornamenti di sicurezza per i vostri dispositivi. Documentate l'intera rete. I dati, le persone, i dispositivi, i sistemi e le strutture dell'azienda devono essere identificati, catalogati e valutati in termini di criticità. Solo così saprete cosa dovete proteggere. Anche se avete esternalizzato la TIC, dovete mantenere una visione d'insieme: siete voi i responsabili.

E-Banking sicuro

Chiarite tutti i processi relativi alle transazioni di pagamento. Imponete in modo coerente il rispetto di tali processi; ad esempio, il principio del doppio controllo, le firme collettive, le interrogazioni tramite un secondo canale, soprattutto in caso di modifiche del conto.

Se possibile, utilizzate un computer separato per i pagamenti, sul quale non navigate in Internet né ricevete e-mail, ma che aggiornate regolarmente. In alternativa, potete effettuare i pagamenti online in un'area separata dal resto delle vostre applicazioni ("sandboxing") o in un sistema virtualizzato dedicato e appositamente protetto. Parlate con la vostra banca di queste e altre misure di sicurezza.

Comunicazione criptata

Le informazioni confidenziali devono essere archiviate in forma criptata (questo vale anche per il cloud) e trasmesse o inviate per posta tradizionale a soggetti esterni. L'accesso ai dati deve avvenire tramite un canale sicuro come una VPN, soprattutto se i dipendenti accedono alla rete aziendale dall'esterno. Comunicate con attenzione con i vostri clienti e le aziende partner. Come primo passo, firmate le e-mail in uscita. Questo garantisce la loro integrità e la loro origine. Le firme digitali delle e-mail consentono inoltre ai clienti di crittografare le e-mail di risposta. In alternativa, potete utilizzare certificati di crittografia per i vostri messaggi.

L'uso di punti di accesso esterni e pubblici (hotspot) deve essere regolamentato in modo particolare, poiché in genere non sono criptati e sono quindi considerati insicuri.

Cloud

Per i servizi cloud vale lo stesso discorso fatto per qualsiasi partnership commerciale: quando si sceglie un provider cloud, assicurarsi che l'azienda sia affidabile (certificati, ubicazione dei dati, rapporti, test, ecc.).

Stabilite un rapporto di fiducia e chiarite le vostre esigenze e le rispettive responsabilità. Prima di utilizzare un servizio cloud, leggete i termini e le condizioni generali del fornitore e prestate attenzione alle norme sulla protezione dei dati. Pensate bene a quali dati volete caricare nel cloud e al rischio associato alla loro archiviazione. Se ci sono requisiti legali particolari, i dati dovrebbero essere archiviati in Svizzera.

È consigliabile non archiviare dati sensibili nel cloud o archivarli solo in forma criptata. In questo contesto, verificate anche i diritti di condivisione se volete condividere i vostri dati, ad esempio restrittivi o limitati nel tempo, e quanto sia facile rimuovere nuovamente i vostri dati dal cloud se volete cambiare servizio in futuro.

Si noti che il cloud è un mezzo di archiviazione online e può quindi essere anch'esso colpito da un attacco informatico. I servizi cloud offrono solo una protezione limitata contro gli attacchi con malware di crittografia (ransomware). Se i dati sono archiviati esclusivamente nel cloud, anche questi possono essere crittografati in caso di attacco. La protezione dipende soprattutto dal fatto che i servizi offrano il ripristino delle versioni precedenti e che questo accesso sia protetto in modo particolare, almeno da una password sicura e da un'autenticazione a due fattori.



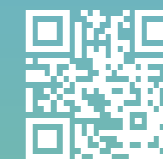
Incaricato federale della protezione dei dati e delle informazioni
www.edoeb.admin.ch



Ufficio federale per la sicurezza delle informazioni Germania
www.bsi.bund.de



Conferenza dei commissari svizzeri per la protezione dei dati (Privatim)
www.privatim.ch



Agenzia dell'Unione europea per la sicurezza informatica
www.enisa.europa.eu

3.3 Rimanete tecnicamente preparati



Impostazioni di base per la sicurezza

Installate una protezione antivirus su ogni computer e attivate la protezione in tempo reale.

Assicuratevi che sia aggiornata regolarmente e che venga eseguita una scansione completa del sistema ogni giorno. Il software obsoleto è un'importante porta d'accesso per il malware. Assicuratevi che i vostri sistemi siano aggiornati (update). Questo vale anche per tutti i programmi e le app, nonché per i sistemi di gestione dei contenuti (CMS) del vostro sito web.

Dovreste utilizzare un firewall personale su ogni computer. Dovreste utilizzare un firewall anche per proteggere la rete aziendale da connessioni indesiderate a Internet. Per impostazione predefinita, il firewall dovrebbe bloccare tutto il traffico ad eccezione del traffico dati autorizzato dalle regole.



Gestione delle vulnerabilità

Assicuratevi che le anomalie e gli eventi rilevanti per la sicurezza vengano riconosciuti in tempo utile.

Monitorate l'infrastruttura di rete, ad esempio con un sistema di rilevamento degli attacchi (IDS) e un sistema di protezione dagli attacchi (IPS). Alcuni di questi sono inclusi anche nei servizi web proxy.

Definite quali file di log (file di log degli eventi) vengono salvati e per quanto tempo. L'analisi dei file di log fornisce informazioni sulla stabilità e sulla disponibilità delle reti, dei sistemi e delle applicazioni. Inoltre, aiuta a riconoscere l'origine di un attacco, a ottenere informazioni sui sistemi infetti nella propria rete e ad adottare contromisure adeguate. In relazione all'archiviazione e all'analisi dei file di log, è necessario osservare gli aspetti relativi alla protezione dei dati.

Tipp: Einfach und umfassend

Molti nuovi sistemi operativi hanno già integrate diverse funzioni di sicurezza, come firewall e protezione di rete, protezione da virus e minacce o aggiornamenti automatici. Attivate le funzioni corrispondenti per tutti i dispositivi della vostra rete.

Le soluzioni all-in-one offrono ad esempio i cosiddetti sistemi di gestione unificata delle minacce. Questa soluzione di sicurezza completa è disponibile come soluzione hardware, software o cloud.



Sicurezza web allargata

Utilizzate componenti aggiuntivi di sicurezza web, come il filtraggio DNS ("Domain Name System") e un proxy web che blocca i siti web noti come dannosi o consente l'accesso solo ai siti web classificati come sicuri ("whitelist"). In questo modo si evitano le richieste di accesso a siti web criminali e si protegge la privacy dell'azienda. Se volete scaricare un programma da Internet, informatevi prima sull'affidabilità del provider e del software in questione. I valori di hash e le firme del software devono essere controllati in base alle specifiche del produttore. Scaricate il software solo dal sito web del produttore.



Segmentazione della rete

Segmentate la rete aziendale in singole aree ("segmentazione della rete"), ad esempio reti separate per la produzione, il personale, la contabilità, ecc. In questo modo si evita, ad esempio, che i computer di controllo degli impianti, non più aggiornabili, diventino un punto di accesso per gli aggressori e mettano a rischio l'intera rete. Utilizzate anche un servizio di directory separato per il vostro backup. In questo modo si può evitare che i criminali già presenti nel sistema accedano al backup.



Accesso remoto (Remote Access)

Protegete l'accesso remoto alla vostra rete con un nome utente, una password e un'autenticazione a due fattori. Utilizzate una connessione sicura tramite una rete privata virtuale (VPN), anche per l'accesso degli amministratori e dei fornitori esterni di servizi TIC. È consigliabile aprire l'accesso alla manutenzione remota solo quando è necessario.



Allegati e macro pericolosi

Il malware elettronico arriva spesso sul computer tramite allegati di posta elettronica camuffati da presunte fatture o domande di lavoro. Gli allegati di posta elettronica potenzialmente dannosi dovrebbero quindi essere già bloccati dal gateway di posta elettronica o dal filtro antispam.

Un elenco dettagliato e aggiornato di tali allegati pericolosi è disponibile sul sito web del UFCS, <https://www.ncsc.admin.ch/govcert#1737483390>

Disattivate le macro di Office se non le utilizzate. Assicuratevi che nessuna macro possa essere eseguita in documenti Office di origine non sicura. Sensibilizzate i vostri dipendenti sul fatto che gli avvisi corrispondenti nei programmi Office non devono essere ignorati.

Suggerimento: il mio dispositivo è infetto da malware?

Avete il sospetto di aver scaricato un malware o che dei criminali informatici siano entrati nel vostro dispositivo? Prestate attenzione ai seguenti segnali di avvertimento:

- Ricevete messaggi, immagini o segnali sonori inaspettati;
- Il vostro programma antivirus segnala una minaccia;
- I programmi vengono aperti o stabiliscono una connessione a Internet da soli;
- I file scompaiono o vengono modificati;
- Vengono inviati messaggi dal vostro account a persone a voi vicine;
- Nella casella di posta elettronica sono presenti messaggi senza mittente o oggetto;
- Il computer è acceso, ma il sistema operativo non si avvia, è lento e/o si blocca;
- Il browser si blocca o sembra strano.



3.4 Salvate i vostri dati

Assicuratevi che i backup delle vostre informazioni siano eseguiti, gestiti e testati regolarmente (testate la riproducibilità dei backup).

Conservate una copia di backup aggiuntiva offline, ad esempio su un disco rigido esterno e al di fuori della sede. In questo modo, tra l'altro, è possibile garantire che, in caso di attacco ransomware e conseguente crittografia dei dati, sia disponibile una copia di backup funzionante. La conservazione dei dati al di fuori della sede è anche finalizzata a proteggerli da furti, incendi e inondazioni.

3.5 Siate pronti ad un attacco

Elaborate una strategia di gestione del rischio in caso di un evento. Definite le priorità, le limitazioni e i rischi massimi accettabili. Preparatevi al fatto che, in caso di incidente, per alcuni giorni non potrete erogare parte dei vostri servizi o dovrete fermare le vostre attività produttive. Procedure e percorsi di escalation ben definiti sono indispensabili per mantenere il controllo in caso di incidente. Organizzate esercitazioni di emergenza. Impostate un adeguato sistema di gestione delle crisi. Si raccomanda inoltre di avere un piano di comunicazione pubblica.

Anche la collaborazione con le imprese partner dovrebbe essere inclusa nelle vostre considerazioni sulla sicurezza.

La reazione a catena che potrebbe essere innescata da un attacco riuscito a un'impresa partner può mettere a rischio l'intera catena del valore e quindi anche la vostra azienda. I collaboratori devono essere sensibilizzati e informati sui possibili segnali di un incidente e devono sapere a chi segnalare eventuali osservazioni.

Per ulteriori informazioni sulla gestione strategica e operativa dei rischi, consultate il portale PMI della Confederazione: <https://www.kmu.admin.ch/>. L'Ufficio federale della protezione della popolazione ha elaborato una guida per la protezione delle infrastrutture critiche: <https://www.babs.admin.ch/it/compiti/protezionecivile/guida.html>. La guida si basa sulle norme e gli standard più comuni in materia di gestione dei rischi, di gestione delle emergenze, di gestione delle crisi e di gestione della sicurezza.



Suggerimento: inserire un contatto di sicurezza sul proprio sito web

In caso di problemi di sicurezza informatica, è molto importante che le autorità di polizia o i fornitori di servizi di sicurezza possano contattare rapidamente il contatto di sicurezza competente. Il nuovo standard "security.txt" offre la possibilità di pubblicare in modo uniforme il contatto di sicurezza sul proprio sito web e di trovarlo quindi più rapidamente. Sul sito web dell'Ufficio federale per la sicurezza informatica è disponibile una guida:



<https://www.ncsc.admin.ch/23-stxt-de>

3.6 Rimanete informati

Informatevi regolarmente sulle ultime strategie dei cybercriminali e imparate come proteggervi. Le seguenti pagine web vi tengono aggiornati:



Cybercrimepolice

www.cybercrimepolice.ch



**Bundesamt für
Cybersicherheit (BACS)**

www.ncsc.admin.ch



iBarry

www.ibarry.ch



Card Security

www.card-security.ch



**Schweizerische
Kriminalprävention (SKP)**

www.skppsc.ch



Ihre Polizei

www.fedpol.admin.ch

Assicuratevi che i vostri collaboratori ricevano regolarmente una formazione adeguata e a più livelli su tutti gli aspetti della sicurezza informatica. Non dimenticate i tirocinanti, i lavoratori in formazione e i collaboratori a tempo parziale. Spiegate loro l'importanza delle misure di sicurezza e il corretto utilizzo delle direttive definite, ad esempio la condivisione di informazioni o le regole per la gestione delle password.

Suggerimento: a cosa i collaboratori possono fare attenzione



Non cliccate su allegati e link in messaggi sospetti (e-mail, SMS, app di messaggistica).



Non condividete informazioni e dati confidenziali tramite canali non personali o con persone sconosciute. Non concedete l'accesso al vostro computer.



Le connessioni Internet pubbliche (anche quelle protette da password) non sono generalmente sicure. Inviare informazioni confidenziali solo tramite connessioni protette da un Virtual Private Network (VPN) o tramite una connessione dati 3G/4G/5G in roaming.



Non lasciate mai incustoditi i vostri materiali, documenti o dispositivi.



Fate spegnere il vostro computer da un professionista della TIC dopo il lavoro. Altrimenti l'account amministratore rimane attivo.



Utilizzate password sicure, composte da almeno dodici caratteri, lettere maiuscole e minuscole, numeri e caratteri speciali, generati in modo casuale. Importante: ogni applicazione deve avere una password propria! Aggiungete alla vostra password un'autenticazione a due fattori, ad esempio un codice via SMS.

4_Cosa sarebbe da considerare nel caso di esternalizzazione dei servizi TIC

Se decidete di esternalizzare la vostra infrastruttura TIC e di farla gestire da una o più aziende esterne, trovate di seguito alcuni consigli. Tenete presente che la responsabilità non può essere esternalizzata o delegata. In caso di incidente, la vostra azienda potrebbe essere l'ultima in una catena di responsabilità.

Requisiti minimi

Già al momento dell'acquisizione di sistemi TIC integrati, è necessario effettuare controlli di sicurezza. Informatevi sulle condizioni generali di contratto (CGC) e sui requisiti relativi alla prestazione di servizi informatici. Tali requisiti devono essere parte integrante dei contratti stipulati con le aziende esterne di servizi TIC. Le disposizioni di legge in materia di obblighi di riservatezza per la manutenzione e la gestione di sistemi TIC da parte di terzi devono essere regolate e l'accesso non necessario a dati personali particolarmente sensibili deve essere vietato. Occorre inoltre effettuare verifiche e stipulare accordi con l'azienda che gestisce la conservazione dei dati (cloud provider).

Audit di sicurezza

L'esecuzione dei servizi previsti dal contratto deve essere controllata periodicamente in base a standard di audit riconosciuti, ad esempio in base a COBIT (Control Objectives for Information and Related Technology) dell'Information Systems Audit and Control Association (ISACA). Per questo motivo, è consigliabile avvalersi dei servizi di un ente di revisione indipendente. L'azienda di servizi TIC può anche sottoporsi a un audit ISAE 3402 Type 2 (International Standard on Assurance Engagements), noto anche come SOC-2 Report (Service Organization Control). L'ente di revisione valuta aspetti relativi alla sicurezza, alla disponibilità, all'integrità e alla riservatezza.

Qualifiche

Le certificazioni secondo standard riconosciuti di protezione dei dati e di sicurezza delle informazioni o i rapporti di controllo di terze parti indipendenti possono essere utili nella scelta del fornitore. Non è necessario scegliere solo partner certificati. Si consiglia di scegliere fornitori di servizi TIC che possano dimostrare di soddisfare i vostri requisiti e di garantire la disponibilità e la sicurezza richieste. Fate verificare o confermare questo da un ente indipendente.

Esistono molti standard e linee guida diversi. I fornitori di servizi TIC dovrebbero essere conformi e familiari con gli standard ISO 27001, ISO 22301, ISO 9001, ISO 14001 e NIST. Se si utilizzano altri standard, il fornitore deve dimostrare di essere conforme a questi ultimi. Se avete bisogno di un livello di protezione più elevato, dovete definire i vostri requisiti specifici.



Non esitate a chiedere spiegazioni se qualcosa vi sembra strano, anche se si tratta di un mittente conosciuto! Non chiamate il numero di telefono indicato nella mail sospetta. Cercate i dati di contatto sul sito web ufficiale, digitando l'indirizzo originale nel browser. Fate attenzione anche al pulsante "Rispondi": scrivete da nuovo l'indirizzo e-mail.



Segnalate eventuali comportamenti sospetti al vostro specialista TIC.

5_Come superare gli attacchi informatici

Se siete vittime di un attacco, dovete agire rapidamente. Ecco come procedere:



Isolare

Disconnettete immediatamente i sistemi infetti dalla rete. Ciò significa: staccare i cavi di rete dai dispositivi interessati e disattivare il WLAN.



Contattare

Contattate la vostra persona di riferimento per le TIC. Contattate la polizia locale. Se vi trovate in una situazione di emergenza, chiamate il numero di emergenza 112.

Discutete i passi successivi con la polizia. Riattivate i dispositivi e i sistemi interessati solo dopo che la polizia ha raccolto le prove. Informate i vostri partner commerciali e i vostri clienti dell'incidente, poiché potrebbero essere anch'essi interessati. Siate consapevoli dei vostri obblighi di notifica, ad esempio in materia di protezione dei dati.



Gestire

Attivate il vostro piano di gestione delle crisi. Riunite il comitato di crisi e affidate la comunicazione alle persone competenti.

5.1 Segnalate un incidente - con o senza danni

Incidenti con danni

In caso di attacco a sistemi TIC, di solito si verificano diverse infrazioni, ad esempio acquisizione di dati senza autorizzazione o accesso non autorizzato a un sistema di elaborazione dati, frode o estorsione.

In questo caso, contattate la polizia o il ministero pubblico e denunciate l'incidente.

Incidenti senza danni

Segnalate online al UFCS (report.ncsc.admin.ch) attacchi informatici o tentativi di frode senza danni.

Ogni segnalazione contribuisce a individuare le attività criminali su Internet e a reagire tempestivamente a eventuali ondate di attacchi. Tuttavia, le informazioni non ufficiali fornite al UFCS non possono essere utilizzate per un'accusa o in un procedimento giudiziario.

5.2 Perché vale la pena rivolgersi alla polizia

La polizia è consapevole della situazione delicata e stressante che si crea per un'azienda. Per questo motivo, cerca di agire in modo discreto e rapido. L'indagine è soggetta al segreto d'ufficio. La vostra infrastruttura non viene intaccata e l'eventuale attività in corso non viene disturbata. In caso d'attacco, la polizia cerca solo informazioni e tracce che siano utili per chiarire il reato.

Durante le indagini, riceverete informazioni importanti che vi aiuteranno a gestire più rapidamente l'evento o a impedire che informazioni aziendali preziose continuino a fuoriuscire. Saprete come hanno agito i criminali e dove si trovava la falla nella sicurezza. In caso di richiesta di riscatto, riceverete un'assistenza specializzata. Le misure di perseguimento penale vengono concordate con voi - potete coinvolgere in qualsiasi momento il vostro consulente legale.

In cambio, potete fornire alla polizia informazioni che aiutino a proteggere altre aziende: le conoscenze anonimizzate derivanti da procedimenti penali servono a ottimizzare le strategie di prevenzione e di lotta esistenti e a svilupparne di nuove.

6_Cercate supporto

Diverse istituzioni offrono informazioni pertinenti sulla sicurezza TIC, strumenti e / o supporto:

Corpi di polizia cantonali e comunali

Diversi corpi di polizia in Svizzera offrono informazioni qualificate sulla prevenzione della criminalità informatica. Se siete interessati, contattate l'ufficio competente del corpo di polizia di competenza.

Ufficio federale della cibersicurezza (UFCS)

L'Ufficio federale per la cibersicurezza, www.ncsc.ch, è il centro di competenza federale per la sicurezza TIC e quindi il primo punto di contatto per l'economia, l'amministrazione, le istituzioni educative e la popolazione in materia di questioni legate al cyberspazio. Se la vostra azienda fa parte delle infrastrutture critiche ma non è ancora membro dell'UFCS, contattate outreach@ncsc.ch.

Servizio informazioni della Confederazione (SIC)

Il SIC, in collaborazione con i servizi di informazione cantonali, aiuta le aziende, le università e le istituzioni di ricerca a informarsi, sensibilizzare e consigliare in materia di proliferazione e spionaggio (www.ndb.admin.ch o prophylax@ndb.admin.ch). Sul sito web del SIC è disponibile una brochure sul tema con le relative raccomandazioni di protezione.

Ufficio federale per l'approvvigionamento economico del Paese (UAE)

L'UAE ha elaborato standard minimi per le TIC e uno strumento di valutazione. Si raccomanda ai gestori di infrastrutture critiche di applicare lo standard minimo per le TIC. In linea di principio, gli standard offrono comunque un aiuto e indicazioni concrete per migliorare la propria resilienza TIC a qualsiasi azienda o organizzazione interessata. Lo strumento di valutazione vi consente di valutare il livello di attuazione delle misure di protezione o di farlo verificare da un'azienda esterna (audit). Lo strumento di valutazione è disponibile all'indirizzo: www.bwl.admin.ch.

Protezione dei dati

Dal 1° settembre 2023 in Svizzera è in vigore una nuova legge che tutela i dati della popolazione. In qualità di azienda, dovete adeguare il trattamento dei dati personali a queste disposizioni. Per il trattamento dei dati personali da parte di privati e di organi federali è competente l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), www.edoeb.admin.ch. Sul portale PMI della Confederazione www.kmu.admin.ch troverete informazioni sulla protezione dei dati.

Lo strumento di protezione dei dati e un elenco delle rispettive autorità di vigilanza sulla protezione dei dati sono disponibili sul sito web della Conferenza dei responsabili della protezione dei dati in Svizzera, www.privatim.ch.

7_Allegati

7.1 Checklist: valutazione rapida della sicurezza informatica

Questa checklist vi aiuta a rispondere alle domande più importanti per una protezione informatica minima.

Per ogni risposta "non chiaro" o "no", effettuate le necessarie verifiche.

Se avete esternalizzato la vostra TIC, verificate se i punti seguenti sono contemplati nel contratto con il fornitore di servizi.

Completate questa valutazione rapida della sicurezza informatica anche per eventuali società affiliate e per i fornitori centrali dell'azienda. Si consiglia inoltre di scambiare informazioni con i principali partner aziendali, poiché gli incidenti informatici possono avere ripercussioni sull'intera catena del valore.

Sul sito web dell'Ufficio federale dell'approvvigionamento economico www.bwl.admin.ch è disponibile uno strumento di valutazione dettagliato per i minimi standard TIC. Questo strumento vi permette di valutare il livello di implementazione delle misure di protezione o di farlo verificare da un'azienda esterna (audit). Verificate regolarmente i punti della checklist, poiché la sicurezza informatica è un compito permanente.

Verificate regolarmente i punti della lista di controllo, perché la cybersecurity è un compito continuo.

Organizzazione e processi	Si	No	Non chiaro
La vostra azienda ha designato un responsabile della sicurezza informatica?			
Avete già effettuato valutazioni dei rischi informatici?			
I rischi informatici principali sono stati identificati, monitorati e documentati?			
Sapete com'è la vostra infrastruttura TIC, ad esempio quali sono i vostri beni, il software, i sistemi TIC esterni pertinenti?			
Avete un piano di emergenza e un piano di comunicazione in caso di attacco informatico?			
L'accesso fisico all'infrastruttura informatica, ai server, alle reti e alle linee di trasmissione dei dati è protetto contro l'accesso di terzi?			
Sensibilizzazione dei collaboratori			
I collaboratori vengono regolarmente formati in materia di sicurezza informatica?			
I collaboratori che hanno accesso a dati sensibili o che sono incaricati di trasferire dati ricevono una formazione adeguata?			
I collaboratori sono a conoscenza delle direttive aziendali?			
Protezione dei dati			
L'azienda dispone di una direttiva interna sulla protezione dei dati / politica di sicurezza delle informazioni e i collaboratori sono a conoscenza di tale direttiva?			
Le attuali disposizioni in materia di protezione dei dati, archiviazione e trattamento dei dati vengono applicate in modo coerente e corretto?			

Controllo degli accessi e diritti	Si	No	Non chiaro
Avete un concetto di autorizzazioni e ruoli per i vostri collaboratori (accesso solo alle informazioni necessarie per la funzione)?			
Sono bloccati i diritti di amministratore locale sui posti di lavoro dei collaboratori?			
Avete una politica di password e utilizzate procedure di autenticazione forti?			
Rete protetta			
I singoli settori della vostra azienda, ad esempio personale e contabilità, sono separati (segmentazione della rete) e gli accessi sono regolamentati? Alternativa per le piccole imprese: utilizzate un computer o un sistema separato per i diversi settori, ad esempio ufficio, personale e e-banking?			
L'accesso esterno (accesso remoto) all'infrastruttura informatica, ai server e alla rete, nonché al cloud, è protetto nella vostra azienda (VPN, autenticazione a due fattori) e può essere disattivato in caso di non utilizzo (accesso controllato)?			
Nel programma di posta elettronica è definito quali allegati sono considerati potenzialmente pericolosi e l'esecuzione di macro nei documenti Office è regolamentata?			
State utilizzando software e/o hardware obsoleti che non sono più supportati ufficialmente con aggiornamenti di sicurezza?			
Installate tempestivamente le correzioni (patch e aggiornamenti di sicurezza) per i vostri sistemi TIC e software?			
Utilizzate un antivirus, un antispyware o una protezione equivalente da malware?			
Dispone di un processo per individuare le vulnerabilità nei vostri software o nei vostri sistemi TIC, in modo da poter adottare misure e trattare le questioni, ad esempio IPS, IDS, log server?			
Tutti i punti di accesso a Internet sono protetti da firewall?			
Utilizza reti wireless cifrate?			
Utilizza componenti di sicurezza web avanzate, come ad esempio un DNS filtering ("Domain Name System") e un web proxy?			
Backup			
I backup sono eseguiti, gestiti e testati (ripristino) regolarmente?			
Conservate una copia aggiuntiva del backup separatamente (offline) e al di fuori del centro dati (offsite, ad esempio in cloud, in una cassetta di sicurezza bancaria)?			
Utilizzate un servizio di directory separato per il backup?			
Contratto con il fornitore di servizi IT e cloud			
La responsabilità in caso di danni e le esclusioni di responsabilità, ad esempio in caso di forza maggiore, sono definite per contratto?			
I livelli di servizio per il funzionamento normale e di emergenza sono chiaramente definiti?			
La strategia di uscita è stata definita e definita per contratto, in particolare per le soluzioni cloud?			
Collaborazione con le autorità di polizia			
La persona responsabile e la persona di contatto in caso di incidente sono state definite e sono disponibili?			

7.2 Certificazioni, standard e linee guida

Esistono numerosi standard e certificazioni diversi, ciascuno con un proprio focus. A seconda delle proprie esigenze, si possono scegliere diversi standard o certificazioni. Alcuni esempi:

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 delle informazioni

ISO 27001, Sicurezza delle informazioni

ISO 27701, Ampliamento della ISO 27001 sulla protezione dei dati

ISO 30141, Architettura di riferimento per l'Internet delle cose (IoT), riservatez-

za dei dati trattati orientamento in conformità al regolamento della UE

2016/679,

Regolamento generale sulla protezione dei dati (GDPR)

NIST Cybersecurity Framework

Linee guida tecniche

EN 50173, Struttura di cablaggio

EN 50600, Centri dati

ANSI/TIA-942, Centri dati

IEC 62443, Requisiti tecnici per la norma industriale

Cloud

ISO 27017, Codice di condotta per i controlli di sicurezza delle informazioni

(basato ISO/IEC 27002, Guida alle misure di sicurezza delle informazioni)

ISO 27018, Codice di condotta per la protezione dei dati personali nel cloud

Altro (soprattutto per fornitori di Hardware)

ISO 9001, Gestione di qualità

ISO 14001, Gestione dell'ambiente

Linee guida per i mandatari

ISO 22300, Norme tecnologiche per la sicurezza e la resilienza

ISO 22318, Supply Chain Continuity

ISO 27036, Sicurezza delle informazioni nella gestione dei fornitori

ISO 31010, Risikomanagement

Ci sono attori che offrono certificazioni senza accreditamenti.

Il servizio di accreditamento svizzero SAS valuta e accredita i seguenti tipi di organismi di valutazione della conformità.



(KBS). Qui si può cercare quale servizio di accreditamento è ammesso per quale norma: [Cerca organismi di valutazione accreditati SAS.](#)



Disponibile su:

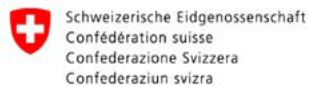
<https://cybercrimepolice.ch/CyberdelikteKMU>

Impressum

Contenuto: Polizia cantonale di Berna, Servizio progetti e cybercrime, su incarico della Rete di supporto alle indagini per la lotta alla criminalità digitale (NEDIK). In collaborazione con l'Ufficio federale per la cybersicurezza (BACS) e l'Ufficio federale per l'approvvigionamento economico del Paese (BWL).

Progettazione e layout: NEDIK.

Traduzione in italiano: Dipartimento delle istituzioni del Canton Ticino



Bundesamt für wirtschaftliche Landesversorgung
BWL

Bundesamt für Cybersicherheit BACS