Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Guida alla sicurezza informatica per le piccole imprese

Complessità dei contenuti
SEMPLICE ●○○

cyber.gov.au

Introduzione

Per una piccola impresa, anche un piccolo incidente di sicurezza informatica può avere un impatto devastante.
Questa guida contiene misure di sicurezza basilari per proteggere la tua azienda dalle più comuni minacce di sicurezza informatica. Come punto di partenza, raccomandiamo le seguenti tre misure:

- Attivazione dell'autenticazione a più fattori
- Aggiornamento dei software
- Back up delle informazioni

Questa guida potrebbe includere misure non rilevanti per la tua azienda, oppure la tua azienda potrebbe avere esigenze più complesse. Dopo aver completato questa guida, consigliamo alle piccole imprese di implementare il Primo Livello di Maturità delle **Otto Misure Essenziali**.
In caso di dubbi su questi consigli o sulla sicurezza informatica in generale, consigliamo di rivolgerti a un professionista del settore informatico o a un consulente di fiducia.

Visita il sito cyber.gov.au per consultare la nostra guida completa, che include consigli su come implementare ogni misura.

Indice dei contenuti

Minacce per le piccole imprese

Messaggi di truffa

Le truffe sono un modo comune con cui i criminali informatici prendono di mira le piccole imprese. Il loro scopo è quello di convincere il personale aziendale a:

- inviare denaro o buoni regalo
- cliccare su link o allegati potenzialmente dannosi
- fornire informazioni sensibili, come le password.

I criminali informatici possono tentare di truffare la tua azienda attraverso e-mail, messaggi di testo, telefonate e social media. Spesso fingono di essere una persona o un'organizzazione di cui si ha fiducia.

Attacchi di phishing

Particolarmente preoccupanti per le piccole imprese sono gli **attacchi di phishing**. Queste truffe spesso contengono un link a un sito web falso in cui si viene invitati ad accedere a un account o a inserire dati riservati.

Generalmente, gli attacchi di phishing compromettono le password degli account. I criminali informatici utilizzano spesso questo metodo per "impossessarsi" degli account dei social media delle piccole imprese e chiedere poi un riscatto.

Modi per ridurre i rischi

Se un messaggio proviene da un'entità nota e sembra sospetto, bisogna fare attenzione. Contatta la persona o l'azienda separatamente per verificare la legittimità del messaggio. Utilizza dati di contatto reperiti da una fonte legittima, ad esempio visitando il sito web ufficiale dell'azienda, e non quelli contenuti nel messaggio sospetto.

Per saperne di più sull'identificazione di truffe e sugli attacchi di phishing, è possibile consultare le seguenti risorse:

- Riconoscere e segnalare le truffe
- Imparare a riconoscere le truffe di phishing
- Rilevare i messaggi di ingegneria sociale.

Studio di caso:

Una dipendente di una società di corrieri ha ricevuto un'e-mail da uno dei suoi dirigenti, che le chiedeva di acquistare 6 carte di credito prepagate MasterCard da 500 dollari ciascuna. Il dirigente ha chiesto alla dipendente di mantenere la riservatezza, in quanto le carte sarebbero state dei buoni regalo per i membri del personale. Una volta acquistate, alla dipendente è stato chiesto di fotografare entrambe le facciate delle carte e di inviarle al dirigente come prova d'acquisto.

Come da istruzioni, la dipendente si è recata in un ufficio postale e ha utilizzato la sua carta di credito personale per acquistare le carte regalo. Ha risposto all'e-mail del dirigente e ha inviato le foto delle carte regalo come prova.

Al ritorno dall'ufficio postale, la dipendente ha consegnato le carte al dirigente, che però non era a conoscenza di nulla. Da un esame effettuato, **risulta poi che tutte le e-mail relative alle carte regalo provenivano da un indirizzo e-mail casuale e non dall'account e-mail legittimo del dirigente. Si trattava di una truffa.**

Attacchi via e-mail

Oltre alle truffe come il phishing, un attacco e-mail comune contro le piccole imprese è la **compromissione dell'e-mail aziendale** (Business email compromise - BEC). I criminali possono spacciarsi per rappresentanti di aziende utilizzando account di posta elettronica compromessi o con altri mezzi, come l'utilizzo di un nome di dominio simile a quello di un'azienda reale. Oltre a rubare informazioni, l'obiettivo di questi attacchi è di solito quello di truffare le vittime per indurle a inviare fondi a un conto bancario gestito dal truffatore.

Modi per ridurre i rischi

La migliore difesa contro gli attacchi via e-mail è la formazione e la sensibilizzazione dei dipendenti. Assicurati che i tuoi collaboratori sappiano essere sempre prudenti nei confronti delle e-mail che contengono:

- richieste di pagamento, soprattutto se urgenti o scadute
- modifiche di coordinate bancarie
- un indirizzo e-mail che non sembra corretto, ad esempio il nome del dominio non corrisponde esattamente alla ragione sociale del fornitore.

Sebbene questi attacchi possano essere devastanti, le misure di mitigazione dei rischi sono semplici e non costano quasi nulla. **Quando il personale riceve e-mail di questo tipo, la soluzione più efficace è quella di chiamare il mittente per avere conferma della legittimità dell'invio.** Non si devono utilizzare i dati di contatto che sono stati inviati nell'e-mail perché potrebbero essere fraudolenti. Si può inoltre introdurre un procedimento formale che il personale deve seguire quando si ricevono richieste di pagamento o si modificano le coordinate bancarie.

Per imparare a proteggere la tua azienda dalle truffe BEC e dalla compromissione delle e-mail, utilizza le seguenti risorse:

- Compromissione dell'e-mail aziendale
- Proteggi la tua azienda dalle frodi e dalle truffe via e-mail
- Cosa fare se la tua azienda è stata presa di mira da frodi o truffe via e-mail.

Studio di caso:

Una piccola impresa edile ha ricevuto un'e-mail dal suo fornitore che le comunicava di aver cambiato banca. Il fornitore ha fornito nuovi dettagli del conto per il pagamento delle fatture. Poiché l'e-mail sembrava legittima, **l'impresa edile non ha chiamato il fornitore per confermare la modifica delle coordinate bancarie.**

L'azienda ha pagato una fattura del fornitore per oltre 70.000 dollari. Il giorno successivo, un altro dipendente ha erroneamente pagato la stessa fattura per un ulteriore importo superiore a 70.000 dollari. In totale, oltre 150.000 dollari sono stati versati sul nuovo conto bancario.

Quando l'azienda ha telefonato al proprio fornitore per chiedere se poteva rimborsare il doppio pagamento, il fornitore ha comunicato che i dati bancari non erano corretti. Un'indagine è stata immediatamente avviata e il fornitore ha scoperto che uno dei suoi account di posta elettronica era stato violato e stava inviando dati bancari fraudolenti. **Nessuna somma di denaro è stata recuperata.**

Software dannoso

Malware è un termine generico che indica software dannosi progettati per causare danni, come ransomware, virus, spyware e trojan. Il malware può:

- rubare o bloccare i file su un dispositivo
- rubare numeri bancari o delle carte di credito
- rubare nomi utente e password
- prendere il controllo o spiare un computer.

Il malware può impedire a un dispositivo di funzionare correttamente, cancellare o corrompere i file o consentire ad altri di accedere a informazioni personali o aziendali. Se il tuo dispositivo è infettato da malware, potresti essere vulnerabile ad altri attacchi. Il malware potrebbe anche diffondersi ad altri dispositivi della tua rete.

Un dispositivo può essere infettato da malware in diversi modi, tra cui:

- visitando siti web che sono stati infettati da malware
- scaricando file o software infetti da Internet
- aprendo allegati di posta elettronica infetti.

Ransomware

Il ransomware è un tipo di malware comune e pericoloso. Funziona bloccando o crittografando i file in modo da non potervi più accedere. Per ripristinare l'accesso ai file viene richiesto un riscatto (ransom), solitamente sotto forma di criptovaluta. I criminali informatici potrebbero anche minacciare di pubblicare o vendere i dati online, a meno che non venga pagato un riscatto.

Modi per ridurre i rischi

Anche se gli antivirus o i software di sicurezza possono aiutare a proteggersi dalle minacce informatiche, nessun software è efficace al 100%. Il personale deve prestare attenzione a e-mail, siti web e download di file e aggiornare regolarmente i propri dispositivi per continuare a garantire la sicurezza.

Per ulteriori informazioni sulla protezione della tua azienda dal ransomware, consulta le seguenti risorse:

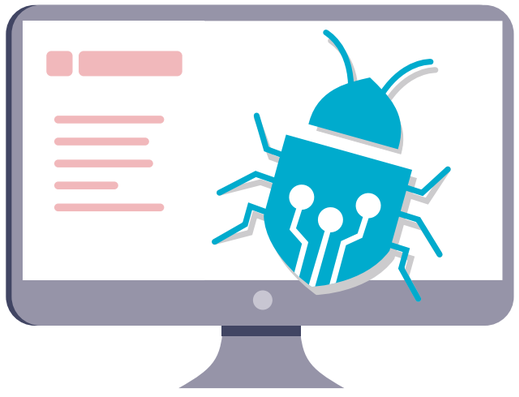
- Ransomware
- Proteggersi dagli attacchi ransomware
- Cosa fare se è stato richiesto un riscatto.

Studio di caso:

Una mattina, i dipendenti di un negozio di ricambi auto si sono presentati al lavoro e non sono riusciti ad avviare il computer del server. Quando il loro provider ha avuto accesso al server, ha trovato una finestra aperta che li informava che tutti i dati del computer erano stati criptati. La nota chiedeva di pagare un riscatto in bitcoin per sbloccare i file.

Al computer era collegata un'unità di backup, anch'essa crittografata dai criminali informatici. Hanno provato a collegare altre unità di backup, ma i file sono stati automaticamente crittografati in pochi secondi. **Non sono riusciti a rimuovere il ransomware prima di tentare di recuperare i loro dati e hanno perso tutti i file di backup che avevano.**

L'unica opzione rimasta era quella di resettare il server e ripartire da zero con un nuovo sistema. L'azienda ha perso molti anni di dati e ha dovuto ricominciare da capo.



Sicurezza degli account

Attivazione dell'autenticazione a più fattori

L'autenticazione a più fattori (MFA) rende più difficile ai criminali informatici l'accesso ai tuoi account.

L'MFA aggiunge un ulteriore livello di sicurezza al tuo account. Si tratta di uno dei metodi più efficaci per proteggere i tuoi account dall'accesso di terze persone, quindi dovresti adottarlo ogni volta che è possibile. Chiunque acceda al tuo account dovrà fornire un'altra informazione oltre al nome utente e alla password. Si potrebbe trattare di un codice univoco proveniente da un messaggio di testo o da un'app di autenticazione. Per ulteriori informazioni, leggi i nostri consigli sull'MFA, disponibili all'indirizzo **cyber.gov.au/mfa**.

✓ **Attiva l'MFA ogni volta che è possibile, a partire dagli account più importanti.**

Implementazione di controlli di accesso

Limitare l'accesso degli utenti può limitare i danni causati da un incidente di sicurezza informatica.

Il controllo degli accessi è un modo per limitare l'accesso a determinati file e sistemi. In genere, il personale non ha bisogno di accedere a tutti i dati, a tutti gli account e a tutti i sistemi di un'azienda. Dovrebbero pertanto poter accedere solo a ciò che è necessario per svolgere le loro mansioni.

La limitazione dell'accesso contribuirà a limitare i danni causati da un incidente di sicurezza informatica. Ad esempio, se il computer di un membro del personale viene infettato da un ransomware, con un adeguato controllo degli accessi il problema potrebbe riguardare solo un piccolo numero di file piuttosto che l'intera azienda.

✓ **Assicurati che ogni utente possa accedere solo a ciò che gli serve per svolgere il suo ruolo.**

Utilizzo di password o frasi d'accesso complesse

Proteggi i tuoi account dai criminali informatici utilizzando una password o una frase d'accesso sicura.

Molte piccole imprese subiscono attacchi informatici a causa di comportamenti scorretti in materia di password. Ad esempio, il riutilizzo della stessa password per più account. Per creare password complesse si possono usare sia i gestori di password che le frasi di accesso.

Un **gestore di password** agisce come una cassaforte virtuale per le tue password. È possibile utilizzarlo per creare e memorizzare password complesse e **uniche** per ogni account. Se si dispone di molti account, questo elimina l'onere di ricordare password diverse per ciascuno. Non è necessario ricordare le password o gli account a cui appartengono, poiché tutto viene registrato nel gestore di password.

Per gli account a cui si accede regolarmente o che non si desidera memorizzare in un gestore di password, consigliamo di utilizzare una frase d'accesso come password. Le frasi d'accesso sono una combinazione di parole casuali, ad esempio "cristallo, cipolla, argilla, pretzel". Sono utili quando si desidera adottare una password sicura e facile da ricordare. Utilizza una combinazione casuale di quattro o più parole e mantienila unica - **non riutilizzare una frase d'accesso** per più account. Per maggiori informazioni, consigliamo di leggere i nostri consigli su frasi d'accesso e gestori di password, disponibili all'indirizzo **cyber.gov.au/passphrases**.

✓ **Utilizza un gestore di password per creare e memorizzare password uniche per ogni account importante.**

Gestione degli account condivisi

La condivisione degli account può compromettere la sicurezza e rende difficile tracciare le attività dannose.

In un'azienda di piccole dimensioni, ci possono essere ragioni legittime per cui il personale deve condividere gli account, ma questo dovrebbe essere evitato il più possibile. Quando più persone utilizzano lo stesso account, può essere difficile risalire a un dipendente specifico e ancor più difficile individuare i criminali informatici che si introducono nel sistema. Se non si cambia la password, i dipendenti potrebbero continuare ad accedere agli account anche dopo aver lasciato l'azienda.

✓ **Limita l'uso di account condivisi e proteggi tutti quelli utilizzati per la tua attività.**

Protezione dei dispositivi e delle informazioni

Aggiornamento dei software

Mantenere i software aggiornati è uno dei modi migliori per proteggere la propria azienda da un attacco informatico.

Gli aggiornamenti possono correggere le falle di sicurezza del sistema operativo e di altri software, in modo da rendere più difficile l'accesso ai criminali informatici. Nuove falle vengono scoperte in continuazione, quindi non ignorare le richieste di aggiornamento. L'aggiornamento regolare del software riduce la possibilità che un criminale informatico sfrutti una debolezza nota per introdurre malware o violare un dispositivo. Se hai bisogno di aiuto, l'ACSC ha pubblicato una guida sugli aggiornamenti.

Se il dispositivo o il software è troppo vecchio, gli aggiornamenti potrebbero non essere disponibili. Se il produttore ha smesso di supportare il prodotto con gli aggiornamenti, si dovrebbe prendere in considerazione l'aggiornamento a un prodotto più recente per rimanere al sicuro. Esempi di sistemi che non ricevono più aggiornamenti importanti sono l'**iPhone 7** e **Microsoft Windows 7**.

Per maggiori informazioni, consigliamo di leggere la nostra guida sugli aggiornamenti, disponibile all'indirizzo **cyber.gov.au/updates**.

✓ **Attiva gli aggiornamenti automatici per i dispositivi e i software.**

Utilizzo di un software di sicurezza

Un software di sicurezza come un antivirus e una protezione ransomware possono aiutare a proteggere i tuoi dispositivi.

Utilizza un software di sicurezza per rilevare e rimuovere il malware dai tuoi dispositivi. Il software antivirus può essere impostato per eseguire regolarmente una scansione alla ricerca di file e programmi sospetti. Quando viene individuata una minaccia, si riceve un avviso e il file sospetto viene messo in quarantena o rimosso.

Molte piccole imprese possono **utilizzare Windows Security** per proteggersi da virus e malware. Windows Security è integrato nei dispositivi Windows 10 e Windows 11 e include una protezione gratuita da virus e minacce. Si può anche utilizzare per attivare le funzioni di protezione contro i ransomware su un dispositivo.

Per prodotti e opzioni alternative, consigliamo di leggere i nostri consigli sul software antivirus, cercando *antivirus* su cyber.gov.au.

✓ **Imposta un software di sicurezza per eseguire scansioni regolari sui tuoi dispositivi.**

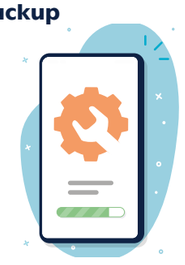
Backup delle informazioni

I backup regolari possono aiutare a recuperare le informazioni in caso di perdita o compromissione.

Il backup delle informazioni importanti dovrebbe essere una pratica regolare o automatica all'interno di qualsiasi azienda. Senza un backup regolare, potrebbe essere impossibile recuperare le proprie informazioni in seguito a un attacco informatico.

Esistono molti metodi e prodotti da utilizzare per il backup delle informazioni. Per consigli dettagliati sul backup aziendale, consigliamo di leggere i nostri consigli per i backup, disponibili all'indirizzo **cyber.gov.au/backups**. L'opzione migliore varia da un'azienda all'altra, quindi è bene rivolgersi a un professionista informatico in caso di dubbi.

✓ **Crea e attua un piano per eseguire regolarmente il backup delle tue informazioni.**



Protezione della rete e dei servizi esterni

Proteggi la tua azienda da un attacco informatico risolvendo le potenziali vulnerabilità della tua rete.

I dispositivi e i servizi della tua rete possono essere un obiettivo primario per i criminali informatici. Molti di questi sistemi possono essere complessi da proteggere, quindi è bene discutere le seguenti raccomandazioni con un professionista informatico.

- **Protezione dei server**: Se si utilizza un NAS (Network Attached Storage) o un altro server a casa o in azienda, è necessario prestare particolare attenzione alla sua protezione. Questi dispositivi sono obiettivi abituali per i criminali informatici in quanto spesso memorizzano file importanti o svolgono funzioni importanti. Sono molte le strategie di mitigazione necessarie per proteggere questi dispositivi. Ad esempio, è importante assicurarsi che i dispositivi server o NAS siano aggiornati regolarmente. Gli account amministrativi devono essere protetti con una frase d'accesso complessa o tramite l'autenticazione a più fattori.
- **Minimizza la presenza verso l'esterno**: Verifica e proteggi tutti i servizi esposti a Internet sulla tua rete. Questo potrebbe includere la funzione di desktop remoto, la condivisione di file, Webmail e i servizi di amministrazione remota.
- **Migra i tuoi dati sui servizi cloud:** Considera l'utilizzo di servizi online o cloud che offrono una sicurezza integrata, invece di doverne gestirne una propria. Ad esempio, utilizza servizi online per la posta elettronica o l'hosting di siti web piuttosto che gestire e proteggere questi servizi da soli.
- **Migliora la sicurezza del router:** Consigliamo di seguire le nostre indicazioni sui modi per proteggere il router, tra cui l'aggiornamento delle password predefinite, l'attivazione del Wi-Fi "ospite" per i clienti o i visitatori e l'utilizzo dei protocolli di crittografia più potenti. Per ulteriori informazioni, è possibile cercare *router* su **cyber.gov.au**.
- **Impara il funzionamento della catena di approvvigionamento informatico (cyber supply chain):** Le aziende moderne spesso esternalizzano più servizi. Ad esempio, utilizzando un Fornitore di servizi gestiti (Managed Service Provider) per la manutenzione dei sistemi elettronici. I problemi di sicurezza di questi servizi o provider potrebbero avere un impatto significativo sulla tua azienda. Per consigli dettagliati sulla gestione del rischio della catena di approvvigionamento informatico, consigliamo di leggere la nostra Guida alla Cyber Supply Chain su **cyber.gov.au**.

✓ **Rivolgiti a un professionista informatico per conoscere le modalità di protezione della tua rete.**

Rafforzamento del tuo sito web

I siti web sono un obiettivo principale per gli attacchi informatici.

Proteggi il tuo sito web seguendo alcune misure di sicurezza di base:

- proteggi l'accesso al tuo sito web con l'autenticazione a più fattori o con una password complessa
- aggiorna regolarmente i sistemi di gestione dei contenuti e i plugin del sito web
- esegui regolarmente il backup del tuo sito web in modo da poterlo ripristinare dopo un attacco informatico.

L'ACSC mette a disposizione ulteriori risorse per i proprietari di siti web. È possibile cercare queste risorse su **cyber.gov.au**:

- Azioni immediate per il tuo sito web
- Implementazione di certificati, TLS, HTTPS e TLS opportunistico
- Sicurezza del sistema dei nomi di dominio per i proprietari di domini
- Preparazione e risposta agli attacchi di negazione del servizio (Denial-of-Service)

✓ **Consigliamo di leggere le risorse dell'ACSC sulla sicurezza dei siti web.**

Ripristino alle impostazioni di fabbrica dei dispositivi prima della vendita o dello smaltimento

I dati presenti sui tuoi vecchi dispositivi potrebbero essere accessibili a estranei.

Se non si smaltiscono i dispositivi in modo sicuro, i criminali informatici potrebbero accedere alle informazioni in essi contenute. Ciò potrebbe includere e-mail, file e altri dati aziendali. È necessario pertanto rimuovere tutte le informazioni dai dispositivi aziendali prima di venderli, scambiarli o gettarli via. Ad esempio, eseguendo un ripristino delle impostazioni di fabbrica. Questo aiuterà a cancellare tutte le informazioni e a ripristinare le impostazioni originali del dispositivo.

Per consigli su come resettare i dispositivi, consigliamo di leggere la nostra guida su come smaltire un dispositivo in modo sicuro Cerca *dispose* su **cyber.gov.au**.

✓ **Esegui un ripristino delle impostazioni di fabbrica prima di vendere o smaltire i dispositivi aziendali.**

Protezione dei dispositivi tramite blocchi e salvaguardia fisica

Limitare l'accesso ai dispositivi aziendali riduce le opportunità di attività dannose.

Limitare l'accesso fisico ai dispositivi aziendali è un modo semplice per prevenire il furto di dati o altre attività dannose. I dispositivi aziendali non devono essere conservati in luoghi in cui il personale non autorizzato o i membri del pubblico potrebbero accedervi.

Utilizza i controlli di sicurezza per proteggere ulteriormente i tuoi dispositivi aziendali. Come minimo, devono essere bloccati con una frase d'accesso, un PIN o con un blocco biometrico. Assicurati che questi dispositivi siano impostati per bloccarsi automaticamente dopo un breve periodo di inattività.

✓ **Configura i dispositivi in modo che si blocchino automaticamente dopo un breve periodo di inattività.**

Protezione dei dati aziendali

I dati in possesso della tua azienda sono un bersaglio appetibile per i criminali informatici.

Le violazioni dei dati sono in aumento: non lasciare che la tua azienda ne sia vittima. È importante capire quali sono i dati in possesso della tua azienda e in quali luoghi. Una volta consapevole dei dati di cui disponi, puoi utilizzare i consigli contenuti in questa guida per proteggere i dati dall'accesso dei criminali informatici. Alcune piccole imprese possono anche avere obblighi aggiuntivi in base alla legislazione.

- **Consolida i dati aziendali.** È possibile che i dati siano archiviati su numerosi dispositivi o servizi. Quando i dati sono decentralizzati, aumenta il numero di sistemi da tenere al sicuro e sottoposti a backup. L'utilizzo di numerosi sistemi può creare maggiori opportunità di attacco per un criminale informatico. Se possibile, conserva i dati aziendali in un luogo centrale, sicuro e con backup regolari. La centralizzazione dei dati può creare una violazione maggiore se i sistemi vengono compromessi, quindi assicurati che questo luogo centrale sia adeguatamente protetto con configurazioni sicure e accesso limitato. Consigliamo di rivolgerti a un professionista informatico o della sicurezza per avere ulteriori consigli.
- **Conosci i tuoi obblighi in materia di protezione dei dati.** Alcune piccole imprese possono avere obblighi legali per il trattamento dei dati personali che raccolgono. Per saperne di più, consigliamo di leggere la guida dell'Office of the Australian Information Commissioner per le piccole imprese, disponibile all'indirizzo **oaic.gov.au**. Se in dubbio, consigliamo di rivolgerti a un professionista legale.

✓ **Sii consapevole dei dati in possesso della tua azienda e delle tue responsabilità nel proteggerli.**

Preparazione del personale aziendale

Educazione dei dipendenti

I dipendenti con buone pratiche di sicurezza informatica rappresentano la prima linea di difesa contro gli attacchi informatici.

I dipendenti devono essere consapevoli dell'importanza della sicurezza informatica, compresi i seguenti argomenti:

- minacce comuni alla sicurezza informatica, come la compromissione della posta elettronica aziendale e il ransomware
- misure di protezione, tra cui password o frasi di accesso complesse, MFA e aggiornamenti dei software
- come riconoscere le truffe e gli attacchi di phishing
- linee di condotta specifiche per l'azienda (ad esempio, processi per la segnalazione di e-mail sospette o per la verifica dell'autenticità delle fatture prima del pagamento)
- cosa fare in caso di emergenza.

Il sito web dell'ACSC contiene risorse riguardanti la maggior parte di questi argomenti all'indirizzo cyber.gov.au/learn. Si possono prendere in considerazione altri modi per formare il proprio personale, ad esempio con un corso formale o una formazione interna. Qualunque sia la decisione, ricorda che la formazione sulla sicurezza informatica non è un requisito una tantum e deve essere aggiornata periodicamente.

✓ **Stabilisci come la consapevolezza della sicurezza informatica verrà insegnata all'interno della tua azienda.**

Predisposizione di un piano di emergenza

Un piano di emergenza potrebbe ridurre l'impatto di un attacco informatico sulla tua azienda.

Quando si risponde a un incidente di sicurezza informatica, ogni minuto è importante. Disporre di un piano di emergenza significa che il personale può dedicare meno tempo a capire cosa fare e più tempo ad agire.

Nel creare il piano di emergenza bisogna prendere in considerazione le seguenti domande:

- Qual è il procedimento che consente al personale di segnalare potenziali incidenti di sicurezza informatica?
- A chi ci si può rivolgere per ottenere assistenza? Ad esempio, i professionisti informatici e la tua banca.
- Come verrà comunicato l'incidente al personale, ai soggetti interessati o ai clienti?
- Come si gestirà l'attività ordinaria se qualche sistema critico è offline?

Bisogna assicurarsi che il personale conosca il piano di emergenza, compresi i ruoli e le responsabilità che può avere. Conserva una copia cartacea del piano nel caso in cui i tuoi sistemi siano offline quando ne hai bisogno.

✓ **Crea un piano di emergenza per gli incidenti di sicurezza informatica.**

Rimanere informati

Diventa un partner dell'ACSC per ricevere le informazioni più recenti da parte dell'ACSC.

Resta al corrente delle ultime minacce e vulnerabilità informatiche diventando un partner di ACSC. Questo servizio invierà newsletter mensili e avvisi ogni volta che viene identificata una nuova minaccia informatica.

La sicurezza informatica è un campo in rapida evoluzione. I criminali informatici sfruttano attivamente le vulnerabilità entro pochi minuti dalla loro scoperta. Rimanere informati sul panorama della sicurezza informatica aiuterà la tua azienda a capire quali sono le minacce che probabilmente dovrà affrontare e come proteggersi.

✓ **Registra la tua azienda con il Programma di partenariato ACSC.**

Dichiarazione di non responsabilità

Il materiale contenuto in questa guida è di carattere generale e non deve essere considerato come consulenza legale o utilizzato per assistenza in particolari circostanze o situazioni di emergenza. Per qualsiasi questione importante, è necessario richiedere un'adeguata consulenza professionale indipendente in relazione alla propria situazione.

Il Commonwealth non si assume alcuna responsabilità per eventuali danni, perdite o spese sostenute in conseguenza dell'affidamento alle informazioni contenute in questa guida.

Per ulteriori informazioni o per segnalare un incidente di sicurezza informatica, contattaci:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Questo numero è disponibile solo per coloro che chiamano dall'Australia.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre