

```
digit separator = '_' is used for the IFormat  
'N' format string: 1_18_76,54  
'E' format string: 1,187654E+004  
Press any key to continue . . . -
```

BRAINCOMPUTING

**Cybersecurity per le PMI:
Come proteggere il tuo business digitale**

CONTENTS

INTRODUZIONE ALLE MINACCE
INFORMATICHE PER LE PMI

| 01

VALUTAZIONE DEI RISCHI E
PIANIFICAZIONE DELLA SICUREZZA

| 02

SICUREZZA DELLE RETI
E DEI SISTEMI INFORMATICI

| 03

GESTIONE DELLE CREDENZIALI
E AUTENTICAZIONE DEGLI ACCESSI

| 04

SICUREZZA DEI DATI
E DELLA PRIVACY

| 05

06

SENSIBILIZZAZIONE ALLA SICUREZZA
E FORMAZIONE DEI DIPENDENTI

07

GESTIONE DELLE MINACCE INTERNE

08

RISPOSTA AGLI INCIDENTI E
PIANIFICAZIONE DELLA CONTINUITÀ
AZIENDALE

09

COLLABORAZIONE CON FORNITORI
DI SERVIZI DI SICUREZZA E
CONSULENTI ESTERNI

10

ULTERIORI RISORSE E STRUMENTI PER
LA CYBERSECURITY DELLE PMI

11

CONCLUSIONI

INTRODUZIONE ALLE MINACCE INFORMATICHE PER LE PMI

Le piccole e medie imprese (PMI) sono spesso viste come target meno attraenti per gli hacker rispetto alle grandi aziende, ma in realtà rappresentano un obiettivo sempre più allettante per i cybercriminali.

Le PMI hanno spesso meno risorse per dedicare alla sicurezza informatica rispetto alle grandi aziende, e ciò le rende più vulnerabili alle minacce informatiche. Inoltre, spesso non sono adeguatamente informate sui rischi e le conseguenze delle violazioni della sicurezza.

Le minacce cibernetiche per le PMI possono assumere diverse forme. I fenomeni più noti, tuttavia, sono: phishing, ransomware, attacchi DDoS e malware. Le attività di phishing, ad esempio, coinvolgono l'invio di email fraudolente che cercano di ingannare e spingere i destinatari a condividere informazioni personali o di login. Il ransomware, invece, è un tipo di malware che blocca l'accesso ai dati dell'azienda e richiede un riscatto per sbloccarli.

Le conseguenze finanziarie delle violazioni della sicurezza possono essere molto gravi per le PMI. Potrebbero dover affrontare costi per la riparazione dei sistemi compromessi, il ripristino dei dati e la perdita di produttività. Inoltre, le violazioni della sicurezza possono causare danni alla reputazione dell'azienda e perdita di clienti.

Per queste ragioni, è essenziale che le PMI adottino misure di sicurezza informatica appropriate al fine di proteggere la propria attività digitale. Solo una pianificazione efficace della sicurezza informatica e la sensibilizzazione dei dipendenti sui rischi possono aiutare a ridurre il rischio di violazioni della sicurezza e minimizzare l'impatto in caso di incidenti.

VALUTAZIONE DEI RISCHI E PIANIFICAZIONE DELLA SICUREZZA

Per proteggere adeguatamente il tuo business digitale, è fondamentale effettuare una valutazione dei rischi e pianificare una strategia di sicurezza informatica. Di seguito sono riportati i passaggi chiave per guidarti in questo processo:

Identificazione dei principali asset digitali da proteggere:

- Fai un inventario di tutti i dati, le informazioni e i sistemi critici per il funzionamento della tua PMI.
- Identifica i dati sensibili, come informazioni personali dei clienti, dati finanziari o proprietari, che richiedono una protezione particolare.

Valutazione dei rischi specifici per la tua PMI:

- Analizza le minacce che potrebbero mettere a rischio i tuoi asset digitali. Ciò può includere minacce esterne come malware, attacchi di phishing o hacking, nonché minacce interne come errori umani o accessi non autorizzati da parte dei dipendenti.
- Valuta la probabilità di queste minacce e l'impatto che potrebbero avere sul tuo business, sia in termini finanziari che reputazionali.

Pianificazione e implementazione di una strategia di sicurezza informatica:

- Definisci gli obiettivi di sicurezza che desideri raggiungere per proteggere i tuoi asset digitali.

Identifica le misure di sicurezza appropriate per mitigare i rischi identificati. Queste possono includere l'implementazione di soluzioni antivirus, firewall, crittografia dei dati, accesso controllato e procedure di backup regolari.

- Sviluppa politiche e procedure di sicurezza per i tuoi dipendenti, come l'uso di password complesse, l'autenticazione a più fattori e la sensibilizzazione sulla sicurezza informatica.
- Assegna responsabilità chiare per la gestione della sicurezza informatica all'interno dell'azienda.
- Stabilisci un piano di risposta agli incidenti che includa procedure per la gestione di violazioni o compromissioni della sicurezza.

Ricorda che la sicurezza informatica è un processo continuo e richiede attenzione e aggiornamento costanti. Mantieni la tua strategia di sicurezza informatica aggiornata, monitora costantemente le minacce emergenti e adatta le misure di sicurezza in base alle nuove sfide che potrebbero sorgere



SICUREZZA DELLE RETI E DEI SISTEMI INFORMATICI

Per garantire la sicurezza delle reti e dei sistemi informatici della tua PMI, ecco alcuni strumenti e best practice che puoi adottare:

Protezione delle reti aziendali:

- Configura e gestisci una rete sicura, utilizzando password forti per i dispositivi di rete e limitando l'accesso solo ai dipendenti autorizzati.
- Utilizza reti virtuali private (VPN) per crittografare il traffico di rete e garantire la sicurezza delle comunicazioni remote.
- Implementa la segmentazione di rete per limitare l'accesso ai dati sensibili solo ai dipendenti autorizzati.

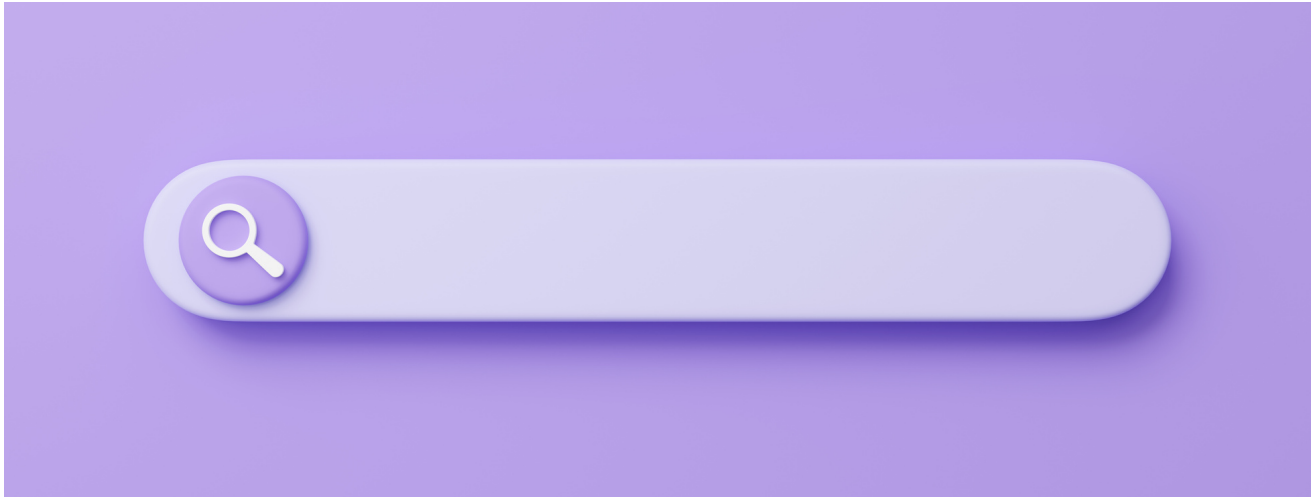
Protezione dei sistemi operativi e delle applicazioni:

- Mantieni sempre aggiornati i sistemi operativi, gli aggiornamenti di sicurezza e le patch dei software. Le vulnerabilità non corrette possono essere sfruttate dagli attaccanti.
- Utilizza software legittimo e con licenza, scaricando le applicazioni solo da fonti affidabili.
- Limita i privilegi degli account degli utenti, assegnando solo le autorizzazioni necessarie per svolgere le loro mansioni.

Utilizzo di firewall, antivirus e software di rilevamento delle intrusioni:

- Installa e configura un firewall per monitorare e controllare il traffico di rete in entrata e in uscita per impedire l'accesso non autorizzato alla tua rete.

- Utilizza un software antivirus affidabile e aggiornato per proteggere i sistemi da malware, spyware e altre minacce.
- Considera l'implementazione di un sistema di rilevamento delle intrusioni (IDS) o di un sistema di prevenzione delle intrusioni (IPS) per identificare e rispondere alle attività sospette o agli attacchi in tempo reale.



È importante monitorare costantemente la sicurezza delle reti e dei sistemi informatici, eseguire scansioni regolari per identificare e risolvere le vulnerabilità, nonché adottare politiche di backup dei dati per garantire la disponibilità delle informazioni anche in caso di incidente di sicurezza.

GESTIONE DELLE CREDENZIALI E AUTENTICAZIONE DEGLI ACCESSI

La gestione delle credenziali e l'autenticazione degli accessi sono due aspetti critici della sicurezza informatica, in quanto rappresentano il primo livello di difesa contro eventuali attacchi informatici.

La gestione delle credenziali riguarda la creazione, l'assegnazione e la gestione di password e altri metodi di autenticazione per accedere a sistemi, applicazioni e dati sensibili. È importante che le password siano robuste e complesse, utilizzando una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Inoltre, è consigliabile utilizzare l'autenticazione a due fattori o multi-fattore per migliorare la sicurezza delle credenziali.

L'autenticazione degli accessi è il processo di verifica dell'identità dell'utente che richiede l'accesso a sistemi, applicazioni e dati sensibili. Ci sono diversi metodi di autenticazione, come l'autenticazione basata su password, l'autenticazione a due fattori, l'autenticazione biometrica e l'autenticazione a certificato digitale. È importante scegliere il metodo di autenticazione più adatto alle esigenze della propria azienda.

Inoltre, è fondamentale garantire una corretta gestione delle credenziali e dell'autenticazione degli accessi per ridurre il rischio di attacchi informatici, in particolare quelli basati sull'ingegneria sociale o sul furto di identità. La formazione dei dipendenti è un aspetto cruciale per sensibilizzare i membri dell'azienda sulla corretta gestione delle credenziali e dell'autenticazione degli accessi, al fine di prevenire violazioni della sicurezza e perdite di dati sensibili.



Infine, l'implementazione di strumenti di gestione delle credenziali e di autenticazione degli accessi può aiutare le PMI a garantire la sicurezza dei propri dati e a mitigare il rischio di eventuali attacchi informatici. Ci sono diversi software e soluzioni di sicurezza disponibili sul mercato che possono essere adattati alle esigenze specifiche della propria azienda.



SICUREZZA DEI DATI E DELLA PRIVACY

La sicurezza dei dati e della privacy è un aspetto critico della cybersecurity per le PMI. Le imprese devono proteggere i propri dati sensibili, inclusi quelli finanziari e quelli dei clienti, nonché informazioni sul personale, per prevenire furti di identità, frodi e violazioni della privacy.

Per garantire la sicurezza dei dati, le PMI devono implementare soluzioni di sicurezza per la crittografia dei dati, la gestione delle password e l'autenticazione a due fattori. È importante anche definire una politica di gestione dei dati, che preveda il backup e la ripristino dei dati in caso di perdita o compromissione.

Inoltre, le PMI devono essere conformi alle normative sulla privacy, come il GDPR (General Data Protection Regulation) in Europa e il CCPA (California Consumer Privacy Act) negli Stati Uniti. Queste normative stabiliscono requisiti rigorosi per la protezione dei dati personali dei consumatori e richiedono alle imprese di adottare misure adeguate per la sicurezza dei dati.

Infine, le PMI dovrebbero considerare l'utilizzo di strumenti e servizi di sicurezza gestita per garantire la sicurezza dei dati e della privacy. Questi servizi possono includere monitoraggio costante della sicurezza, gestione degli incidenti, analisi dei rischi e altro ancora.

SENSIBILIZZAZIONE ALLA SICUREZZA E FORMAZIONE DEI DIPENDENTI

La sensibilizzazione alla sicurezza e la formazione dei dipendenti sono elementi fondamentali per creare una cultura aziendale orientata alla sicurezza informatica. Ecco alcuni suggerimenti per promuovere la consapevolezza e fornire una formazione periodica ai dipendenti:

Creazione di una cultura aziendale orientata alla sicurezza informatica:

- Comincia dall'alto. L'impegno della dirigenza nell'importanza della sicurezza informatica invia un segnale forte a tutta l'organizzazione.
- Stabilisci politiche e procedure chiare in materia di sicurezza informatica e comunicale a tutti i dipendenti.
- Includi la sicurezza informatica come parte dei valori e delle aspettative aziendali.
- Promuovi la responsabilità individuale dei dipendenti nella protezione dei dati e delle risorse aziendali.

Formazione periodica dei dipendenti sulla sicurezza e sull'adozione di best practice:

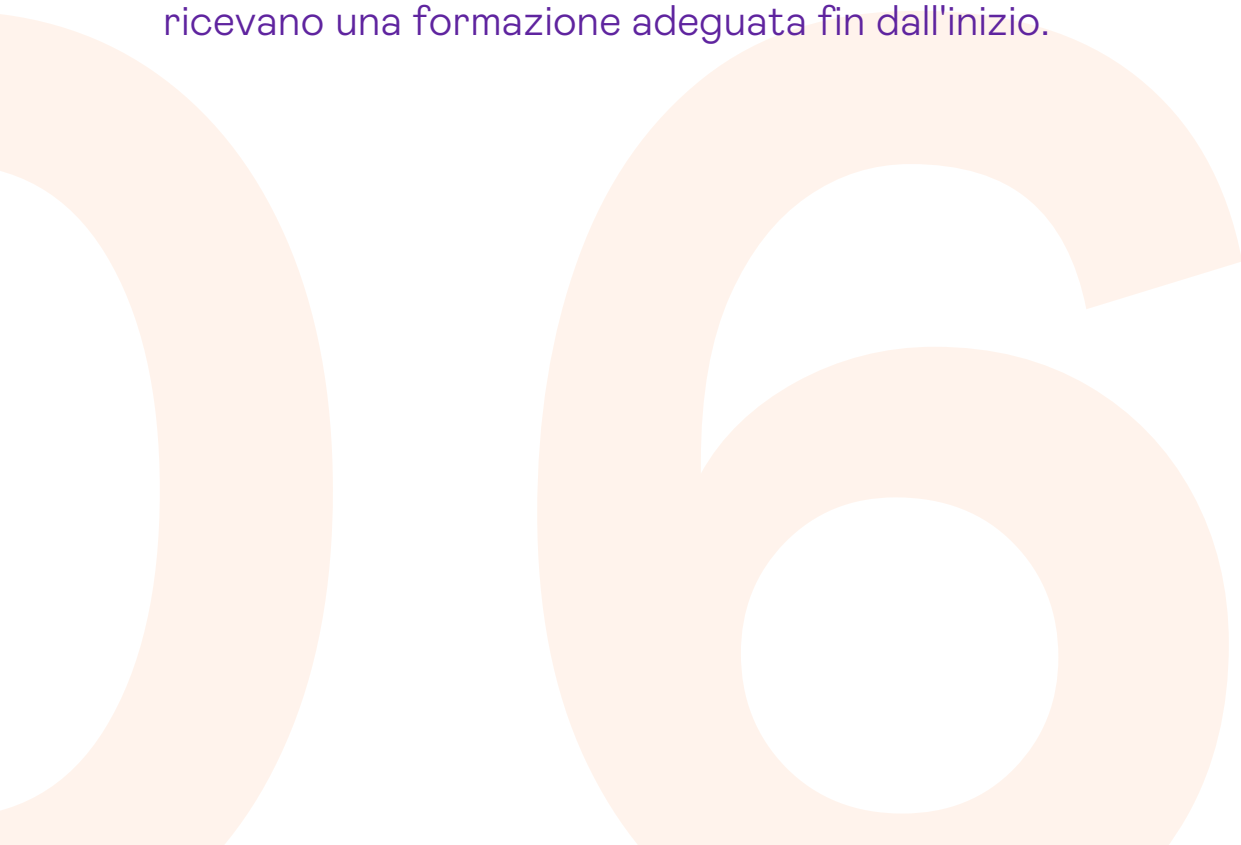
- Organizza sessioni di formazione regolari per sensibilizzare i dipendenti sui rischi informatici (come gli attacchi di phishing), sull'uso sicuro delle password e sulle pratiche di navigazione sicura.
- Offri esempi concreti di situazioni di rischio e fornisci linee guida pratiche su come affrontarle.

- Coinvolgi esperti di sicurezza informatica per tenere sessioni di formazione o per fornire risorse educative come guide e video.
- Promuovi una cultura di condivisione delle informazioni sulla sicurezza, per consentire ai dipendenti di segnalare le potenziali minacce e condividere le migliori pratiche di difesa.

Fornisci risorse e strumenti per supportare la sicurezza informatica:

- Metti a disposizione dei dipendenti risorse informative, come guide, checklist e linee guida, per aiutarli a comprendere e applicare le best practice di sicurezza informatica.
- Implementa strumenti di sicurezza, come software antivirus, firewall personalizzati e strumenti di autenticazione a più fattori, per consentire ai dipendenti di proteggere i loro account e i dati aziendali in maniera più semplice.

Ricorda di mantenere la formazione sulla sicurezza informatica un processo continuo. Aggiorna regolarmente i dipendenti sulle nuove minacce e sulle best practice, incoraggia una cultura di condivisione delle informazioni sulla sicurezza e assicurati che tutti i nuovi assunti ricevano una formazione adeguata fin dall'inizio.



GESTIONE DELLE MINACCE INTERNE

La gestione delle minacce interne è un aspetto cruciale della sicurezza informatica aziendale. Per affrontare efficacemente questa sfida, ecco alcuni punti chiave da considerare:

Identificazione delle minacce interne e delle pratiche di sicurezza dei dipendenti:

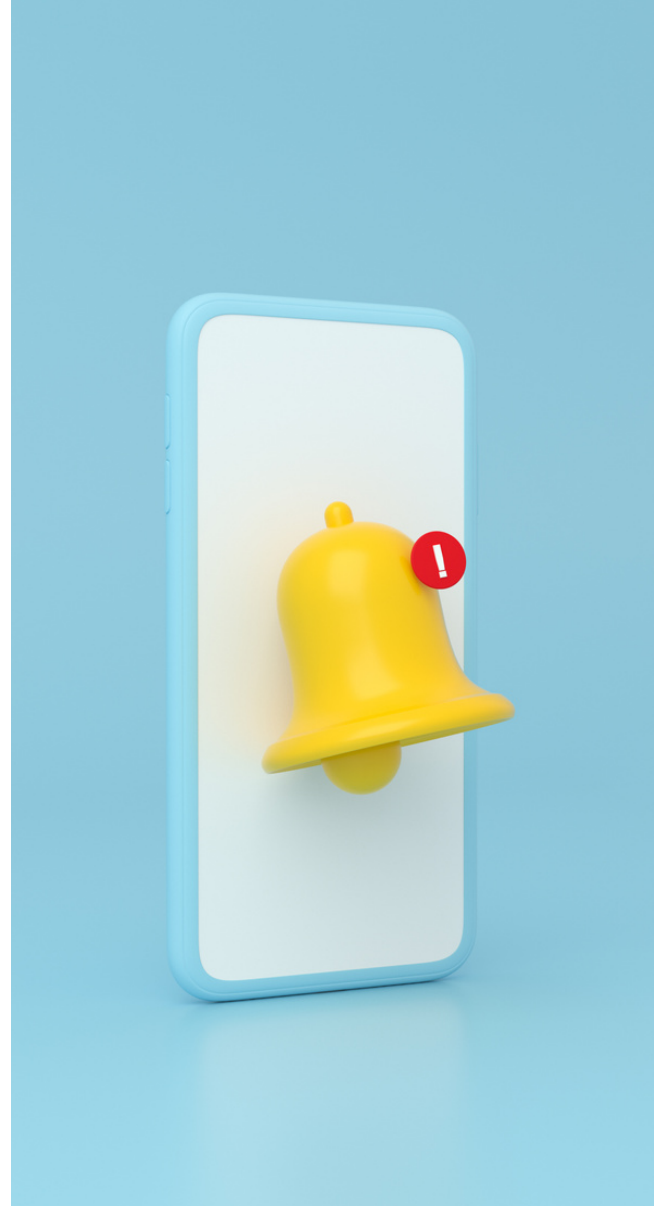
- Valuta i potenziali rischi associati ai dipendenti, come accessi non autorizzati, uso improprio delle risorse aziendali o divulgazione non autorizzata di informazioni sensibili.
- Mantieni un registro dei privilegi di accesso degli utenti e assicurati che siano adeguati alle loro responsabilità lavorative.
- Sensibilizza i dipendenti sulle politiche di sicurezza aziendale, comprese le best practice per l'uso di password sicure, la condivisione responsabile delle informazioni e l'uso corretto dei dispositivi aziendali.

Limitazione dei privilegi di accesso:

- Assegna i privilegi di accesso ai dati e ai sistemi in base al principio del "minimo privilegio", garantendo che i dipendenti abbiano solo l'accesso necessario per svolgere le proprie attività lavorative.
- Regola gli accessi in base ai ruoli e alle responsabilità dei dipendenti, assicurandoti che le autorizzazioni siano regolarmente riviste e aggiornate in base alle modifiche nella struttura organizzativa.

- Implementa l'autenticazione a più fattori per rafforzare l'accesso ai sistemi aziendali, richiedendo ulteriori metodi di verifica oltre alle sole credenziali di accesso.
- Monitora l'accesso ai dati sensibili, i tentativi di accesso non autorizzati e gli eventi di modifica o eliminazione dei file.
- Stabilisci protocolli per la notifica e la gestione degli incidenti di sicurezza interni, in modo da poter affrontare tempestivamente le violazioni o le attività sospette.

Ricorda che è importante trovare un equilibrio tra sicurezza e produttività. Non si tratta solo di limitare gli accessi e monitorare le attività, ma anche di promuovere una cultura di fiducia e responsabilità tra i dipendenti, fornendo formazione continua sulla sicurezza informatica e comunicando chiaramente le politiche aziendali.



RISPOSTA AGLI INCIDENTI E PIANIFICAZIONE DELLA CONTINUITÀ AZIENDALE

La risposta agli incidenti e la pianificazione della continuità aziendale sono elementi essenziali per garantire la prontezza e la ripresa delle operazioni in caso di violazioni della sicurezza o interruzioni impreviste. Di seguito sono riportati i punti chiave per affrontare queste situazioni:

Creazione di un piano di risposta agli incidenti:

- Identifica un team di risposta agli incidenti che abbia competenze specifiche in materia di sicurezza informatica e pianifica le responsabilità di ciascun membro del team.
- Stabilisci procedure chiare per la segnalazione, la gestione e la documentazione degli incidenti di sicurezza.
- Prepara una lista di contatti di emergenza, che includa sia personale interno che fornitori esterni di servizi di sicurezza e recupero dei dati.
- Definisci i criteri per la valutazione e la classificazione degli incidenti, in modo da poter rispondere tempestivamente e in modo appropriato.

Pianificazione della continuità aziendale in caso di violazioni o interruzioni:

- Identifica i processi critici per l'operatività dell'azienda e stabilisci strategie per garantire la continuità in caso di interruzioni, come ad esempio l'utilizzo di sistemi di backup e ripristino dei dati.

- Crea piani di ripristino specifici per le diverse minacce o scenari di violazione, ad esempio attacchi ransomware, perdita dei dati o interruzioni delle infrastrutture IT.
- Valuta le esigenze di business e stabilisci obiettivi di ripristino accettabili (RTO) e obiettivi di punto di ripristino (RPO) per ogni processo critico.
- Testa regolarmente i piani di continuità aziendale per verificare l'efficacia delle strategie di ripristino e apportare eventuali miglioramenti.

Comunicazione e coordinamento:

- Definisci i canali di comunicazione interni ed esterni durante gli incidenti di sicurezza, inclusi i protocolli per la comunicazione con i dipendenti, i clienti, i fornitori e le autorità competenti.
- Stabilisci una catena di comando e una struttura decisionale per garantire una gestione efficiente e coordinata degli incidenti.
- Documenta le lezioni apprese da incidenti precedenti e utilizzale per migliorare i piani di risposta e le strategie di continuità aziendale.

È fondamentale testare regolarmente i piani di risposta agli incidenti e di continuità aziendale per assicurarsi che siano aggiornati e adeguati alle esigenze in continua evoluzione dell'azienda. La tempestiva risposta agli incidenti e la pianificazione della continuità aziendale possono aiutare a minimizzare gli impatti negativi e garantire una ripresa rapida e sicura delle operazioni.

COLLABORAZIONE CON FORNITORI DI SERVIZI DI SICUREZZA E CONSULENTI ESTERNI

La collaborazione con fornitori di servizi di sicurezza e consulenti esterni può offrire un vantaggio significativo per migliorare la sicurezza informatica dell'azienda. Ecco alcune considerazioni da tenere presente:

Valutazione di partner di sicurezza affidabili e consulenti specializzati:

- Ricerca e valuta fornitori di servizi di sicurezza e consulenti specializzati che abbiano una comprovata esperienza nel settore della sicurezza informatica.
- Verifica le loro referenze, certificazioni e testimonianze di clienti precedenti per garantire che abbiano una solida reputazione.
- Assicurati che abbiano una profonda comprensione delle esigenze specifiche della tua azienda e delle normative di settore applicabili.

Considerazioni sulla terziarizzazione dei servizi di sicurezza informatica:

- Valuta i vantaggi e gli svantaggi della terziarizzazione dei servizi di sicurezza informatica in base alle esigenze e alle risorse aziendali.
- Identifica quali servizi di sicurezza possono essere adeguatamente gestiti internamente e quali potrebbero trarre vantaggio dalla collaborazione con partner esterni.

- Stabilisci chiare linee guida e accordi contrattuali per garantire la riservatezza, l'integrità e la conformità dei dati e delle informazioni condivise con i fornitori di servizi esterni.

Comunicazione e collaborazione efficaci:

- Definisci ruoli e responsabilità chiari per la collaborazione con i fornitori di servizi di sicurezza e i consulenti esterni.
- Comunica apertamente le tue esigenze e obiettivi di sicurezza informatica agli esperti esterni e assicurati che comprendano appieno le tue aspettative.
- Fornisci tutte le informazioni pertinenti sui tuoi sistemi, reti e dati per consentire una valutazione accurata dei rischi e una progettazione di soluzioni adeguate.

Monitoraggio e valutazione delle prestazioni:

- Stabilisci indicatori chiave di performance (KPI) per monitorare l'efficacia dei servizi di sicurezza forniti dai partner esterni.
- Pianifica regolari revisioni delle prestazioni e incontri di valutazione per assicurarti che i partner di sicurezza stiano soddisfacendo le tue aspettative.
- Mantieni una comunicazione continua con i fornitori di servizi esterni per affrontare eventuali problemi o miglioramenti necessari.

La collaborazione con fornitori di servizi di sicurezza e consulenti esterni può apportare competenze specializzate e un punto di vista oggettivo per migliorare la sicurezza informatica dell'azienda. Assicurati di stabilire una relazione di fiducia, definire chiare aspettative e mantenere una comunicazione aperta per massimizzare i benefici di questa collaborazione.

ULTERIORI RISORSE E STRUMENTI PER LA CYBERSECURITY DELLE PMI

Risorse online utili:

- Sito web del National Institute of Standards and Technology (NIST): Offre linee guida e raccomandazioni per la sicurezza informatica, compresi documenti specifici per le PMI.
- Sito web dell'European Union Agency for Cybersecurity (ENISA): Fornisce risorse e best practice per la sicurezza informatica delle PMI, inclusi materiali di sensibilizzazione e linee guida.
- Portale della sicurezza informatica del governo degli Stati Uniti: Offre una vasta gamma di risorse, strumenti e consigli per la sicurezza informatica delle PMI.
- Comunità e forum di sicurezza informatica: Partecipare a comunità online o forum specializzati può fornire opportunità per imparare dalle esperienze di altri professionisti della sicurezza informatica e condividere conoscenze e best practice.

Strumenti e soluzioni di sicurezza consigliati:

- Firewall: Implementare un firewall per proteggere le reti aziendali da accessi non autorizzati e attacchi esterni.
- Antivirus e anti-malware: Utilizzare software antivirus e anti-malware per rilevare e rimuovere minacce informatiche, come virus, malware e spyware.
- Soluzioni di gestione delle patch: Mantenere i sistemi operativi e le applicazioni aggiornate applicando regolarmente le patch di sicurezza rilasciate dai fornitori.

- Soluzioni di autenticazione a più fattori (MFA): Implementare l'autenticazione a più fattori per aggiungere un ulteriore livello di sicurezza nell'accesso ai sistemi e alle applicazioni aziendali.
- Soluzioni di crittografia dei dati: Utilizzare strumenti di crittografia per proteggere i dati sensibili durante la trasmissione e lo stoccaggio.
- Strumenti di monitoraggio della sicurezza: Implementare strumenti di monitoraggio della sicurezza che consentono di rilevare e rispondere tempestivamente a eventi di sicurezza anomali o sospetti.
- Backup e ripristino dei dati: Eseguire regolarmente backup dei dati critici e implementare un piano di ripristino dei dati in caso di perdita o violazione.
- Servizi di consulenza e gestione della sicurezza: Considerare l'opportunità di lavorare con fornitori di servizi di consulenza specializzati in sicurezza informatica per valutare i rischi e implementare misure di sicurezza efficaci.

Ricorda che la scelta degli strumenti e delle soluzioni di sicurezza dovrebbe essere basata sulle esigenze specifiche della tua azienda, il budget disponibile e l'ambiente operativo. È consigliabile valutare attentamente le opzioni e consultare esperti o consulenti qualificati per ottenere raccomandazioni personalizzate in base alle tue esigenze.

CONCLUSIONI

Le minacce informatiche rappresentano una sfida significativa per le PMI, ma investire nella sicurezza informatica è essenziale per proteggere il proprio business digitale. In questo ebook, abbiamo esplorato diverse tematiche legate alla cybersecurity per le PMI.

Abbiamo iniziato offrendo una panoramica delle minacce cibernetiche che le PMI possono affrontare, evidenziando le conseguenze finanziarie e reputazionali delle violazioni della sicurezza. Abbiamo poi esaminato la valutazione dei rischi e la pianificazione della sicurezza come passi fondamentali per proteggere il tuo business digitale.

Abbiamo discusso dell'importanza dell'identificazione dei principali asset digitali da proteggere e della valutazione dei rischi specifici per la tua PMI. Inoltre, abbiamo esplorato l'importanza di pianificare e implementare una strategia di sicurezza informatica, inclusi gli strumenti e le soluzioni consigliati.

Abbiamo sottolineato l'importanza della sensibilizzazione alla sicurezza e della formazione dei dipendenti per creare una cultura aziendale orientata alla sicurezza informatica. Inoltre, abbiamo esaminato la gestione delle minacce interne, come l'identificazione delle minacce e le pratiche di sicurezza dei dipendenti.

Infine, abbiamo affrontato la risposta agli incidenti e la pianificazione della continuità aziendale come componenti chiave della sicurezza informatica. Abbiamo sottolineato l'importanza di creare un piano di risposta agli incidenti e di pianificare la continuità aziendale in caso di violazioni o interruzioni.

Ricordati che la sicurezza informatica è un processo in continua evoluzione. È fondamentale rimanere aggiornati sulle ultime minacce e adottare una mentalità proattiva per proteggere la tua PMI.

Collaborare con fornitori di servizi di sicurezza affidabili e consulenti specializzati può fornire competenze aggiuntive e un punto di vista oggettivo.

Speriamo che questo ebook ti abbia fornito una buona base di conoscenza per comprendere le sfide e le opportunità nella cybersecurity per le PMI. Implementando le best practice e adottando un approccio strategico alla sicurezza informatica, puoi proteggere il tuo business digitale e mitigare le minacce cibernetiche

I DATI DELLA TUA AZIENDA SONO DAVVERO AL SICURO?

Se domani qualcuno ti privasse di tutti i tuoi dati e di quelli dei clienti cosa accadrebbe?

Risolvi il tuo problema ora affidandoti al protocollo

BrainSAFE

**In soli 3 Step mettiamo
in sicurezza la tua azienda**

PROTEGGITI ORA



BRAINCOMPUTING



Dal 2001 ad oggi, siamo diventati il principale partner di sviluppo software per grandi aziende e Brand quotati in Borsa. Realizziamo soluzioni dal forte impatto, basate su tecnologie evolute e impiegate in tutti i segmenti di mercato.

THE HUMAN TOUCH

braincomputing.com

BRAINCOMPUTING

braincomputing.com