

Cyber Security Guide - PMI

Vi mostriamo la giusta strada
nella giungla digitale

Sui Baloise Digital Scouts

Il team Digital Scouts di Baloise è costituito da collaboratori e collaboratrici motivati/e e interessati/e. Come ambasciatori della digitalizzazione, offriamo un aiuto per trovare la strada giusta nella giungla digitale. L'organizzazione dei Baloise Digital Scouts è nata da una collaborazione tra Group IT e Corporate Communications.

I Baloise Digital Scouts forniscono un contributo facoltativo nell'ambito della Corporate Social Responsibility di Baloise, poiché le esigenze della società vanno oltre l'acquisto di prestazioni di sicurezza.

I collaboratori Baloise dispongono di un vasto know-how che viene messo a disposizione della società al di là delle prestazioni di servizio rilevanti per l'attività aziendale.

Avete interesse a partecipare a uno dei nostri eventi informativi sul tema della cyber security?

Scriveteci un'e-mail a:
scouts@baloise.com



Su questa brochure

Questa brochure ha lo scopo di aiutare le PMI a informare i propri dipendenti in merito ai rischi e pericoli che si celano nell'uso quotidiano di Internet, in ufficio e a casa. Inoltre, essa spiega quali sono le basi della cyber security, presentando delle direttive preventive volte a evitare proprio questi incidenti informatici.

I rischi a livello di cyber security sono presenti sotto molte forme e possono provocare danni di dimensioni e portata devastanti. Sono ancora le persone la causa del maggior numero di incidenti di sicurezza informatica nelle aziende. Una chiara comprensione dei rischi e delle conseguenze del proprio agire può però contribuire in modo sostanziale a limitare questo rischio.

Tutela delle informazioni al di fuori dei locali aziendali

Social engineering

Per molte aziende i viaggi di affari sono all'ordine del giorno o costituiscono addirittura lo scopo aziendale. In questi casi è importante garantire la sicurezza delle informazioni ed essere consapevoli dei rischi. Che vi troviate in treno, nella lobby dell'hotel, in un bar oppure per strada: ovunque c'è qualcuno che origlia oppure che legge da dietro le vostre spalle e che, all'occasione, potrebbe sfruttare le informazioni a suo vantaggio. I dipendenti devono quindi essere sensibilizzati per poter provvedere alla tutela delle informazioni anche al di fuori dei locali aziendali.

Home office

I dipendenti che lavorano da casa devono essere consapevoli del fatto che sono tenuti a proteggere i dati aziendali allo stesso modo come se si trovassero in ufficio. Questo significa anche non mischiare i dati aziendali con quelli privati. È quindi meglio avere dispositivi separati. Se tuttavia i dipendenti

possono utilizzare i loro dispositivi (privati), devono ricevere anche le informazioni necessarie per la tutela dei dati. Regolate almeno i seguenti punti:

- svolgimento di aggiornamenti regolari
- utilizzo di pagine HTTPS e di VPN per una connessione sicura
- smaltimento sicuro di informazioni scritte sensibili (da non gettare nella carta)
- utilizzo di immagini di sfondo e di parti di contenuti durante le videoconferenze
- svolgimento di backup
- notifica di circostanze insolite

Nei luoghi pubblici

Appena vi trovate a lavorare in luoghi pubblici, che si tratti di un pranzo di affari al ristorante oppure mentre tornate a casa in treno, le conversazioni possono essere origliate. Per questo è importante scegliere le parole in modo tale che chi ascolta non possa trarre alcuna conclusione. È raccomandabile inoltre l'uso di un filtro protettivo

quando estranei hanno vista libera sul vostro portatile o sul vostro cellulare. Certe conversazioni dovrebbero essere svolte solo in locali protetti. Sussiste inoltre anche il pericolo di furto dei dispositivi se vengono lasciati incustoditi anche per pochissimo tempo.

Suggerimenti

- Sensibilizzate i vostri dipendenti affinché possano preservare la sicurezza delle informazioni anche quando si trovano in viaggio di affari oppure a casa.
- Rendete sicure le conversazioni svolte in pubblico ad esempio nominando solo le iniziali dei nomi oppure dite "la mia organizzazione" anziché il nome dell'azienda.
- Utilizzate il filtro privacy per evitare che le persone intorno a voi possano leggere sul vostro schermo.



Password e sicurezza

Le password non andrebbero mai scritte e non dovrebbero mai essere comunicate a nessuno. L'autenticazione a più fattori è un metodo buono e semplice per aumentare la sicurezza di un account. In questo caso, ad esempio, al momento del login dopo aver inserito user name e password viene richiesto un ulteriore codice generato da un'app di autenticazione che avrete installato sul vostro dispositivo mobile. È importante utilizzare per ogni account password diverse che non si assomiglino troppo tra loro. Se sussiste il dubbio che una password

sia andata persa oppure sia stata compromessa in un altro incidente informatico, deve essere subito cambiata. È molto importante quindi non cambiare solo un numero o una lettera, bensì utilizzare una password completamente nuova.

Password manager

Per ogni servizio dovrebbe essere utilizzato un account separato con password diverse. I cosiddetti password manager servono a semplificare la creazione e la memorizzazione di password nuove ed esistenti.

Con queste applicazioni è possibile generare una password sicura e salvarla in combinazione con un account. L'applicazione stessa viene protetta grazie a una complessa master password o, sullo smartphone, anche tramite identificazione con impronta digitale o face ID. In questo modo il collaboratore deve ricordarsi solo la master password e poi può consultare tutte le altre password.

Checklist per la sicurezza delle password

- Almeno 12 caratteri (quanti più caratteri, tanto più sicura la password)
- Maiuscole e minuscole
- Numeri e caratteri speciali come: !, &, %, €, +
- Nessuna parola elencata nei dizionari
- Nessuna successione di lettere come "abcdefgh"
- Password mai usate prima
- L'ideale: password da una frase-password

Ecco come creare una frase-password

1. Scegliete una frase che vi viene in mente senza alcun problema.
2. Utilizzate tutte le lettere iniziali nella loro successione, maiuscole, minuscole e cifre. Questa successione di caratteri diventa la nuova password.
3. Sostituite infine la punteggiatura con un carattere speciale per creare così una password sicura e facile da ricordare.

Esempio:

A febbraio del 1994 nacque mio figlio.
Quest'anno ha compiuto 24 anni!

Frase-password: Afd94nmf.Qahc24a!

Suggerimenti

- Utilizzate l'autenticazione a più fattori anche per il vostro password manager e prediligete le app di autenticazione rispetto ai codici tramite SMS.
- Non date a nessuno le vostre password.
- Verificate su pagine come ibarry.ch se i vostri dati di accesso sono già stati trovati in una raccolta di dati. In caso affermativo, cambiate assolutamente la vostra password.



Social engineering

Gli attacchi di social engineering, di base, sfruttano le emozioni delle persone. Gli hacker possono usare la disponibilità o la curiosità delle loro vittime contro di loro, per farle cadere in trappola. Possono anche incutere paura alle proprie vittime con minacce oppure manipolandole facendo leva sulla presunta urgenza delle richieste. Molto spesso però gli hacker abusano semplicemente della fiducia umana delle proprie vittime, ad esempio per entrare in possesso di dati confidenziali. Il social engineering può essere praticato durante una conversazione diretta, ma anche online oppure al telefono.

I seguenti esempi hanno lo scopo di aiutarvi a riconoscere un certo schema ricorrente.

Il vostro interlocutore

- vi chiede en passant delle informazioni confidenziali,
- si presenta come un collaboratore e chiede accesso a un'area protetta,
- insiste sull'urgenza della sua richiesta, minacciandovi,
- vi esorta a fare un'eccezione alle regole.

Se siete già stati vittima di un attacco del genere oppure se lo siete attualmente, consigliamo di adottare i seguenti comportamenti.

- Mantenete la calma.
- Non date informazioni di sorta, a meno che non sappiate con certezza con chi state parlando e quali sono le informazioni che questa persona può ricevere su di voi e sulla vostra azienda.
- In caso di richieste, esigete sempre di vedere il badge di collaboratore o visitatore e non lasciate mai entrare uno sconosciuto nell'area protetta.
- Ponete domande anche voi (ad esempio per identificare la persona) e se necessario, ripetetele. Questo blocca da una parte la costante richiesta di informazioni di chi vi sta di fronte e dall'altra vi aiuta

- a capire la situazione. Se l'attacco si svolge per telefono, chiedete un numero di telefono per richiamare (le chiamate di questo tipo spesso avvengono da un numero di telefono anonimo oppure non visibile) oppure terminate la conversazione senza dare informazioni.
- Tenete a mente che non
- volete sbarazzarvi subito dell'ingegnere sociale bensì che lo volete identificare. In questo modo potete evitare che in futuro faccia altri tentativi di attaccare voi e i vostri dipendenti.



Suggerimenti

- Fate attenzione a cosa rendete noto sui social media. Queste informazioni possono essere viste non solo da amici e conoscenti.
- Oggi l'intelligenza artificiale viene utilizzata per ingannarvi ancora meglio su diversi canali.
- Se siete incerti, contattate la persona in questione su un altro canale che avete già in comune.

Phishing



Il phishing è una forma di social engineering tramite la quale si cerca di ottenere la fiducia del destinatario, carpire informazioni confidenziali oppure convincerlo a agire in un certo modo, allo scopo di danneggiare l'azienda. Il phishing è uno delle più importanti porte di accesso per gli attacchi hacker.

Con l'e-mail sopra riportata si spiega da cosa riconoscere un'e-mail di phishing e come comportarsi nel modo giusto.

Fattori di riconoscimento (evidenziati in rosso) dall'alto verso il basso.

1. Il mittente indicato ha un indirizzo Swisscom sbagliato.

2. Formulazione impersonale, senza nome. Di solito, quando il cliente è conosciuto, l'appellativo è personalizzato.
3. L'ortografia differisce dalle regole conosciute.
4. Il link, come l'indirizzo e-mail, non è legato a Swisscom.

Altre caratteristiche tipiche delle e-mail di phishing

- Uso di una lingua inconsueta (ad esempio l'inglese sebbene utilizzate il servizio in italiano)
- Formattazioni o loghi diversi nell'e-mail
- E-mail all'indirizzo commerciale sebbene il mittente venga utilizzato solo in ambito privato

Come comportarsi con le e-mail di phishing?

Non tutte le e-mail di phishing sono sempre facili da riconoscere. Se sussiste il dubbio che un'e-mail ricevuta possa essere un'e-mail di phishing, non aprire alcun allegato né cliccare su link contenuti nella mail.

Non rispondere direttamente all'e-mail cliccando su "Rispondi". Se l'e-mail è stata inviata da un indirizzo aziendale non personale, ad esempio il support o il servizio clientela, contattate l'azienda attraverso un canale indipendente verificato. Andate ad esempio direttamente tramite la barra del browser sulla pagina dell'azienda e cercate lì delle possibilità di contatto. Se avete un reparto di IT, contattate i colleghi che ci lavorano per notificare loro l'e-mail ed eventualmente per avvertire altri colleghi.

Come posso proteggermi?

Utilizzate una password diversa per ogni login. Quando c'è la possibilità, attivate un'autenticazione a più fattori. Questa offre un'ulteriore protezione e riduce il rischio di un abuso. Nessuna banca vi chiederà mai tramite e-mail di modificare una password o di verificare i vostri dati della carta di credito.

Suggerimenti

- Il phishing è un fenomeno che non riguarda solo le e-mail ma anche gli SMS (smishing), le telefonate (vishing) e i codici QR (quishing).
- Nel dubbio, contattate il servizio clienti del mittente tramite telefono o e-mail.
- Chiedetevi se aspettavate questo messaggio.



Ransomware

Questo termine è costituito dall'inglese "ransom" che sta per riscatto e "malware" ovvero software dannoso. Si tratta infatti di software dannosi, detti anche trojan di estorsione o crypto trojan. L'obiettivo dei criminali è quello di chiedere un riscatto in denaro. Questo viene ottenuto crittografando i dati in rete oppure rubando i dati prima della crittografia, inviandoli a un server esterno dei criminali. Dopodiché viene chiesto un riscatto in denaro per lo sblocco dei dati oppure per la non pubblicazione degli stessi.

Come funziona un attacco di ransomware?

Ci sono diverse possibilità di accesso per un attacco di ransomware. Quella più utilizzata è tuttora la classica e-mail di phishing. Sensibilizzate quindi i vostri dipendenti in merito ai rischi e, quando si tratta di e-mail, fate sempre particolare attenzione a non cliccare per distrazione su link o aprire allegati. Questo potrebbe infatti far sì che un ransomware acceda alla rete aziendale, si espanda al suo interno e provochi il maggior danno possibile.

Un'altra possibilità di accesso sono i sistemi con punti deboli, ovvero quando non sono stati fatti gli aggiornamenti di sicurezza ad esempio di sistemi operativi o browser web.

La terza via di accesso più utilizzata sono gli accessi esposti alla manutenzione da remoto, raggiungibili direttamente tramite Internet.

Come posso proteggermi e tutelare anche la mia azienda?

Applicando misure preventive, è possibile ridurre in modo considerevole il rischio.

- Installate gli aggiornamenti di sicurezza appena vengono resi noti.
- Utilizzate solo software ancora supportati dal fornitore.
- Fate backup regolari, se possibile automatizzandoli, e salvateli al di fuori della vostra rete.
- Verificate regolarmente se i backup sono funzionanti e fate dei test di recupero.
- Al momento della scelta del backup, valutate quanto tempo serve per il recupero completo e quale perdita di dati può essere ritenuta accettabile per la vostra azienda.
- Sensibilizzate i dipendenti su come comportarsi in caso di attacco informatico e su come comunicare la presenza di e-mail sospette o di circostanze insolite.

Cosa fare in caso di attacco?

Mantenere la calma. Nella maggior parte dei casi può essere utile rivolgersi a specialisti esterni che hanno esperienza con attacchi hacker. Questi possono infatti fornirvi consulenza, aiutarvi a chiarire come si è verificato l'attacco e quali sono gli step da seguire per poter riprendere il prima possibile a lavorare.

Contattate l'Ufficio federale della cibersicurezza (UFCS). I loro specialisti vi supportano con informazioni utili sull'analisi e su come procedere.

Suggerimenti

- Utilizzate solo software ancora supportati dal fornitore.
- Redigete un piano di azione per un eventuale attacco hacker.
- Installate su tutti i dispositivi un programma di endpoint security per riconoscere tempestivamente eventuali attacchi.



Ulteriori direttive preventive importanti

Prendere precauzioni

La sicurezza delle informazioni è una vera e propria sfida per qualsiasi azienda. Preparatevi in anticipo a un attacco hacker. Redigete un piano di azione e esercitatevi sul da farsi in caso di attacco hacker. Quando questa eventualità diventa realtà, è troppo tardi per pensarci.

Salvataggio dati: fate backup e verificateli regolarmente

Dati sensibili come informazioni sui clienti possono andare persi non solo nel caso di un attacco hacker. Anche altri eventi come incendi o danni da acque possono provocare una perdita di dati. Ricordate pertanto di fare regolarmente delle copie di sicurezza dei vostri dati, i cosiddetti backup. È importante anche che verifichiate regolarmente che i dati salvati possano essere ripristinati. Salvate i backup separatamente rispetto ai dati di origine, di modo che possano essere accessibili in caso di attacco. Al momento della creazione del backup pensate già in anticipo a quale perdita di dati potete ritenere accettabile. Pianificate i vostri cicli di backup in base a ciò.

Aggiornamenti

Installate tempestivamente gli aggiornamenti di sicurezza disponibili per i vostri sistemi operativi e programmi. Accertatevi che i programmi impiegati vengano ancora supportati dal fornitore.

Buon senso

Quando navigate in Internet o eseguite delle operazioni con dati sensibili, affidatevi sempre al vostro buon senso. Non vi fate mettere sotto pressione da un'e-mail o da una telefonata. Avete sempre tempo per riflettere.

Sostegno statale

L'Ufficio federale della cibersicurezza (UFCS) offre informazioni e supporto per pericoli attuali e misure nonché un modulo di notifica per aziende e privati in caso di attacchi hacker.

Come faccio a verificare se io o i miei dati sono stati colpiti?

iBarry è la piattaforma svizzera per la sicurezza informatica. Questa pagina mette a disposizione informazioni e strumenti per qualsiasi azienda che desidera sensibilizzare i propri dipendenti.

La pagina offre anche controlli di sicurezza con i quali è possibile verificare se sono stati rubati i propri dati di accesso presso servizi web.

Suggerimenti

- **Supporto statale presso l'Ufficio federale della cibersicurezza (<https://www.ncsc.admin.ch/ncsc/it/home.html>)**
- **iBarry – La piattaforma per la sicurezza informatica (<https://www.ibarry.ch/it/>)**

Baloise Group

Aeschengraben 21

CH-4002 Basel

baloise.com

www.baloise.com/digital-scouts