Baloise DIGITAL SCOUTS

Cyber Security Guide – PMI

Vi mostriamo la strada attraverso la giungla digitale.

www.baloise.com/digitale-pfadfinder

Baloise Group

Informazioni sugli scout digitali

La truppa degli scout digitali di Baloise Group è composta da collaboratori motivati ed interessati. Come ambasciatori della digitalizzazione, offrono un aiuto per riuscire a trovare la giusta strada nella giungla digitale. L'organizzazione degli scout digitali Baloise nasce da una collaborazione tra GroupIT e Public Affairs.

Obiettivo e scopo degli scout digitali

Gli scout digitali Baloise forniscono un contributo facoltativo nell'ambito della Corporate Social Responsibility di Baloise, in quanto 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 ad uno dei nostri eventi informativi sul tema cyber security? Scriveteci un'e-mail: **pfadfinder@baloise.com**

Introduzione

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

I rischi a livello di cyber security sono presenti sotto molte forme e possono provocare danni di dimensioni elevate con conseguenze devastanti. Il principale punto debole nella sicurezza IT di un'impresa è e rimane sempre l'essere umano. Una chiara comprensione dei rischi e delle conseguenze del proprio agire può però contribuire in modo evidente a limitare la possibilità di fare errori.

I termini principali in breve

Social engineering
È “l’arte” di manipolare le persone allo scopo di indurle ad adottare un certo comportamento, ad esempio, vista la buona fede di una determinata persona, si cerca di manipolarla in modo tale da farsi confidare informazioni riservate. Facendo appello alla disponibilità delle vittime, il social engineer cerca di procurarsi l’acceso a dati sensibili.

Phishing
Tentativi di accedere ai dati personali di utenti Internet attraverso l’uso di e-mail, siti Internet o messaggi falsi allo scopo di danneggiare le persone coinvolte (ad esempio furto di dati o di valori pecuniari). Il phishing è una forma particolare di social engineering.

Cybermobbing
Termine generale che indica quei comportamenti volti a diffamare ed importunare altre persone o imprese avvalendosi dell’uso di Internet o di dispositivi mobili. Fa parte del cybermobbing anche il furto di identità, ad esempio allo scopo di svolgere transazioni o rilasciare affermazioni a nome di altri. Si tratta anche qui di una forma particolare di social engineering.

Malware
Termine generale che indica i software che eseguono funzioni indesiderate e dannose. Il malware spesso non si diffonde da solo, bensì utilizza un programma ospite e, facendo leva sull’utilità di esso, cerca di indurre l’utente a installarlo. I programmi malware più conosciuti sono i trojan, gli spyware e i ransomware.

Ransomware
(dall'inglese "ransom" per "riscatto")
Chiamati anche cryptolocker o virus del riscatto, sono programmi di malware con cui l'intruso riesce ad accedere a determinati dati per poi bloccare l'utilizzo di essi o l'accesso a tutto il sistema informatico. Lo scopo è estorcere denaro per poter riacquisire l'accesso ai propri dati. Nel 2017 gli attacchi dei malware WannaCry e NotPetya hanno ottenuto risonanza a livello mondiale mettendo completamente k.o. tra gli altri anche ospedali e aziende di logistica.

Distributed Denial of Service (DDoS)
Blocco che viene provocato da un sovraccarico di richieste ai servizi IT esposti a Internet, come un sito web, un e-shop oppure un forum, e che impedisce l'utilizzo del servizio IT attaccato. Questo può avvenire a causa di sovraccarichi non intenzionali oppure in seguito a un attacco mirato. Si tratta di una forma di ricatto sempre più utilizzata in tempi di sempre maggiore disponibilità di canali di vendita digitali.

Sensibilizzazione
Password e sicurezza

Le password non andrebbero mai scritte e non dovrebbero mai essere comunicate a nessuno. L'autenticazione a più fattori è un ottimo metodo e semplice per aumentare la sicurezza di un account. Ad esempio, al momento del login viene inviato all'utente un SMS al numero di cellulare registrato contenente un codice numerico per poter proseguire con la procedura di login. Per ogni account dovrebbero essere utilizzate password diverse, non troppo simili tra loro. È necessario essere consapevoli del fatto che le password possono andare perse e che quindi è bene cambiarle regolarmente. È molto importante quindi non cambiare solo un numero o una lettera, bensì utilizzare una password completamente nuova.

In caso di sospetto di uso illecito dell'account, è fondamentale modificare subito la rispettiva password.

Cassaforti per password

Le cosiddette cassaforti per password (password vault) servono a semplificare la creazione e la memorizzazione di password nuove ed esistenti, poiché idealmente per ogni servizio si dovrebbe utilizzare un account proprio con password diverse. Si tratta di applicazioni che permettono di generare una password sicura e di 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 riconoscimento facciale. In questo modo il collaboratore deve ricordarsi solo la master password e poi può consultare tutte le altre password.

Ecco alcuni buoni esempi di cassaforti per password:
SecureSafe, 1Password e Keeper Security.

Checklist per la sicurezza delle password

- ☐ Almeno otto caratteri
- ☐ Maiuscole e minuscole
- ☐ Numeri e caratteri speciali
- ☐ Nessuna combinazione di lettere contenuta in dizionari
- ☐ Password mai usata prima

Suggerimento

Se non utilizzate alcuna cassaforte per password, espedienti mnemonici e frasi per password possono aiutare a creare nuove password e quindi a ricordarle più facilmente. Si tratta di frasi semplici che permettono di creare una password utilizzando, ad esempio, le prime lettere di ogni parola.

Esempio:

→ password impostata: Mio figlio è nato nel febbraio 1994. Ha compiuto 24 anni quest'anno.

→ Tutte le lettere iniziali nel loro ordine e le lettere maiuscole o minuscole e i numeri compongono la nuova password. Inoltre, si scambiano i segni di punteggiatura con un carattere speciale e si crea una password sicura e facile da ricordare:

Mio figlio è nato nel febbraio 1994. Ha compiuto 24 anni quest'anno.
→ Passwort: **Mfènnf1Hc2aqa**

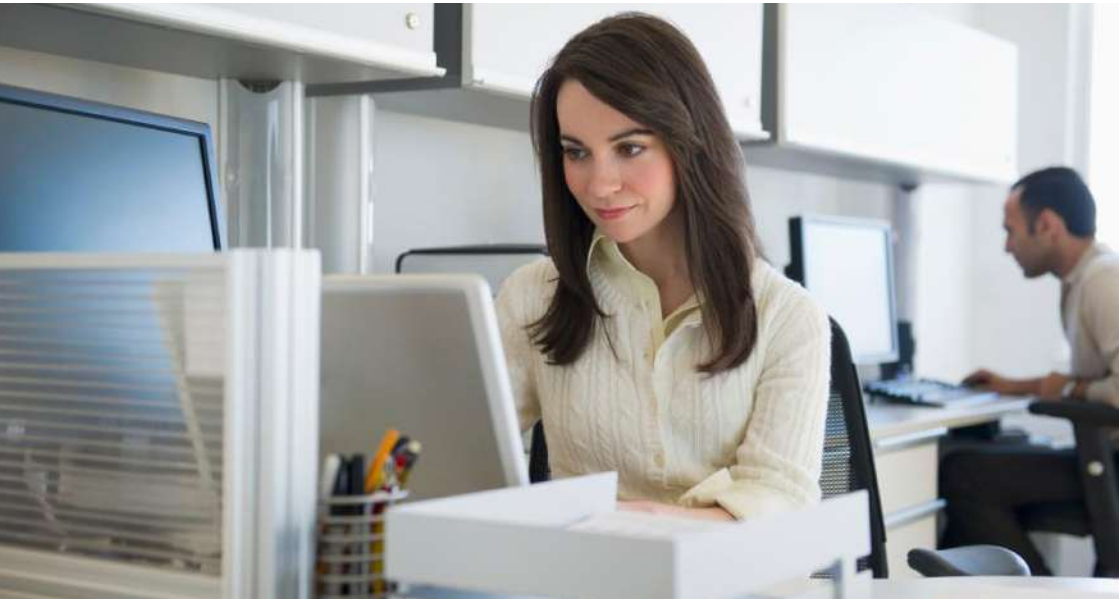
Social Engineering
Esempio e comportamento da seguire

Gli attacchi di social engineering sfruttano in linea di principio le emozioni umane. Gli hacker possono utilizzare l'avidità o la curiosità delle proprie vittime contro di loro per farle cadere in trappola. Possono anche incutere paura alle proprie vittime ricorrendo a minacce o facendo leva sulla presunta urgenza delle proprie richieste e quindi manipolandole. Molto spesso però gli hacker abusano anche semplicemente della fiducia delle proprie vittime, ad esempio per entrare in possesso di dati riservati.

Il social engineering può essere praticato nei vostri confronti durante una conversazione, 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 in modo casuale delle informazioni confidenziali

- La vostra interlocutrice si presenta come collaboratrice e chiede l'accesso ad un'area protetta



- → Il vostro interlocutore insiste sull'urgenza della sua richiesta, minacciandovi.

- → La vostra interlocutrice vi esorta a eludere eccezionalmente il regolamento previsto

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 alcun tipo di informazione, a meno che non sappiate con certezza con chi state parlando e quali sono le informazioni che questa persona può ricevere sulla vostra azienda.

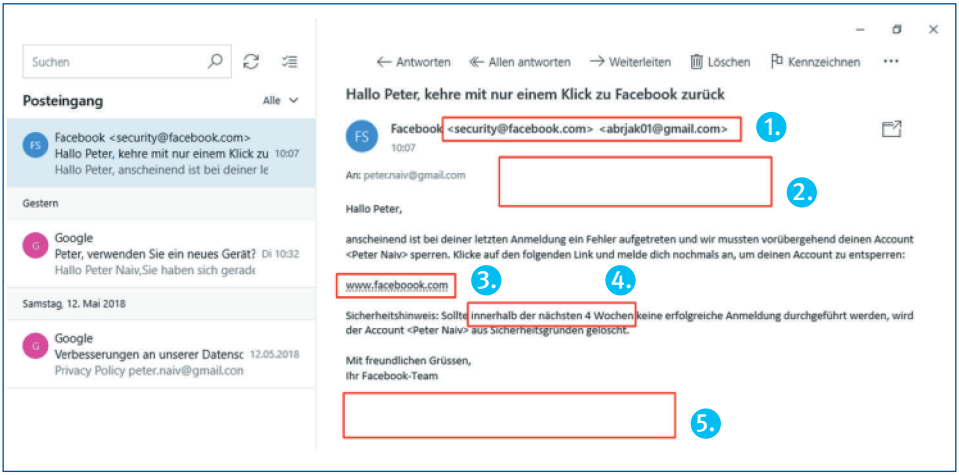
- → In caso di richieste, esigete sempre di vedere il badge del dipendente o del visitatore e non lasciate mai entrare uno sconosciuto nell'area protetta.

- → Fate domande (ad esempio per identificare la persona) e se necessario ripetetele. Questo blocca da una parte la costante richiesta di informazioni di chi vi sta difronte e vi aiuta a comprendere meglio la situazione.

- → Se l'attacco si svolge per telefono, chiedete di farvi dare un numero per poter richiamare (le chiamate di questo tipo arrivano spesso da un numero anonimo o sconosciuto). Oppure interrompete la comunicazione, riattaccando.

- → Tenete a mente comunque che il vostro scopo non è quello di riuscire a scacciare il social engineer, bensì di identificarlo per potergli così impedire di perpetrare nuovi tentativi di attacco contro di voi ed i vostri collaboratori. Ricordate che gli hacker spesso e volentieri non lavorano da soli.

Phishing
Esempio e comportamento da seguire



Con l'e-mail sulla destra si spiega come riconoscere un'e-mail di phishing e come comportarsi nel modo giusto.

Fattori di riconoscimento (riquadri rossi) dall'alto verso il basso:

1. Il mittente indicato ha due indirizzi e-mail, il secondo dei quali non sembra assolutamente essere quello di un impiegato di Facebook.
2. Manca il logo Facebook. Tutta la e-mail non ha il solito formato tipico di Facebook.
3. Il link indicato per accedere a Facebook contiene una "o" di troppo. Inoltre il link stesso non sembra assolutamente indirizzare verso una pagina di login o di sblocco della pagina.

4. La questione sembra essere un po' urgente. La stessa frase contiene anche una minaccia sotto forma di possibile cancellazione dell'account.

5. Mancano il classico disclaimer e la nota sulla protezione dei dati a fine e-mail. Non sono neppure indicate le opzioni di presa di contatto con il support di Facebook. Se in seguito l'account dovrebbe essere veramente cancellato, qui sarebbero sicuramente riportate delle informazioni di contatto.

Altre caratteristiche tipiche delle e-mail di phishing:
- → Formulazioni impersonali
- → Errori di battitura e problemi con gli accenti
- → Uso di una lingua inconsueta (ad esempio l'inglese sebbene utilizziate il servizio in italiano)
- → Diversi tipi di formattazione nell'e-mail.

Cifre e fatti:
45% degli utenti Internet cliccano sui link contenuti nelle e-mail di mittenti sconosciuti.

92 % di tutti gli attacchi hacker iniziano con un'e-mail di phishing.

Come comportarsi con le e-mail di phishing?
Non tutte le e-mail di phishing sono identificabili a prima vista. In caso di sospetto, potete procedere nel seguente modo:
- → E-Mail löschen; sollte es sich wirklich um eine wichtige Mail handeln, wird sich ein echter Onlinedienst nochmals melden.
- → Cancellare l'e-mail; se dovesse trattarsi effettivamente di un'e-mail importante, il vero servizio online vi contatterà.
- → Verificare manualmente (senza cliccare sul link all'interno dell'e-mail) lo status del profilo o del servizio.
- → Chiamare il supporto clienti del mittente e chiedere informazioni. Il numero di telefono del supporto clienti di un fornitore di servizi si trova facilmente con una ricerca su Google.

Ricordate che le aziende serie, come istituti bancari e assicurativi, non inviterebbero mai i propri clienti a reagire a una comunicazione importante tramite link in una e-mail. Di norma, in quanto clienti, venite sempre informati anche telefonicamente.

Se ricevete una (presunta) e-mail dalla vostra banca o dalla vostra assicurazione in cui vi viene richiesto di effettuare il login tramite un link fornito, potrebbe effettivamente trattarsi di una e-mail di phishing. Se non siete sicuri, potete avviare il vostro browser ed effettuare il login direttamente nel portale della banca o dell'assicurazione, dove potrete scoprire se l'istituto finanziario aspetta una reazione da parte vostra. In alternativa, potete anche informarvi telefonicamente chiamando la vostra banca o assicurazione.

Phishing via SMS

Gli attacchi di phishing possono essere effettuati anche via SMS che può essere inviato al cellulare. Controllare i messaggi SMS con dei link incorporati per aiutare a rilevare i tentativi di phishing:

- → Verificare il nome ed il numero del mittente (dati di contatto)
- → Verificare l'ortografia
- → Visualizzare i link (ad es. il nome della società del mittente scritto correttamente?)
- → In caso di dubbio, contattare il centro clienti del mittente per telefono o per e-mail.

Protezione da ransomware
e reazione in caso di attacco

Il ransomware può accedere in diversi modi al vostro sistema e danneggiarvi con il blocco dei vostri dati. Tenete a mente le seguenti misure per evitare questo tipo di ricatto:

→ Attenzione alle e-mail, soprattutto all'apertura di allegati. I ransomware vengono trasmessi soprattutto tramite e-mail e si propagano all'interno del vostro sistema nel momento in cui cliccate su un link o scaricate un allegato. Usate assolutamente un antivirus per verificare gli allegati di mittenti sconosciuti prima di aprirli.

→ Attenzione ai dispositivi di memorizzazione come le chiavette USB e i dischi rigidi portatili. Soprattutto se non conoscete l'utente precedente del dispositivo e non siete completamente sicuri del contenuto del dispositivo stesso, non dovreste mai collegarlo al vostro sistema.

→ Mantenete sempre aggiornati i vostri sistemi. Le nuove versioni dei sistemi operativi contengono spesso miglioramenti in fatto di sicurezza. Anche gli aggiornamenti del programma antivirus contengono miglioramenti per il riconoscimento e la difesa antivirus e dovrebbero essere fatti regolarmente.

Utilizzate inoltre una soluzione di backup e create regolarmente copie di sicurezza dei vostri dati.

In caso di attacco

→ Non pagate il riscatto richiesto! In questi casi spesso poi il riscatto viene aumentato e i dati rimangono criptati.

→ Rivolgetevi a un professionista e cercate di ripristinare il sistema con una versione di backup precedente all'attacco.

Ulteriori direttive preventive importanti

Attribuire le responsabilità
La sicurezza delle informazioni è il compito e la sfida di ognun collaboratore. Tuttavia, è importante nominare una persona responsabile per la sicurezza delle informazioni della vostra azienda ed un sostituto. Il responsabile per la sicurezza si assume i compiti inerenti la sicurezza ed informa regolarmente voi ed i vostri collaboratori in merito alla situazione attuale relativa alla sicurezza delle informazioni all'interno della vostra azienda. Egli è la prima persona a cui rivolgersi in caso di domande, incertezze e attacchi.

Salvataggio dati – esecuzione di backup
Dati sensibili come informazioni sui clienti oppure transazioni possono andare persi non solo nel caso di un attacco hacker. Anche altri fattori esterni come l'incendio o i danni da acque possono provocare la perdita di dati.

Ricordate pertanto di fare regolarmente delle copie di sicurezza dei vostri dati, i cosiddetti backup. Anche in questo caso sono in vendita programmi di diversa qualità e di diverso prezzo. L'importante è che verifichiate regolarmente che i dati salvati possano essere ripristinati e che i backup vengano conservati in un luogo diverso rispetto a quello in cui si trova il supporto dati originale.

Consigliamo inoltre l'uso di un firewall per difendervi dagli attacchi esterni nonché di un antivirus che verifichi regolarmente l'eventuale presenza di aggressori nel vostro sistema e nei file in esso presenti.

La maggior parte dei programmi antivirus, di firewall e di backup offre una versione di test oppure è completamente gratuita. Pertanto, vi consigliamo di prendervi il tempo necessario per testare alcuni programmi e scegliere una soluzione adeguata nel prezzo e nelle prestazioni alle esigenze della vostra azienda.

Nel frattempo, anche le soluzioni di backup in un cloud sono diventate comuni. Siate però consapevoli che per i vostri dati vale la legge sulla protezione dei dati del paese in cui si trova il server del cloud. Inoltre, dovreste comunque continuare a fare anche backup fisici dei vostri dati.

Aggiornare sistemi operativi e programmi
Ricordate di eseguire regolarmente e frequentemente gli aggiornamenti

di assistenza e sicurezza per il proprio sistema operativo e i programmi in uso. Queste patch chiudono le falle e le lacune note, aumentando così la sicurezza per tutte le funzioni utilizzate.

Tutti i sistemi operativi e programmi per computer o smartphone hanno degli errori. Gli autori di malware sfruttano queste falle per penetrare nel computer o nello smartphone.

Buon senso
Quando navigate in Internet o eseguite delle operazioni con dati sensibili, affidatevi sempre al vostro buon senso.

Per ulteriori linee guida preventive, informazioni in merito alla cyber security e interessanti attacchi hacker dal vivo, partecipate agli eventi informativi e alle presentazioni degli scout digitali Baloise.

L'attività di hacker è punibile
Qualsiasi tipo di attacco hacker è proibito dalla legge.

Sostegno statale
Der Bundesrat hat am 18. April 2018 die neu erarbeitete Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018–2022 verabschiedet. Die Strategie baut
Il 18 aprile 2018, il Consiglio federale ha emanato la Strategia nazionale per la protezione della Svizzera contro i cyberrischi (SNPC) per il periodo dal 2018 al 2022. La strategia pone le basi sulla prima SNPC (2012-2017) e mostra le misure volte a ridurre i rischi cyber, rispondendo alla situazione di minacce attuali. Per ulteriori informazioni sulla SNPC, consultare il sito **www.isb.admin.ch**.

Dal 2010, lo Stato offre inoltre la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) su **www.melani.admin.ch**, dove trovate informazioni in merito ai pericoli e alle misure attuali, come anche un modulo di annuncio per attacchi a danno di privati e PMI.

Have I Been pwned?
Il servizio web Have I Been pwned (HIBP) raccoglie e analizza i cosiddetti data dumps che gli hacker mettono in rete dopo aver messo a segno i loro data breach. HIBP offre agli utenti la possibilità di verificare se, in questo mare di informazioni rese note e quindi non più protette, si trova anche il proprio indirizzo e-mail o il proprio user name. Inoltre è possibile impostare anche una funzione con la quale si viene informati tramite e-mail in caso i propri dati dovessero essere resi noti in un data breach. È inoltre possibile cercare tra le password rese pubbliche. Per questo motivo è importante utilizzare più password, poiché quelle rese note nei data breach vengono vendute in Internet e non possono quindi essere più utilizzate.

https://haveibeenpwned.com

Baloise Group
Aeschengraben 21
CH-4002 Basel
pfadfinder@baloise.com

www.baloise.com

000.1038 i 1.20 100