Cyber MSME

Cybersecurity per Micro, Piccole e Medie Imprese

Cybersecurity: come migliorare il tuo piano di gestione durante una crisi – best practices

By CTS Customized Training Solutions & CASE

Erasmus+

Indice – clicca sui link per andare alle slides rilevanti:

Per proteggere la tua azienda dagli attacchi informatici, segui questi passaggi:

1. Rinforza le password

Sembra scontato, ma una password sicura è la prima arma per proteggersi dagli attacchi informatici. Cambiarla spesso, inoltre, aiuta a ridurre i rischi.

Passwords best practices

È risaputo che una buona password deve contenere almeno una lettera maiuscola, almeno un numero, e almeno un simbolo(like % # &). Inoltre, deve avere almeno 7 caratteri.
Ecco un esempio:

Erasmus+

Cyber MSME

Mettiamo caso che hai un cane di nome Rusty. Lo hai adottato nel 2018. Così la password del tuo PC e della tua mail è **Rusty-2018**. Facile da ricordare, giusto?

Ma anche facile da decifrare!

Allora, cosa fare?

Impara come pensare a delle password sicure. Una buona password, difficile da decifrare, deve essere:

- **Lunga (non più corta di 15 caratteri)**
- **Deve avere sia lettere maiuscole che minuscole**
- **Non deve contenere lettere sostituite comuni (es:"h0m3" al posto di "home" è troppo ovvio)**
- **Non deve contenere parole abusate (come "qwerty", "12345")**

Erasmus+

Utilizza un gestore di password

Un gestore di password è un programma per computer, basato sul servizio web o plug-in, che permette agli utenti di generare e gestire le loro password. È possibile scegliere Keeper, Lastpass, o Dashlane.

Se non riesci a scegliere, puoi saperne di più consultando il seguente link: https://en.wikipedia.org/wiki/List_of_password_managershttps://en.wikipedia.org/wiki/List_of_password_managers

2. Al posto delle password, utilizza passphrases

Una passphrase è una combinazione di parole e simboli che formano una frase. La frase non deve essere grammaticalmente corretta. Le passphrase di solito contengono fino a 40 caratteri. La principale differenza con le password sono gli spazi –le password non li hanno, le passphrase ce l'hanno.

Erasmus+

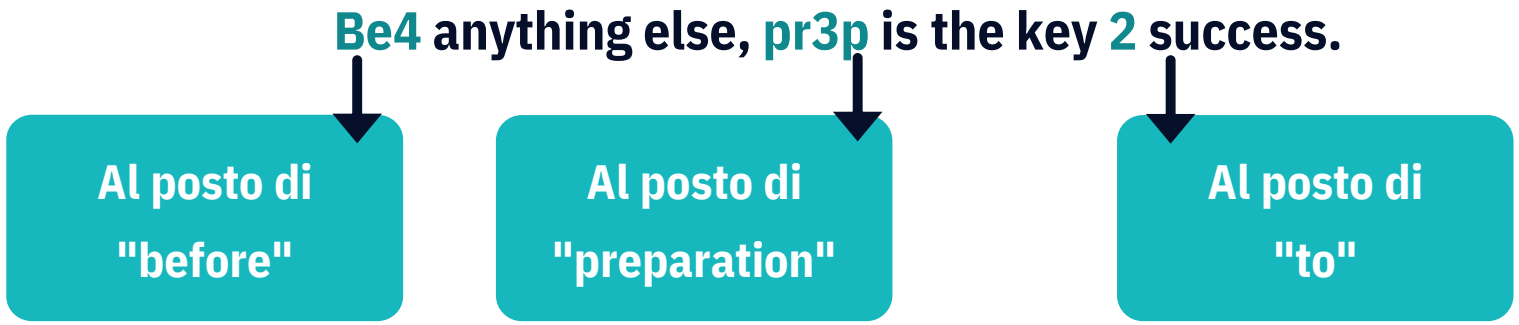
Passphrases best practices

- Utilizza una passphrase facile da ricordare ma non comune.
- Utilizza abbreviazioni non comuni.
- Aggiungi gli spazi.
- Utilizza lettere maiuscole (all'inizio della frase o per alcune parole).
- Cambia alcune lettere con dei numeri.
- Aggiungi la punteggiatura

Relevant links: TechTarget > Passphrase (https://searchsecurity.techtarget.com/definition/passphrase);
John Carroll University > Password vs Passphrase (https://password.jcu.edu/public/passphrase.php)

Erasmus+

Una passphrase potrebbe essere presa da una citazione di Alexander Gram:



Oppure essere formata da numeri e parole a caso:

Male h0rse 21, viLLag3 rAce.

Qualsiasi cosa scegli, ricordati di aggiornare la passphrase regolarmente. Non scriverla da nessuna parte così non c'è il rischio che venga scoperta. Decidi a chi farla sapere –
anche all'interno del team non c'è bisogno che tutti sappiano le password e passphrase.

3. Se possibile, utilizza più di un livello di autenticazione

Un hacker potrebbe decifrare una password o una passphrase.Questo è il motive per cui, se ne hai la possibilità, utilizza **l'autenticazione a due fattori (2FA)**. 2FA è un livello addizionale di sicurezza per la tua password/ passphrase, creato per garantire che nessuno oltre a te la la possa decifrare, a meno che non sia stato tu a dirglielo.

Come funziona 2FA?

- Puoi programmare la 2FA sia su un'app che su internet. Innanzitutto, ti saranno richieste le credenziali di accesso.
- In secondo luogo, sia sull'app che su internet ti verrà richiesto il secondo livello di verifica (e.s. tramite un messaggio). Devi inderire il codice per effettuare il log-in.
- Un'altra possibilità è utilizzare le impronte digitali.

Erasmus+

4. Non scrivere a nessuno la password

Se hai bisogno di condividere la password con il tuo team, utilizza un gestore di password come Keeper, LastPass, or DashLane.

5. Imposta domande di sicurezza difficili da indovinare

Spesso, quando si crea un profile viene richiesto di impostare una domande di sicurezza.
Il più delle volte, le risposte sono semplice da trovare sui tuoi social media.
(e.s. film preferito, giorno del primo appuntamento, nome del primo gatto, etc.).

Informati e scegli delle domande non facile da indovinare. Inoltre, informa i tuoi impiegati e partner.

Relevant link: Avast > How to create a strong password (https://blog.avast.com/strong-password-ideas)

6. Aggiorna regolarmente tutte le app

Preoccupati di aggiornare costantmente l'antivirus. Fai una scansione del PC almeno una volta a settimana. Ricorda che qualsiasi tipo di connessione ad internet è vulnerabile, e tu la utilizzi quotidianamente.

Inoltre, preoccupati di aggiornare il Sistema operativo, web browser, cloud, le app di comunicazione, etc.
La più piccolo vulnerabilità potrebbe rendere più facile un attacco da parte dei cybercriminali.

7. Aggiorna regolarmente i device

Gli imprenditori spesso si dimenticano di aggiornare device differenti da laptop e pc, ma durante le attività I cybercriminali potrebbero attaccare qualsiasi dispositivo. Potrebbero attaccare il route, la stampante o il fax. Aggiorna il firmware e tutti gli altri dispositive connessi alla rete— persino il microonde e il forno della cucina.

Erasmus+

8. Stai attento quando utilizzi reti Wi-Fi pubbliche

Il wi-fi pubblico è disponibile ovunque, nei ristoranti,nei coffee shops, o all' aeroporto. Come imprenditore, potresti aver bisogno della rete in qualsiasi momento. La domanda è: è sicuro utilizzare wi-fi pubblici?

Se è possible, cerca di utilizzare il tuo router personale. Puoi utilizzare l'hotspot o un device esterno. Questa eventualità è sempre più sicura del wi-fi pubblico.

Come proteggersi, allora, dai persicoli della rete wi-fi pubblica?

La soluzione migliore è utilizzare un VPN (Virtual Private Network).

Relevant link: Kaspersky > **Public Wifi Security** (https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cos’è un VPN?

VPN è l’acronimo di Virtual Private Network. Virtual in quanto la rete non esiste in un luogo fisico, ma virtuale. Private si spiega da solo: è una rete di cui non si può usufruire gratuitamente. È generalmente più sicura di una rete pubblica perchè limita le connessioni ed è molto più difficile per i cybercriminali spiare i dati attraverso una rete pubblica.

Come ottenere l’accesso?

È possibile impostare la propria VPN o utilizzare uno dei tanti fornitori di servizi VPN a pagamento. Siate cauti! Anche se potresti imbatterti in VPN gratuite in tutto il web, usarle potrebbe essere ancora più pericoloso che usare la connessione wifi gratuita in aeroporto. Dipende tutto da come funzionano le VPN.

Relevant link: Algo VPN > **Self hosted VPN solution** (https://github.com/trailofbits/algo)

Erasmus+

Come funziona un VPN?

Quando si accede a qualsiasi risorsa su Internet, l'intera comunicazione avviene tramite pacchetti. Un pacchetto è un piccolo pezzo di dati che seguono percorsi diversi per raggiungere la destinazione finale. Ecco come appare una "vita" semplificata di un pacchetto senza VPN:

Dalla figura si nota come i vostri pacchetti viaggiano non criptati attraverso la rete wifi gratuita. Ciò significa che qualsiasi hacker che ha ottenuto l'accesso a tale rete li può intercettare e quindi rubare tutti i dati sensibili inviati e ricevuti.

Erasmus+

Ora confrontiamolo con la "vita" del pacchetto con VPN abilitato :

Come puoi vedere, il pacchetto è crittografato fino al server VPN. Questo come avviene? Il client VPN installato sul dispositivo incapsula il pacchetto originale in un altro, criptato. Quel pacchetto criptato viene quindi inviato attraverso il wifi gratuito e il Internet Service Provider al server VPN.

Infine, il server VPN decripta il pacchetto originale e lo passa alla destinazione originale.

Confrontandolo con l'esempio precedente, anche se gli hacker rubassero i pacchetti crittografati sulla rete libera, avrebbero comunque bisogno di crackare la crittografia prima di vedere i tuoi dati.

Svantaggi nell’utilizzo delle VPN

Naturalmente, come in tutte le cose, ci sono degli svantaggi. Prima di tutto, la VPN che si sta utilizzando deve essere assolutamente affidabile. Infatti, la tua VPN potrebbe essere progettata per intercettare tutti i dati proprio mentre qualche malintenzionato sta utilizzando una rete pubblica per ottenerli. Ciò significa che le VPN impostate con scopi fraudolenti sono estremamente pericolosi per il vostro business.

In secondo luogo, i fornitori di VPN più popolari, proprio a causa della sicurezza che forniscono, spesso attraggono utenti con cattive intenzioni. Ciò implica che potreste ritrovarvi ad essere banditi dall'accesso ai luoghi o alle risorse popolari poiché condividete lo stesso indirizzo di IP dell'estremità con qualcuno che lo ha usato per un cattivo scopo in passato.

Infine, la velocità. Il livello extra di protezione di solito limita la velocità a cui è possibile accedere alle risorse. Mentre questo è trascurabile quando si utilizzano le reti wifi gratuite (dove la velocità di Internet non è molto alto, per cominciare) potrebbe limitare le prestazioni della rete domestica.

9. Fare un inventario

Oggi, possedere un business comporta degli sforzi, da parte tua e del tuo team, molto maggiori rispetto a qualche anno fa. È necessario ricordare molti più nomi di app, login, password ecc..

Cosa succede se qualcuno dimentica le proprie credenziali? O se uno dei vostri dipendenti perde lo smartphone? Cosa fare in questi casi?

Innanzitutto, prepara l'azienda ad ogni eventualità stilando un inventario.

Quest'ultimo deve includere tutti i dati relativi ai dispositivi e ai servizi online.

Inoltre, vi consigliamo di prepararlo insieme ad un esparto di cybersecurity e di ricontrollarlo periodicamente. È importante averlo a portata di mano così sarà più semplice gestire una crisi in caso si verifichi un attacco improvviso.

Come preparare l'inventario?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Esempio di inventario:

- **Lista dei device> modello, memoria, archiviazione, Sistema operativo, IP, numero di serie**> utilizzatore corrente (nome dell'addetto) > data di inizio
- **Impostazioni di configurazione per verificare che il dispositivo sia configurator correttamente** > specifiche, data dell'aggiornamento> data di inizio
- **Connessioni alla rete, protezioni, e VPN** > fornitore, località, stato, configurazione > data di inizio
- **Antivirus e altri software protettivi**> fornitore, stato, località, data dell'aggiornamento, versione aggiornata> data di inizio

- **Lista delle applicazioni e dei software >** fornitore, versione aggiornata> persona/device autorizzata all'accesso > data di inizio
- **Lista degli account degli utenti, inclusi quelli dormienti, condivisi, locali, admin, etc.** > località, stato> data di inzio
- **Backup** > stato > data di inizio
- **Lista delle vulnerabilità, gaps, e attacchi** > località, stato, risposta e passaggi di recupero> data di inizio

Relevant link: Verve Industrial > **What is OT/ICS Asset Inventory and Why is it the Foundation of a Cyber Security Program?** (https://verveindustrial.com/resources/blog/what-is-ot-ics-asset-inventory-and-why-is-it-the-foundation-of-a-cyber-security-program/)

Erasmus+

Dove conservare l’inventario?

Le GI utilizzano piattaforme speciali come:

- **Otorio** (https://www.otorio.com)
- **Axonius** (https://www.axonius.com/platform)

È disponibile una demo gratuita se ti piacerebbe testarle.

Oppure, puoi affidarti alle soluzioni pensate dalla global IT community:

- **CIS Controls** (https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/)

Questo strumento è libero e open source. È costantemente aggiornato, e tra i suoi sviluppatori ci sono aziende, agenzie governative, istituzioni e individui provenienti da ogni parte dell'ecosistema (cyber-analisti, cercatori di vulnerabilità, fornitori di soluzioni, utenti, consulenti, politici, dirigenti, università, revisori dei conti, ecc.).

10. Disattivare i servizi non utilizzati

Grazie all’inventario, è possibile gestire i servizi inutilizzati, prodotti e applicazioni che stanno per scadere o sono già scaduti. Ricordi quante volte hai inserito i tuoi dati aziendali, incluso il numero della tua carta di credito per attivare un'app? Esattamente...

Quindi, se non riattivi l'account, quell'informazione sarà disponibile per il potenziale hacker.

11. Rivedi le connessioni tra i device

Non tutti i dispositivi aziendali hanno bisogno di parlare tra di loro o la rete. Rivedere tutte le connessioni e decidere se è necessario o no.

Se si gestisce un database enorme o transazioni finanziarie forse sarebbe meglio farlo su un computer specifico che non ha alcuna connessione con altri dispositivi aziendali.

12. Crea livelli di accesso ai dati

Inoltre, così come non tutti i dispositivi devono necessariamente parlare tra di loro, non tutti i dipendenti hanno bisogno di avere accesso a tutti i dati, account e documenti. Se hai già creato l'inventario, è possibile controllare i dispositivi e il software. Ora è il momento di creare un altro documento che vi aiuterà a gestire la sicurezza informatica - livelli di accesso ai dati.

Il livello di accesso è un insieme di autorizzazioni o restrizioni fornite per accedere ai dati.

Se sei un programmatore si possono semplicemente codificare i livelli di accesso in app o sul sito web. Tuttavia, non solo i programmatori hanno la possibilità di creare diversi livelli di accesso. Anche se non si dispone di un background IT si può fare.

Dove iniziare?

Principi livello di accesso ai dati

Come abbiamo detto, i livelli di accesso si basano su una serie di autorizzazioni e restrizioni. Prima di tutto, è necessario categorizzare tutti i dati, tra cui app e software, e si deve dare loro la priorità, ad esempio.

categoria A	livello più alto di priorità
categoria B	Livello alto di priorità
categoria C	Livello medio di priorità
categoria D	Livello basso di priorità
categoria E	Livello più basso di priorità

importanza

Erasmus+

Questa tabella è solo un esempio, naturalmente. Sta a voi decidere quanti livelli indicare. La cosa più importante è stabilire chi dovrebbe avere accesso ai dati e su quali basi.

Ad esempio, i dati sensibili, conservati nella tua banca dati clienti, potrebbero essere accessibili solo alle due persone a cui servono per lavorare quotidianamente. In caso di crisi, possono esseresono raggiunti da altri 2 dipendenti. In questo modo, si implementerà correttamente uno dei punti del piano di gestione delle crisi informatiche.

Infatti, se solo poche persone conoscono i dati, pensate a come questo renda più semplice gestire una crisi- se i dati sopracitati saranno condivisi al di fuori dell'impresa, infatti, sarà più semplice individuare il colpevole
Avrete 4 persone da controllare, i loro dispositivi e la loro storia operativa. Questo è molto più facile di controllare tutti i dipendenti, partner e fornitori.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

I livelli di accesso possono essere creati da soli o con il supporto di un esperto. Qualunque cosa tu scelga, ricordati di informare i tuoi dipendenti sul tipo di livello che hai loro assegnato. Informali su come utilizzare questi livelli durante l'attività ordinaria e in caso di crisi.

Inoltre, ricordati di aggiornare la lista periodicamente, soprattutto ogni volta che uno dei vostri dipendenti cambia posizione, viene promosso o lascia l'azienda.

Dai l'incarico a qualcuno di occuparsi di questo aspetto, si potrebbe trattare di:

- un esperto di sicurezza informatica
- un consulente di sicurezza informatica
- un analista di sicurezza informatica
- un amministratore del sistema IT.

Erasmus+

13. Non conservare tutti i dati in un unico posto

Ciò non significa che non è possibile mantenere i dati in un unico cloud sicuro. Il punto è che se alcuni dati importanti per la vostra azienda, come i dati dei clienti o dati finanziari, sono conservati in un'unica schermata, sarà facile per un cybercriminale rubarli tutti con uno screenshot fatto con lo smartphone.
Questo implica anche valutare se sia il caso fornire un telefono aziendale a tutti i dipendenti.

Ricorda che un semplice screenshot può essere facilmente rubato mentre un collaboratore sta semplicemente lavorando in un caffè o all'aeroporto ecc...
Quindi, è importante informare i dipendenti che anche la connessione tramite VPN non li protegge completamente contro l'hacking dei dati.
Devono sempre proteggersi ulteriormente.

Erasmus+

14. Utilizza protezioni per lo schermo TPU

Come abbiamo detto, anche unVPN non può proteggere completamente i tuoi dati in un luogo pubblico. Ecco perché ti consigliamo di utilizzare speciali screen protector in TPU (poliuretano termoplastico).

Si tratta di un tipo di plastica molto resistente, perché migliorata fortificata chimicamente, capace di resistere ai graffi, ed è anche molto più flessibile. Perché è utile?

Perché viene utilizzata anche per realizzare cover per lo schermo speciali, i quali impediscono che il contenuto dello schermo venga visualizzato da chiunque lo guardi di lato.

Per gli altri, quindi, lo schermo apparirà solo nero e nessuno avrà modo di scattare una foto di lato.

Relevant link: Viola Pan > **Part Three: PET, TPU, or Tempered Glass – all you need to know to choose a screen protector** (https://www.linkedin.com/pulse/part-three-pet-tpu-tempered-glass-all-you-need-know-choose-viola-vmax/)

Erasmus+

15. Insegnalo agli altri

Tenete a mente che la sicurezza informatica non è un'attività una tantum. E 'un piano a lungo termine che dovrebbe essere attuato progressivamente e con saggezza. Richiede il coinvolgimento di tutti i dipendenti, anche se non necessariamente allo stesso modo. Tutto dipende dal piano di gestione delle crisi informatiche dell'azienda.

Non dimenticare che le persone sono l'anello debole del tuo sistema di sicurezza informatica, per questo è importantissimo formarli e informarli di ogni aggiornamento apportato.

Sei pronto per iniziare?

Erasmus+

Grazie per l'attenzione!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.