



Cyber MSME



Cybersecurity per Micro, Piccole e Medie
Imprese

Sicurezza informatica sul budget

Come proteggere l'attività quando ogni centesimo conta.

By CTS Customized Training Solutions & CASE

Introduzione

Questo Toolkit è ideale per le PMI che vogliono incrementare la loro sicurezza informatica e non hanno budget molto elevati. Vi proporremo alcuni software e hardware ma vi incoraggiamo a fare anche delle ricerche extra sugli argomenti che tratteremo.

Introduzione

Quando parliamo di cybersecurity e hackeraggi, subito pensiamo ai film Hollywoodiani, alle aziende miliardarie, agli hacker che digitano velocemente sulla tastiera, server giganti e interface testuali (l'ultima è veritiera). Questo immaginario ci porta a credere che può succedere solo alle aziende più grandi e con molte risorse per proteggerci. Ma può una PMI con un budget ristretto implementare ugualmente sistemi di sicurezza?

Certamente!



Soluzioni di terzi vs. Soluzioni fatte in casa

Prima di iniziare a parlare di VPNs e Ad-blockers diamo un'occhiata ai vocaboli che andremo ad utilizzare:

Terze parti

Questo significa che altri lo faranno per voi. Generalmente, ciò che devi fare è installare un'app ed eseguire dei passaggi basilari- l'hosting e la configurazione vengono fatte dalla società esterna.

Vantaggi:

Facilità di configurazione e di accesso; nessuna competenza e conoscenza extra richiesti; mercato altamente competitivo rende diverse aziende offrono un sacco di servizi extra.



Svantaggi:

I piani di pagamento potrebbero non essere adattati alle tue esigenze, facendoti così pagare per servizi di cui non usufruisci; stai affidando i tuoi dati a una terza azienda; i costi sono più alti.

Self-hosting:

Questo significa che il responsabile per la sicurezza dei dispositivi sei tu. Oltre ad un dispositivo, avrai bisogno di un software appropriato, nonché delle conoscenze per installarlo e configurarlo accuratamente.

Vantaggi:

Stai ottenendo esattamente quello che vuoi; puoi unire l'utile al dilettevole, imparando nuove cose; puoi provare gratuitamente i software open-source disponibili; puoi immedesimarti nel ruolo da hacker utilizzando Linux e linee di comando :)



Svantaggi:

Sono richieste conoscenze informatiche di base; il server è necessario (ed è un costo)

Self-hosting sul budget

Parlando di Self-hosting ti sarai chiesto: come potrei scegliere questa opzione se non so nulla di hosting e non posso spendere migliaia di euro per l'infrastruttura? In realtà non devi spendere così tanto per l'infrastruttura e non devi neanche possederne una!

Prima di tutto, il cloud hosting è molto importante. Tutti i grandi player del mondo IT (Amazon, Google, Microsoft) offrono piattaforme cloud, inoltre ce ne sono decine messi in commercio da aziende più piccole (Digitalocean e Heroku per citarne alcuni).

Tutti offrono una prova gratuita (da 1 a 3 mesi a seconda della piattaforma), in modo da avere il tempo di imparare e provare a fare le cose da soli (invece di pagare in anticipo).



Una volta terminata la prova gratuita, il costo mensile sarebbe di 5/10 euro – di gran lunga inferiore rispetto ad acquistare servizi di terza parti.

E che ne pensate di acquistare un server? Sarebbe economico e poco ingombrante, no?

Un dispositivo adatto alla vostra PMI, infatti, potrebbe costarvi meno di 100 euro e stare nel palmo della mano.

Vi presentiamo Raspberry Pi, un piccolo computer a tutto tondo.



Il nostro Raspberry Pi con mandarino in scala.

P.S= Il mandarino era delizioso!



Oltre ad essere in grado di essere un VPN e Ad-blocker (in una volta sola!) ha decine di altre funzioni (server multimediali, archiviazione cloud, armadi giochi arcade, specchi intelligenti, emulatori di console retrò - le possibilità sono enormi). Gli ultimi modelli potrebbero essere comodamente utilizzati anche come PC di backup in caso di guasto improvviso con un sistema operativo Linux dedicato in grado di navigare sul web e giocare con facilità multimediale. Con un prezzo di circa 60-100 euro a seconda del modello, potrebbe essere la soluzione più conveniente nel lungo periodo.

Abbiamo già spiegato in dettaglio cos'è una VPN e perché dovresti usarla, ma ecco un utile promemoria. Un VPN è una rete virtuale che protegge la tua privacy nascondendo i dati che invii in un ulteriore livello di crittografia. Viene utilizzato principalmente quando si naviga in reti pubbliche o non protette, dando maggiori chance ai cybercriminali di rubare i tuoi dati. Molte aziende offrono servizi VPN e investono molto in pubblicità (se sei un utente frequente di Youtube sono sicuro che hai incontrato almeno un annuncio VPN).



Opzioni di Notable VPN:

Terze parti:

Non faremo nomi specifici poiché il mercato è fortemente competitivo e le differenze all'interno dei principali fornitori sono minime. Ma, digitando "miglior VPN + anno in corso" in un motore di ricerca a vostra scelta otterrete risultati rilevanti in pochi secondi.

Prezzo: circa 10 euro al mese (confrontando le offerte migliori). Inoltre, per risparmiare conviene fare un abbonamento di lungo periodo.

Self-hosted:

OpenVPN (<https://openvpn.net/vpn-software-packages/>) **Pricing:** Open source/free for

use
AlgoVPN (<https://github.com/trailofbits/algo>) **Pricing:** Open source/free for use



Ad-blockers

Probabilmente avete già sentito parlare di Ad-blockers. Ci sono buone possibilità che li state utilizzando proprio in questo momento! Gli Ad-blockers sono la risposta, a lungo ricercata, per bannare quei fastidiosissimi annunci e rendere la pubblicità più user-friendly. Inoltre, sono anche un'importante fonte di sicurezza.

In che modo?

Gli annunci ingannevoli sono la metodologia più usata per compromettere l'integrità della tua rete e sabotarla- basta un clic di troppo. Inoltre, le pubblicità appesantiscono la tua rete internet, e questo potrebbe essere un problema quando hai un accesso limitato ad internet o l'abbonamento mensile a un piano dati. Se state tracciando la vostra consegna e una pubblicità rallenta la connessione, sicuramente non ne sarete felici.

E allora cosa fare?



In primo luogo, esistono due tipi di Ad-blockers. L'Ad-blockers dal lato cliente che installi sul browser e l'Ad-blockers basato sulla risoluzione DNS. I primi sono installati come applicazioni sul browser, i secondi hanno bisogno di una macchina su cui operare. Qual è la principale differenza?

Immaginate di voler censurare una scena a luce rosse mentre state guardando un film. Utilizzare l'Ad-blockers lato-clienti significherebbe coprirsi gli occhi con le mani. Non l'avete vista, ma la scena era ancora lì e il film ha impiegato di più per finire. Il costo non è stato elevato, ma pensate di doverlo fare centinaia di volte al giorno...il costo alla fine aumenterebbe!

Utilizzare la risoluzione DNS significa tagliare la scena prima che venga mandata in onda, accorciare il film e quindi risparmiare.

Un altro vantaggio è la possibilità di far funzionare il DNS sfruttando la rete internet, e quindi non dover installare un client blocker per ogni dispositivo che si intende



Opzioni Ad-blocking Notable DNS :

Terze parti:

Nextdns (<https://nextdns.io>) - Piano personale gratuito limitato a 300k al mese; piano Pro è di circa 2 euro al mese, Business plan a partire da circa 200EUR all'anno fino a 50 dipendenti.

Prezzi: circa 10 euro/mese su un piano mensile (confrontando le offerte dei migliori fornitori), più conveniente se acquistato in piani a lungo termine (3-5 euro al mese).

Self-hosted:

Pi-hole (<https://pi-hole.net>) – Le istruzioni per installarlo le trovi al seguente link:

<https://github.com/pi-hole/>

Prezzo: Open source/free per l'utilizzo



Grazie per l'attenzione!

