Cyber MSME

Cybersecurity per Micro, Piccole e Medie Imprese

Suggerimenti essenziali per la sicurezza del router

Migliora la sicurezza della tua rete in pochi passaggi

By CTS Customized Training Solutions & CASE

Erasmus+

Seguendo questi semplici suggerimenti renderai la rete della tua PMI più sicura:

1. Guarda la data di fabricazione del router

Utilizzi lo stesso router dall'inizio dell'attività ed è stato sempre affidabile? Ti sei affezionato e non vuoi sostituirlo? Ricorda, però, quando in gioco c'è la sicurezza dell'azienda non c'è spazio per i sentimenti.

Non ci sono scorciatoie per capire se un router è da cambiare oppure no. Gli esperti consigliano di sostituirlo ogni 2/3 anni, massimo 5. Tuttavia, è consigliato cambiarlo immediatamente se il dispositivo è supportato esclusivamente da un protocollo di crittografia noto per avere delle vulnerabilità (affronteremo questo argomento successivamente).

2. Aggiorna il firmware

Hai acquistato un nuovo router, lo hai impostato e non hai più guardato il pannello di gestione? È capitato da tutti, ma è buona prassi fare un check-in di tanto in tanto. I router, come qualsiasi altro devices connesso a internet, ricevono aggiornamenti costantemente dal firmware. Alcuni si aggiornano automaticamente, altri occorre farlo manualmente e, se non lo si fa, si potrebbero perdere aggiornamenti di sicurezza important.

3. Disattivare la configurazione protetta Wi-Fi (WPS)

Quando aggiornate il pannello di gestione, assicuratevi di aver spento il WPS. Che cos'è il WPS? È un metodo per collegare un nuovo dispositivo alla rete premendo un pulsate fisico sul router. Può sembrare pratico, ma è veramente pericoloso continuare. Perchè?

Perchè il WPS è il metodo più utilizzato dai cybercriminali per accedere senza autorizzazione alla tua rete. Molti si basano esclusivamente su questo pulsante per compiere i loro attacchi. Spegnerlo è il primo passo da fare per mantere la tua rete sicura.

4Non utilizzare protocolli di crittografia WEP o WPA

Durante la configurazione del WI-FI ti viene richiesto se vuoi proteggere la rete con una password e, se si, con quale protocollo di crittografia. Questo è il momento più critico perché ci vengono date veramente tante opzioni (WEP; WPA; WPA-PSK; WPA2-PSK 2 ecc..). Perché ne esistono così tante? Quale scegliere e per quale motivo?

Per farla semplice: i protocolli di crittografia sono un modo per autorizzare solo le connesioni che hanno la chiave richiesta (in questo caso la password) e tenere gli altri lontano.

WEP è stato il primo e fu lanciato nel 1999. Fu sostituito da WPA (WI-FI Protected Acces) nel 2003 e successivamente da WPA2 nel 2004. Dal 2018, invece, è in uso WPA3.

Quale utilizzare, allora? La risposta è scontata: la versione più aggiornata. Se il vostro dispositivo è supportato solo da crittografia di tipo WEP e WPA, affrettati a sostituirlo. Entrambi questi protocolli, infatti, hanno delle vulnerabilità ormai note ai cybercriminali che possono sfruttare a loro vantaggio. Oggi il più utilizzato è WPA2 ma, se si sta considerando di sostituirlo il prima possibile, si consiglia l'acquisto di WPA3.

Allora, perché quelli pericolosi sono ancora in giro? Tieni presente che il dispositivo che si connette al router deve anche essere in grado di leggere il protocollo di crittografia. Non è raro in azienda dover utilizzare uno specifico dispositivo in grado di leggere esclusivamente il protocollo precedente. Se questo è il caso, prendi in considerazione l'idea di creare una rete extra solo per quel dispositivo in modo da no compromettere anche la sicurezza di tutti gli altri.

5. Crea una rete extra per gli ospiti

”Posso connettermi al vostro WI-FI?” è una domanda molto frequente.

Nel 95% dei casi gli ospiti non avranno cattive intenzioni, ma ricorda: i loro dispositivi potrebbero già essere stati compromessi dai cybercriminali senza esserne a conoscenza, e creare una rete guest da un dispositivo mobile ormai è possibile in pochissimi passaggi!

6. Imposta una password sicura per proteggere la rete☺

Tutti i suggerimenti di cui abbiamo parlato sono importanti, ma questo è cruciale!

Nessun altro espediente funzionerà se non imposterai prima una password altamente sicura -puoi saperne di più consultanto il nostro Toolkit «Best Practice».

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.

Grazie per l’attenzione!

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.