


Quali insegnamenti possiamo trarre dal COVID-19: sicurezza e pianificazione della continuità

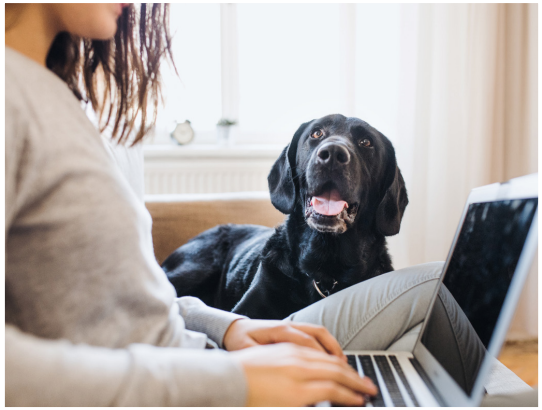
WatchGuard®

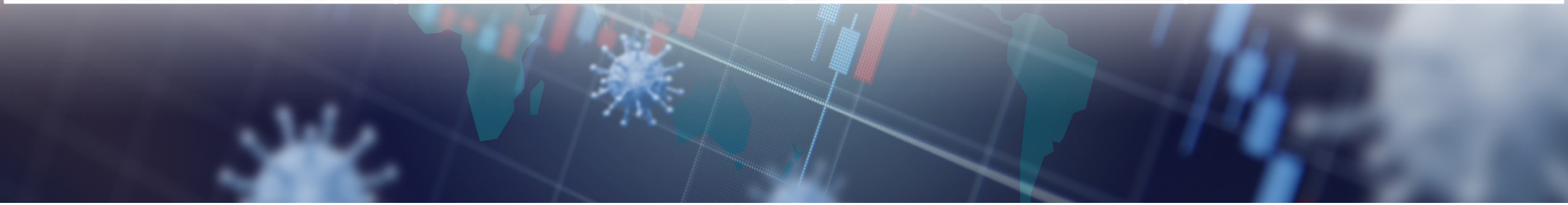
Sommario

INTRODUZIONE

Mentre il nuovo coronavirus (COVID-19) si diffonde in pressoché tutto il mondo, la società si trova a fronteggiare una pandemia di proporzioni mai viste. Le scuole sono chiuse, i viaggi limitati, gli eventi vengono annullati e gli uffici si svuotano: tutti questi provvedimenti allo scopo di limitare la diffusione del COVID-19. Il CDC (Center for Disease Control) ha addirittura consigliato ai datori di lavoro di adottare policy per consentire ai dipendenti di lavorare da remoto in modo da favorire il distanziamento sociale. Recependo l'invito, le aziende si sono rapidamente mobilitate per far fronte alla minaccia e, di conseguenza, oggi il numero di persone che lavorano da casa è più elevato che mai nella storia recente. Semplicemente per dare un'idea di quanto siano alte le cifre, secondo uno studio, in America i telelavoratori sono aumentati del 159% negli anni compresi fra il 2005 e il 2017. È corretto affermare che oggi, a causa dell'epidemia di coronavirus, i numeri sono aumentati enormemente.

Per quanto la risposta al coronavirus non abbia precedenti, per molte aziende la formula di lavorare da casa è un esperimento che le proietta in territori decisamente inesplorati. In questo e-book verranno esposte alcune strategie per mantenere la continuità aziendale durante l'epidemia di coronavirus.





ANALISI DELLA SITUAZIONE DEL COVID-19:
LE ATTUALI SFIDE PER LA CONTINUITÀ AZIENDALE

I rischi legati alla sicurezza informatica sono sempre presenti. Tuttavia, una delle problematiche derivanti dall'avere una forza lavoro operativa a distanza è che le probabilità di essere vittima di attacchi informatici aumentano significativamente. Senza i benefici forniti dalle protezioni della rete principale, gli utenti in mobilità possono infettarsi senza che l'IT aziendale ne venga a conoscenza e quindi propagare l'infezione a tutto l'ambiente quando si riconnettono alla rete.

Gli hacker sfruttano la paura del coronavirus

Appare chiaro che, per sferrare gli attacchi, gli hacker approfittano di qualsiasi novità importante o evento mondiale. In questo momento di grande paura, le caselle e-mail e gli account dei social media dei dipendenti sono inondati di notizie, commenti, video e link sul virus. Purtroppo i criminali informatici fanno leva sulle paure per mettere a segno attacchi di phishing, entrare nei sistemi degli utenti o infiltrare malware.

Di seguito alcuni esempi di come gli autori delle minacce sfruttano il coronavirus:

- **Fingendosi l'Organizzazione Mondiale della Sanità** (OMS). L'OMS ha segnalato messaggi di phishing sospetti che sembravano provenire dall'organizzazione e affermavano di avere importanti informazioni sanitarie da fornire. Alle vittime veniva richiesto di fare clic su un link, scaricare un file o comunicare informazioni sensibili.
- **Infiltrando malware.** Un gruppo di hacker ha sfruttato l'epidemia di coronavirus per infettare vittime in Mongolia utilizzando un malware sconosciuto in precedenza, con una campagna che è stata recentemente scoperta, denominata "Vicious Panda".
- **Diffondendo il trojan Emotet**. Gli hacker si sono serviti di avvisi che sembravano utili per prevenire la diffusione del coronavirus inviandoli a utenti mirati in Giappone, nell'ambito di una campagna di spam ideata per infiltrare il trojan Emotet. Emotet è in grado di "dirottare" account e-mail e di eseguire lo spoofing dei messaggi per infiltrarsi più in profondità nell'ambiente.
- **Utilizzando una falsa app di tracciamento del virus che introduce ransomware.** Un'app che si spaccia per un sistema di tracciamento dell'epidemia di coronavirus consiste di fatto in un ransomware che blocca il telefono. "COVID19 Tracker", questo il nome dell'app, infetta il dispositivo e richiede un riscatto di 100 dollari in Bitcoin entro 48 ore.

Utenti inesperti fuori dalla rete

Con le aziende costrette a chiudere gli uffici pressoché dall'oggi al domani, il COVID-19 sta determinando l'adozione di risolute policy per favorire il lavoro da casa per gran parte dei dipendenti. Mentre la flessibilità sul luogo di lavoro è ormai la norma per molte attività, in un'azienda media soltanto il 30% della forza lavoro è in grado di lavorare da casa in un dato momento. Molte società si sono adoperate per mettere a disposizione le risorse necessarie a garantire la sicurezza delle persone che lavorano da casa, fornendo in tutta fretta computer portatili ai dipendenti o mandandoli a casa con dei computer fissi che non erano nati per l'uso all'esterno della rete protetta. Questi dispositivi non solo necessitano di sicurezza ora che vengono utilizzati all'esterno della rete, ma è anche necessario assicurarsi che non introducano malware o altre minacce una volta che si riconnetteranno alla rete tramite la VPN o al rientro in ufficio.

VPN sovraccariche

Con il coronavirus cha ha confinato i dipendenti in casa, l'utilizzo delle VPN è aumentato vertiginosamente, i ricercatori stimano infatti che l'incremento del traffico sia stato del 50% nell'arco di una settimana. Soltanto negli Stati Uniti, si prevede che l'utilizzo delle VPN aumenti del 150% in un mese di tempo. L'improvvisa migrazione di utenti dagli uffici aziendali a postazioni di lavoro domestiche ha indotto molte aziende a fare salti mortali per fornire ai dipendenti licenze VPN. Il rischio è che, senza connettività VPN, gli utenti non possano accedere alle risorse necessarie oppure che utilizzino connessioni non sicure per accedervi.

Il problema della larghezza di banda

Non sono solo i dipendenti a dover restare a casa. Con le scuole chiuse, anche bambini e ragazzi seguono lezioni da remoto, giocano o semplicemente navigano in Internet. Tutti quindi consumano larghezza di banda, soprattutto se utilizzano applicazioni che impiegano molte risorse, come quelle per la videoconferenza. Nelle località più colpite dal virus si è assistito a un incremento dell'uso di Internet fino al 90%. Come risposta, molti ISP stanno offrendo ai clienti una maggiore velocità o larghezza di banda, oppure eliminano i limiti di dati per evitare sconfinamenti dai piani prestabiliti.

L'utilizzo delle VPN è aumentato vertiginosamente, **raggiungendo il 50% di incremento del traffico nell'arco di una settimana**.

Soltanto negli Stati Uniti, si prevede che **l'utilizzo delle VPN aumenti del 150% nell'arco di un mese**.

OTTO SUGGERIMENTI RIVOLTI AI LEADER DEI TEAM IT PER UTILIZZARE LA SICUREZZA COME MEZZO PER FORNIRE L'ACCESSO E FAVORIRE LA PRODUTTIVITÀ

1. INVENTARIARE E VALUTARE LE RISORSE AZIENDALI PER IL TELELAVORO

Sebbene il 92% delle aziende offra la possibilità di lavorare a distanza, questa opportunità non è stata resa disponibile in egual misura a tutti i dipendenti. Per molte società, il passaggio al telelavoro è avvenuto repentinamente e non c'è stato il tempo di provvedere a una pianificazione adeguata. Ora è arrivato il momento di verificare e valutare le nuove necessità di accesso alla rete e di considerare le implicazioni a livello di sicurezza. I fornitori di servizi di sicurezza gestita (MSSP) sono esperti nella valutazione della sicurezza e sono in grado di aiutare le aziende di medie dimensioni ad acquisire maggiore velocità e a soddisfare le esigenze dei propri utenti.

Chi è abituato a lavorare a distanza ed è sempre in viaggio probabilmente già dispone delle risorse necessarie anche nel lungo periodo. Per le persone che prima non lavoravano da casa, può invece essere utile stilare un inventario di tutti i dati e le applicazioni a cui accedono regolarmente. Partendo da questo, sarà possibile stabilire a quali sistemi devono avere accesso, chi ha la necessità di accedere e quale sia il modo migliore di fornire questi accessi. Collaborando con i capireparto si potranno recepire le esigenze specifiche dei vari team e predisporre ciò che serve.

Di seguito un elenco di controllo dei fattori da prendere in considerazione:

- ✔ Il dipendente dispone di un dispositivo soggetto a restrizioni o è necessario acquistare altri telefoni/computer portatili?
- ✔ Le licenze VPN presenti in azienda sono sufficienti per essere distribuite a tutti gli utenti a cui servono o è necessario a cquistarne altre?
- ✔ Il dipendente dispone di un accesso a Internet adeguato per svolgere le sue mansioni?
- ✔ Di che sistemi ha bisogno per svolgere le sue mansioni?
- ✔ Necessita di un accesso sicuro a sistemi e dati sensibili?
- ✔ Quali applicazioni cloud utilizza regolarmente?
- ✔ È configurata l'autenticazione a più fattori per il dipendente?

2. STABILIRE QUALI SONO LE ASPETTATIVE IN MATERIA DI TELELAVORO E COMUNICARLE

È probabile che per molti dipendenti dell'azienda questa sia la prima esperienza di telelavoro, ecco perché questo è il momento giusto per comunicare al team la policy aziendale sul telelavoro e chiarire quali sono le aspettative nei confronti di chi lavora da remoto. Circa il 24% delle aziende non aggiorna la propria policy sul telelavoro da oltre un anno, quindi questa potrebbe essere un'opportunità per farlo. Una semplice e-mail o una chiamata in conferenza con i membri del team possono essere molto efficaci.

Alcune questioni che può essere utile risolvere:

- **Disponibilità**: quali sono gli orari di lavoro previsti per il team? Quando sarà disponibile l'IT?
- **Velocità di risposta**: i telelavoratori devono rispondere immediatamente? In tal caso, in che modo rendere nota questa aspettativa? Ad esempio, le richieste realmente urgenti devono essere avanzate esclusivamente per telefono?
- **Piattaforme**: è opportuno ricordare ai dipendenti quali strumenti e piattaforme devono utilizzare, incluse piattaforme di archiviazione in cloud, strumenti di comunicazione/videoconferenza, strumenti per la gestione dei progetti, ecc., invitandoli a evitare tutte le altre piattaforme non soggette a restrizioni.
- **Dispositivi**: se il team utilizza dispositivi aziendali, è bene ricordare alle persone quali sono le policy riguardanti l'utilizzo di queste risorse. Se invece per lavoro vengono utilizzati i dispositivi personali, questo è un buon momento per fornire un'indicazione di quali dispositivi sono adatti a questo scopo e in che modo devono essere svolte le attività lavorative su tali dispositivi.
- **Segnalazione di incidenti**: che cosa deve fare un dipendente qualora abbia il sospetto che le informazioni dell'azienda possano essere state compromesse? A chi deve segnalare la violazione e quali procedure deve seguire per limitare le conseguenze negative?

3. PROMUOVERE UNA CULTURA CHE FAVORISCA LA SICUREZZA INFORMATICA

Molti responsabili aziendali sanno che la cultura del luogo di lavoro è un elemento importante nel determinare il successo o il fallimento. Devono ora rendersi conto che la stessa dinamica vale per la sicurezza informatica. Quando i dipendenti sono sotto la minaccia di attacchi mirati, come nel caso che qualcuno si finga un membro del team, spesso è proprio la cultura aziendale a fare la differenza e a consentire di intercettare l'attacco o impedire che infetti l'intera rete.

Gli hacker si avvalgono di diverse tecniche e utilizzano come armi l'autorità e l'urgenza per manipolare gli utenti e indurli ad agire secondo i loro desideri. I responsabili devono favorire l'apertura di canali di comunicazione, in modo che, se un dipendente, anche al livello più basso dell'organizzazione, si rende conto di qualcosa che potrebbe costituire una minaccia, si senta autorizzato a segnalarlo sapendo che riceverà la dovuta attenzione.

Suggerimenti per promuovere una cultura che favorisca la sicurezza informatica:

- **Raccontare i fatti.** Se un dipendente identifica un'e-mail di phishing o scopre che il suo computer portatile è infettato da ransomware, condividere in azienda ciò che gli successo può servire a chiarire agli altri qual è la posta in gioco oltre che a evitare attacchi analoghi. Può essere utile anche parlare di attacchi simili subiti da altre aziende.
- **Premiare i comportamenti virtuosi.** Se i dipendenti segnalano un possibile attacco, potrebbero evitare grossi problemi all'azienda, quindi perché non premiarli per questo comportamento? Incentivare i dipendenti a segnalare le attività sospette può essere utile per suscitare la consapevolezza e coinvolgere gli altri.
- **Essere cortesi.** Diciamocelo, nelle aziende ci sono persone con un livello molto variabile di competenze tecnologiche. Semplicemente non è realistico pensare che i dipendenti possano evitare tutte le minacce e seguire tutte le policy. Le persone sbagliano. Per questo è importante avere un atteggiamento incoraggiante.

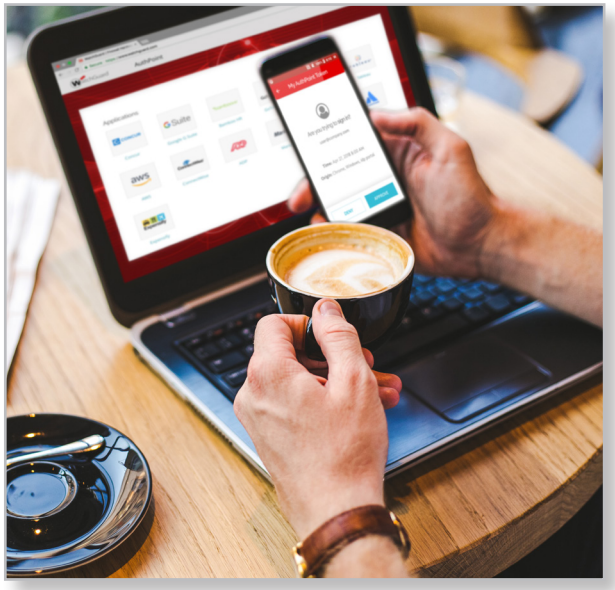
4. IMPLEMENTARE L'AUTENTICAZIONE A PIÙ FATTORI

Ora che le aziende si trovano a gestire una forza lavoro che opera per lo più da remoto, la protezione dell'accesso agli strumenti interni diviene un problema di grande rilievo. Per di più gli hacker mirano sempre più a carpire le credenziali, puntando direttamente sulle informazioni degli account utente. Per questo motivo, è consigliabile implementare l'autenticazione a più fattori (MFA) per tutti gli utenti, così da autenticarli in modo completo ogni volta che si connettono alla rete.

L'autenticazione a più fattori consente di proteggere l'accesso alle applicazioni e agli ambienti cloud a cui i telelavoratori possono accedere direttamente da Internet, aggiungendo un ulteriore livello di protezione in un momento in cui le aziende sono più vulnerabili.

Caratteristiche da ricercare in una soluzione MFA:

- **Disponibilità nel cloud.** A differenza dell'autenticazione MFA, per la quale è necessario un token hardware, le soluzioni basate su cloud permettono agli utenti di scaricare un'applicazione sul telefono ed essere subito operativi.
- **Copertura delle applicazioni.** La soluzione scelta deve essere integrabile per proteggere le applicazioni critiche necessarie ai dipendenti.
- **Semplicità.** La soluzione deve essere intuitiva per gli utenti, anche quelli con meno competenze tecniche.
- **Diversi metodi di autenticazione.** Supporto di varie opzioni di autenticazione sia online che offline per garantire che gli utenti autorizzati possano accedere agli strumenti di cui hanno necessità, quando servono.
- **Supporto di vari token.** Oggi l'autenticazione MFA viene generalmente fornita da siti di social media, banche, rivenditori, ecc. È utile dotarsi di una soluzione che permetta di consolidare i token in un'applicazione MFA intuitiva per semplificare l'accesso da parte degli utenti.



5. ESTENDERE L'ACCESSO ALLA VPN AGLI UTENTI PRIORITARI

Affinché i dipendenti mantengano la stessa produttività lavorando da remoto, è essenziale una connessione sicura alla sede principale dell'azienda e alle applicazioni critiche. Le reti private virtuali (VPN) aggiungono un livello di sicurezza alle reti private e pubbliche, consentendo a persone e organizzazioni di inviare e ricevere dati via Internet in modo sicuro.

Gli utenti, in genere, necessitano di due tipi di VPN:

1. **VPN basata su client.** Operante al livello della rete, una VPN basata su client fornisce agli utenti l'accesso a tutta la rete.

2. **VPN senza client.** Le VPN senza client in genere richiedono semplicemente un browser e connettono gli utenti ad applicazioni e servizi specifici.

Di norma le aziende forniscono VPN soltanto a un gruppo limitato di dipendenti che lavorano da remoto o viaggiano spesso, non a tutto il personale. Poiché nelle attuali circostanze l'uso delle VPN si sta espandendo esponenzialmente, di seguito sono forniti alcuni suggerimenti per gestirne l'utilizzo ed evitare interruzioni:

- **Concedere priorità nell'uso della VPN agli utenti ad alto rischio**. Per alcuni dipendenti l'accesso alla VPN può essere più importante che per altri e per qualcuno potrebbe addirittura non essere necessario. Sapere chi ha la necessità di accedere e a quali sistemi e rendere disponibile la VPN in base alle priorità può essere utile per evitare di sovraccaricare la rete.

- **Utilizzare un firewall in cloud per far fronte alla domanda.** Registrare un picco nella domanda di servizi VPN non implica necessariamente dover fare spazio nella stanza dei server. I firewall in cloud aiutano a bilanciare i carichi del traffico destinato alla sede centrale sulla VPN e sono scalabili in base alle connessioni necessarie per l'azienda.

- **Imporre l'autenticazione MFA.** Senza MFA, anche una sola serie di credenziali VPN potrebbe conferire a malintenzionati l'accesso totale alla rete. Gli utenti che si connettono utilizzando la VPN devono essere autenticati in modo completo utilizzando come minimo due fattori.

- **Distribuire un firewall tabletop.** L'implementazione di un firewall tabletop negli uffici domestici degli utenti può fornire una protezione UTM completa senza appesantire la VPN aziendale.

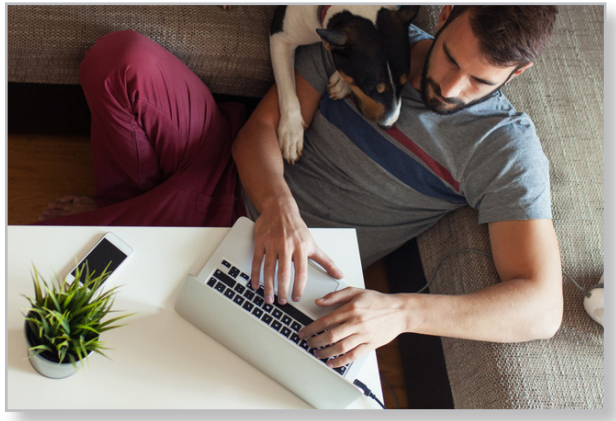
6. GARANTIRE LA SICUREZZA DEGLI UTENTI DAI CLIC PERICOLOSI CON FILTRI DNS

È più complesso garantire la sicurezza degli utenti che navigano in Internet se si connettono dall'esterno della rete. Con i dipendenti bloccati a casa, è probabile che i computer portatili aziendali vengano utilizzati anche per una serie di attività personali di navigazione in rete e controllo dell'e-mail. I filtri DNS in cloud permettono di bloccare le connessioni e limitare l'accesso ad aree di Internet rischiose. È in tal modo possibile evitare clic su link dannosi o tentativi di connessione a domini correlati a phishing e malware senza passare per la VPN.

Fattori da considerare per una soluzione basata su filtri DNS:

- **Produttività e applicazione delle policy.** Con più dipendenti che lavorano fuori ufficio, per motivi di produttività, potrebbe essere utile anche limitare l'accesso degli utenti a determinati tipi di contenuti, ad esempio social media e siti per adulti. Si possono adottare controlli granulari, come la capacità di bloccare utenti e gruppi, oltre che stabilire gli orari in cui queste regole devono essere applicate.

- **Supporto per iniziative di training sulla sicurezza.** Molte aziende hanno già varato iniziative di training sulla sicurezza informatica per i dipendenti, ma dato che adesso lavorano fuori ufficio, è più importante che mai in questo momento rafforzare le conoscenze in materia. Alcune soluzioni di filtri DNS non solo bloccano le connessioni pericolose, ma forniscono anche un aggiornamento all'utente su come identificare minacce simili ed evitarle in futuro.



7. MANTENERE GLI ENDPOINT LIBERI DA MALWARE

Per effetto del coronavirus, le minacce costituite da malware e ransomware sono aumentate e il rischio di infezione non è mai stato così elevato, in quanto, lavorando da casa, gli utenti non possono più beneficiare della protezione di un firewall. Sebbene le soluzioni antivirus per gli endpoint intercettino molte delle minacce, non hanno alcun potere contro il malware elusivo zero day che osserviamo anche troppo spesso. Le soluzioni di rilevamento e risposta per gli endpoint (EDR) non solo rilevano anche queste minacce avanzate, ma sono in grado di neutralizzarle e riportare al normale funzionamento il dispositivo infettato agendo al 100% da remoto.

Funzioni essenziali di una soluzione EDR:

- **Metodi di rilevamento.** Per individuare malware avanzato occorrono tecniche avanzate. Sono da preferire le soluzioni che utilizzano diversi metodi di rilevamento, fra cui analisi comportamentale ed euristica e sandbox.

- **Automazione e IA.** Una risposta rapida alle minacce può evitare di incorrere in gravi problemi. Automatizzando il rilevamento e la risposta, l'effetto è pressoché istantaneo.

- **Isolamento dell'host.** Quando viene rilevata una minaccia, si deve interrompere la connessione dell'host infettato con le altre parti della rete, per evitare che l'infezione si propaghi.

8. Mantenere il controllo del Wi-Fi

Il lavoro da casa può comportare problemi di sicurezza anche per quanto riguarda il Wi-Fi. Per chi abita in zone residenziali ad alta densità di popolazione, ad esempio in palazzi e condomini, tutti i dispositivi Wi-Fi, inclusi citofoni, console di giochi e dispositivi IoT, possono costituire un punto di vulnerabilità sfruttabile da vicini malintenzionati, che potrebbero trarre vantaggio dal fatto che nello stesso stabile lavorano da remoto molte persone e il Wi-Fi rappresenta circa il 50% di tutto il traffico IP.

Considerazioni sul Wi-Fi per il telelavoro:

- **Prendere in considerazione l'adozione di access point certificati in ambiente wireless attendibile**, come WatchGuard AP225W, per conferire al reparto IT aziendale la piena visibilità sulle prestazioni dei client e della rete, in modo da poter supportare al meglio i telelavoratori.
- **Preconfigurare gli access point** per facilitare l'implementazione da parte degli utenti a casa.

In zone residenziali ad alta densità di popolazione, ad esempio nei condomini, il Wi-Fi costituisce quasi il **50% di tutto il traffico IP**.

PERCHÉ È IMPORTANTE CHE LE AZIENDE SIANO PREPARATE QUANDO SI PARLA DI SICUREZZA IT

Detto in maniera semplificata: non si può prevedere tutto. I responsabili aziendali sanno che ci saranno ostacoli ed eventi imprevisti lungo il percorso. Che cosa si può fare quindi per proteggere il futuro del business? Un programma per essere preparati non è garanzia di perfezione, ma può fornire gli strumenti giusti per affrontare le sfide in maniera controllata e le risorse necessarie a garantire la continuità operativa.

In questo momento si tratta dell'epidemia di coronavirus, ma potrebbe anche essere altro, non necessariamente una calamità. Eventi importanti che sovvertono il normale funzionamento di una città, ad esempio la coppa del mondo, oppure un errore umano, possono spingere le aziende a ricorrere ai piani di emergenza. Qualunque situazione che spinga ad adattarsi rapidamente a cambiamenti improvvisi costituisce la prova suprema di quanto sia importante conoscere bene l'organizzazione e le sue esigenze.

Perché? Perché dimostra a dipendenti, clienti e altri soggetti chiave che l'azienda è in grado di operare anche in situazioni senza precedenti e questo è un vantaggio per il marchio, ma soprattutto instaura un grande senso di affidabilità nella community e crea un precedente di valore per gli anni a venire.

Perché? Perché dimostra a dipendenti, clienti e altri soggetti chiave che l'azienda è in grado di operare anche in situazioni senza precedenti.

ELENCO DI CONTROLLO PER LA CONTINUITÀ AZIENDALE DELL'IT

Valutazione delle risorse aziendali per il telelavoro

L'azienda è preparata?	Sì	No	Azione
La policy aziendale sul telelavoro è stata aggiornata nel corso degli ultimi 12 mesi?			
Sono state comunicate le aspettative ed è stata resa nota la policy relativa al telelavoro per tutti i dipendenti?			
È necessario acquistare altri telefoni/computer portatili in modo che tutti i dipendenti possano disporre di un dispositivo soggetto a restrizioni?			
Le licenze VPN sono sufficienti per essere distribuite quando servono?			
Il dipendente dispone di un accesso a Internet adeguato per svolgere le sue mansioni?			
È stato verificato se i dipendenti che lavorano da remoto hanno accesso ai sistemi o alle piattaforme necessarie per svolgere adeguatamente le loro mansioni? *ad es., applicazioni cloud*			
L'azienda è in grado di applicare misure di sicurezza per evitare il rischio di attacchi informatici anche lavorando da remoto? *ad es., Wi-Fi protetto, connessione VPN, autenticazione a più fattori*			
È necessario rivedere il budget IT per fornire le risorse necessarie?			
È necessario svolgere training sulla sicurezza per il personale che lavora da remoto?			

SERVIZI GRATUITI UTILI PER LE PICCOLE E MEDIE IMPRESE IN QUESTA SITUAZIONE SENZA PRECEDENTI

Per un periodo di tempo limitato, WatchGuard offre servizi gratuiti o a prezzi scontati per aiutare le aziende a proteggere i propri telelavoratori. Visita la nostra **pagina di risorse per i telelavoratori** per informazioni sulle offerte speciali di WatchGuard Passport, è disponibile anche un pacchetto di servizi di sicurezza incentrati sugli utenti, concepiti per bloccare i tentativi di phishing, applicare la policy per il web e autenticare le persone da qualsiasi ubicazione geografica.

Scopri di più

Per maggiori dettagli, contatta il tuo rivenditore WatchGuard autorizzato o visita **https://www.watchguard.com.**.

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella fornitura di servizi relativi a sicurezza di rete, Wi-Fi protetto, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi della nostra azienda hanno ottenuto la fiducia di circa 10.000 rivenditori in tutto il mondo, che provvedono alla sicurezza di più di 80.000 clienti. La missione di WatchGuard è rendere la sicurezza accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, facendo di WatchGuard la soluzione ideale per le aziende distribuite e le piccole e medie imprese. La sede centrale di WatchGuard si trova a Seattle (Washington, Stati Uniti); l'azienda dispone di uffici dislocati in Nord America, Europa, Asia e America Latina. Per saperne di più, visita WatchGuard.com.

WatchGuard

Vendite Italia: 800-911-938 • Vendite internazionali: 1.206.613.0895 • Web: www.watchguard.com/it

Cod. articolo WGCE67298_040720