CIBA BROKERS
COMPAGNIA ITALIANA BROKERS DI ASSICURAZIONE

Dieci consigli per proteggersi da attacchi cyber quando si lavora da casa

Sia per lavoro che per uso personale, la nostra dipendenza dalla tecnologia non è mai stata così elevata. Man mano che questa dipendenza cresce, aumentano anche i rischi informatici ad essa associati, specialmente quando più persone lavorano o studiano da casa.

I criminali informatici sanno che quando più persone comunicano online, interagiscono con la tecnologia attraverso diverse modalità, utilizzando anche reti o software per la prima volta: spesso, quindi, tentano di sfruttare queste situazioni, usando l'inganno per ottenere accesso a informazioni protette. Allo stesso tempo, i team aziendali IT e Operations lavorano fuori orario per mantenere le reti attive senza interruzione, influendo potenzialmente sulla capacità delle stesse di rilevare rapidamente attività dannose.

Ciò rende la protezione delle informazioni riservate estremamente impegnativa. Come Ciba Brokers, desideriamo fonire spunti utili per prevenire eventuali problemi. Seguire questi dieci suggerimenti può aiutare aziende e dipendenti a proteggersi da attacchi informatici, anche in periodi di incertezza.

Best practice aziendali

1 Prepararsi ad affrontare i problemi delle risorse IT, sia dal punto di vista del personale sia a livello tecnologico

Quando più persone si connettono in remoto, gli help desk potrebbero dover affrontare un volume di chiamate più elevato del normale e potrebbero essere necessarie più risorse al di fuori dell'orario standard di lavoro. Allo stesso tempo, la larghezza di banda della rete, le capacità di archiviazione dei dati e la potenza di elaborazione vengono messe alla prova. Nonostante questo aumento del traffico, l'attenzione ai dettagli non può mancare. Le aziende sono incoraggiate a considerare tali esigenze, preparare un piano per riallocare le risorse in base alle necessità e prendere atto che questa dipendenza dalla tecnologia potrebbe aumentare nel tempo.

2 Assicurarsi che rete, software e applicazioni siano aggiornati

Le tecnologie di accesso da remoto presentano vulnerabilità note e sono molto spesso l'anello debole che i criminali informatici utilizzano per accedere alle informazioni protette. Assicurarsi che tutti i software e le applicazioni siano aggiornati e rimediare a eventuali punti deboli identificati.

3 Assicurarsi che le risorse siano allineate, prima che si verifichi un incidente

Le organizzazioni dovrebbero assicurarsi che i loro piani di business continuity, i team di ripristino di emergenza e i piani di risposta agli incidenti informatici siano allineati. I criminali informatici sanno che la dipendenza dalla rete e dalla sua disponibilità sono tanto più alte quante più persone accedono ad essa da remoto, e tenteranno di sfruttare questa situazione.

4 Rivedere le policy in atto e monitorare tutte le possibili eccezioni in termini di sicurezza

Quando le risorse IT vengono portate al limite, le organizzazioni potrebbero dover fare alcune eccezioni alle policy, agli standard o alle pratiche di sicurezza esistenti. Va attuato un processo di revisione approfondito per garantire che tali eccezioni siano attentamente monitorate e risolte. Inoltre, la maggior parte delle politiche di smart working non erano state originariamente elaborate in vista di una conversione globale al lavoro da remoto; anch'esse andrebbero quindi riviste attentamente.

sede legale e direzione generale
Palazzo Confcooperative
via A. Calzoni, 1/3
40128 Bologna
tel. 051 7096411 - fax 051 7096422

sede di Rimini
Via Caduti di Marzabotto, 38
47922 Rimini
tel. 0541 410927 - fax 0541 412413

sede di Forlì
Via Oriani, 1
47121 Forlì
tel. 0543 35074 - fax 0543 27089

sede di S. Marino
Via Strada Rovereta, 42
47891 Falciano (RSM)

sede di Ancona
Via Ghino Valenti, 1

segreteria@cibabrokers.it
cibabrokers@registerpec.it
www.cibabrokers.it

CIBA BROKERS
COMPAGNIA ITALIANA BROKERS DI ASSICURAZIONE

5 Usare l'autenticazione a più fattori: se non è già stata implementata, ora è il momento

Gli account con accesso tradizionale (nome utente e password) sono facili da penetrare. Ogni qual volta possibile, l'autenticazione a più fattori va impostata su tutti gli account. Ciò richiede che si forniscano almeno due fattori di autenticazione, o prove di identità, prima di poter accedere a dati protetti, creando così una seconda linea di difesa contro le attività criminali. Questo ulteriore livello di protezione è molto importante quando più persone accedono alle reti da remoto, ovvero quando i criminali informatici dispongono di più punti di accesso alle reti private.

Best practice per i dipendenti

6 Connettersi a Internet solo tramite una rete protetta

Quando si è connessi a una rete pubblica, qualsiasi informazione condivisa online o tramite app mobile può essere letta da qualcun altro. Va sempre utilizzata una rete privata virtuale (VPN) per crittografare la propria attività. La maggior parte delle aziende fornisce una VPN ai propri dipendenti, per garantire un accesso remoto sicuro per uso lavorativo. Account VPN personali sono offerti da vari fornitori di servizi.

7 Usare password complesse

Molte persone usano una versione simile o la stessa password per ogni loro attività, sia lavorativa sia personale. Purtroppo, questo significa che una singola password rubata può essere riutilizzata dagli hacker su più siti per sbloccare dozzine di account. Ricordare password sicure e complesse per ogni account può essere difficile, se non impossibile. È consigliabile utilizzare un software di gestione delle password, per assicurarsi di disporre sempre di password complesse e uniche. Le password sono infatti la base di solide pratiche in materia di sicurezza online.

8 Cliccare su link, aprire allegati e scaricare software solo se provenienti da risorse affidabili

Molte persone vogliono rimanere informate sulle ultime notizie, specialmente durante i periodi di incertezza. I criminali informatici lo sanno e tenteranno di trarne vantaggio mascherando collegamenti dannosi come link informativi. Una volta cliccato, quel link dannoso può essere usato per accedere alle informazioni private di una persona o di un'azienda e/o congelare computer o reti. Se non si è sicuri della fonte, consultare il sito web ufficiale dell'organizzazione in questione. Se sono rilevanti, le informazioni saranno pubblicate anche in quella sede.

9 Verificare gli URL dei siti web prima di condividere informazioni riservate

I criminali informatici possono creare siti web fasulli in cui sia l'URL che la homepage appaiono molto simili a quelli di un sito affidabile, come il proprio fornitore di assistenza sanitaria, la banca o il provider di posta elettronica. Invece di seguire il collegamento nell'e-mail, è conveniente digitare l'URL manualmente. E assicurarsi che il sito che si sta visitando contenga HTTPS nell'URL: questi siti sono più sicuri di quelli con HTTP

10 Non rispondere a richieste di informazioni da fonti sconosciute, soprattutto se la richiesta riguarda informazioni o password identificabili come personali

I criminali informatici cercheranno di convincere le persone a condividere informazioni riservate, fingendo di essere un nostro conoscente o collaboratore di lavoro. Prestare particolare attenzione nell'identificare con chi si condividono le informazioni, anche se si ritiene che la richiesta provenga da una risorsa o organizzazione attendibile. Non essere frettolosi: prima di rispondere, prendersi il tempo necessario per verificare la richiesta e capire se è appropriata.

Ridurre al minimo i rischi informatici e rispondere a una crisi

Ogni polizza Ciba Brokers offre strumenti e servizi per rispondere rapidamente a incidenti informatici gravi. I consulenti Ciba Brokers sono a vostra disposizione presso ogni sede operativa, per una consulenza personalizzata: i riferimenti sono pubblicati a lato.

sede legale e direzione generale
Palazzo Confcooperative
via A. Calzoni, 1/3
40128 Bologna
tel. 051 7096411 - fax 051 7096422

sede di Rimini
Via Caduti di Marzabotto, 38
47922 Rimini
tel. 0541 410927 - fax 0541 412413

sede di Forlì
Via Oriani, 1
47121 Forlì
tel. 0543 35074 - fax 0543 27089

sede di S. Marino
Via Strada Rovereta, 42
47891 Falciano (RSM)

sede di Ancona
Via Ghino Valenti, 1

segreteria@cibabrokers.it
cibabrokers@registerpec.it
www.cibabrokers.it