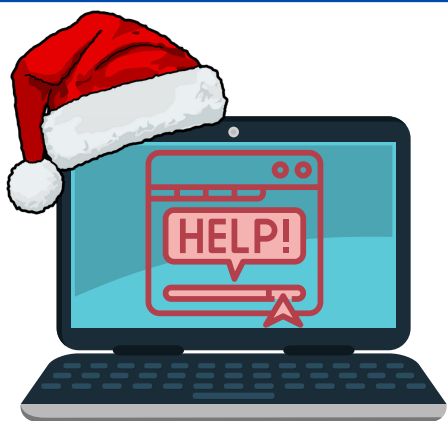


Bonus Track #1: Natale, cosa fai prima di chiudere per ferie?

Business Provider
COREUP



Sai qual è il periodo preferito dai **cybercriminali** per sferrare i loro attacchi hacker alle aziende?

Durante i giorni di chiusura, quindi il **periodo natalizio** è un momento perfetto. Perché? Quando gli uffici sono fermi o molti dei collaboratori sono in ferie, l'attenzione è minore e si è più vulnerabili a subire un attacco.

Ci sono però delle strategie per tenere i dati al sicuro, anche quando non ci sei.

"Ma se in ufficio non c'è nessuno e i pc sono spenti siamo al sicuro!"

Ci sentiamo dire spesso questa frase. La nostra risposta è: "Sì, ma anche no".

Esistono infatti dei malware (chiamati **"logic bomb"**) che possono essere installati e rimanere nascosti per mesi prima di attivarsi. Ecco perché ogni momento andrebbe monitorato da un **MSP** e la **rete protetta**. Come? Con EDR, MDR, XDR, Firewall, etc.

I cybercriminali usano modalità di attacco sempre diverse e in continua evoluzione. Non dobbiamo più immaginare l'hacker solitario che attacca dal suo nascondiglio, bensì aziende strutturate, create per frodare utilizzando sistemi automatizzati che scandagliano le **vulnerabilità** e attaccano quindi a colpo sicuro.

Alcuni consigli per proteggersi dagli attacchi hacker (non solo a Natale!):

- Aggiorna sempre il software del tuo pc: gli aggiornamenti di sicurezza includono patch per vulnerabilità che possono essere sfruttate dai criminali informatici.
- Utilizza una password forte e diversa per ogni account online. Hai mai sentito parlare di Keeper?
- Evita di aprire email o allegati da fonti sconosciute.

CHECK UP: COSA CONTROLLARE PRIMA DELLA CHIUSURA NATALIZIA

Prima di andare in ferie è buona norma controllare alcune cose per godersi il riposo senza pensieri e tenere l'azienda al sicuro.

Ecco alcune domande utili per fare un check dei **#todo** pre-ferie:

- I **backup** sono disponibili e consultabili?
- Hai verificato che i gruppi di **continuità** possano garantire la copertura energetica in caso di mancanza di energia elettrica?
- Hai valutato se è il caso di spegnere parte della tua **infrastruttura IT** o di lasciarla accesa?
- Hai verificato se i sistemi di **sicurezza** sono aggiornati?
- Hai verificato che il condizionatore in sala server e/o il termostato della sala CED funzionino alla perfezione?

Hai dei dubbi? Chiamaci .

030.4194040
info@coreup.it
www.coreup.it

Core Up Srl
Via Bruno Buozzi, 1/A
25125 Brescia (BS)



Seguici
su LinkedIn:
Core Up Srl

Bonus Track #2: le frodi e i pericoli del web nel periodo natalizio



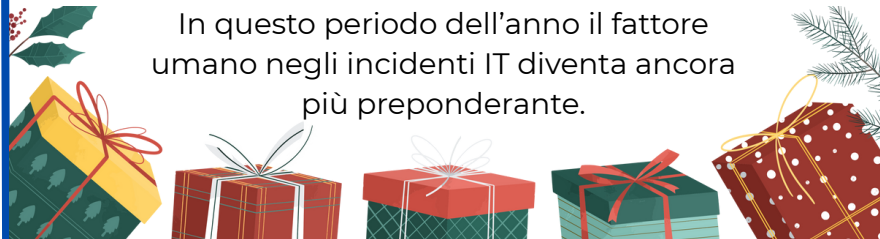
I mesi di novembre e dicembre, cioè il periodo prefestivo natalizio, sono i più proficui per le **frodi informatiche** ai danni degli utenti che intensificano gli acquisti online proprio in vista del Natale.

Quindi le **credenziali** dei servizi online sono a **rischio** soprattutto in questo momento dell'anno.

STRESS E FRETTA: I NEMICI DELLO SHOPPING NATALIZIO ONLINE

La corsa ai regali genera stress e spesso viene gestita di fretta: questa situazione rende gli **utenti più vulnerabili** e meno attenti. I cybercriminali lo sanno e sfruttano proprio questa situazione per attaccare.

In questo periodo dell'anno il fattore umano negli incidenti IT diventa ancora più preponderante.



QUALI SONO LE MINACCE ONLINE PIÙ COMUNI SOTTO NATALE?

I pericoli del web da cui imparare a difendersi e che vanno per la maggiore sotto Natale sono:

Phishing: attenzione alle finte e-mail che sembrano provenire da marchi noti mentre hanno l'obiettivo di rubare dati personali e finanziari invitando a cliccare su link malevoli.

E-commerce fasulli: soprattutto a Natale vengono creati finti siti di shopping online che offrono regali natalizi a prezzi convenienti ma sono generati solo per rubare i dati della carta di credito dell'acquirente.

Furto d'identità: i cybercriminali possono rubare i dati sensibili sia per accedere a conti bancari sia per commettere azioni illecite sfruttando l'identità rubata.

MASSIMA ATTENZIONE QUANDO SI ACQUISTA ONLINE: ECCO COSA CONTROLLARE

Core Up raccomanda di prestare la massima attenzione quando si compra online:

- Accertati che l'e-commerce sia sicuro: controlla che ci siano la sigla HTTPS e il lucchetto nella barra degli indirizzi, verifica i dati di contatto dell'azienda e la sua presenza sui social media
- Rifletti prima di cliccare su un banner che offre sconti o promozioni: a volte proprio gli enormi (e irrealistici) vantaggi che sponsorizza sono un campanello di allarme
- Non compilare form di dubbia provenienza con i tuoi dati personali
- Leggi attentamente le recensioni di chi ha acquistato prima di te
- Verifica che le descrizioni dei prodotti siano dettagliate

