PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4667 di Lunedì 30 marzo 2020

Misure di sicurezza informatica nello smart working

Raccomandazioni di ENISA per datori di lavoro e dipendenti per raggiungere un livello soddisfacente di sicurezza informatica, quando si lavora a distanza.

ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione, ha reso disponibili alcune raccomandazioni per datori di lavoro e dipendenti utili in caso di smart working e telelavoro.

Il rispetto di queste raccomandazioni per una maggiore sicurezza dei sistemi informatici a disposizione, permetterà di raggiungere un livello soddisfacente di sicurezza, quando si lavora a distanza.

1. Raccomandazioni per i datori di lavoro

- accertatevi che le caratteristiche tecniche e le protezioni della rete VPN aziendale siano in grado di sostenere un elevato numero di collegamenti simultanei
- mettete a disposizione un sistema di videoconferenze per i clienti aziendali, con capacità audio e video
- tutti gli applicativi aziendali devono essere accessibili solo tramite canali di comunicazione cifrati, come ad esempio SSL VPN e IPSec VPN
- l'accesso alle applicazioni deve essere salvaguardato utilizzando sistemi di autentica a più fattori
- impedite il collegamento diretto ad Internet di interfacce remote di accesso al sistema, come RPD
- si raccomanda di usare sistemi di autentica mutua in fase di accesso a sistemi aziendali, vale a dire client to server e server to client
- per quanto possibile, fornite apparati informatici aziendali ai dipendenti in smart working. Prima di consegnarli, accertatevi che il software di sicurezza sia aggiornato e che tutti i dipendenti si accertino di effettuare regolari e tempestivi aggiornamenti afferenti alla sicurezza. Si raccomanda anche di avere a disposizione uno schema rapido di sostituzione di apparati in avaria
- apparati personali utilizzati come BYOD - bring your on device, come laptop aziendali e smartphone, devono essere verificati a livello di sicurezza, utilizzando appropriate piattaforme,
- accertatevi che vi siano sufficienti risorse IT per offrire assistenza ai dipendenti in smart working o rimediare tempestivamente a problemi tecnici
- accertatevi di aver aggiornato le procedure per fronteggiare incidenti afferenti alla sicurezza e violazione dei dati e che i dipendenti siano stati aggiornati su questi temi
- accertatevi che ogni trattamento di dati effettuato nel contesto di smart working sia conforme alle vigenti disposizioni afferenti alla protezione dei dati personali

2. Raccomandazioni per i dipendenti in smart working

- se possibile, utilizzate computer aziendali invece che computer personali. Per quanto possibile, non svolgete sullo stesso computer attività di smart working e attività personali; fate particolare attenzione a qualsiasi messaggio di posta elettronica che faccia riferimento al coronavirus
- collegatevi via Internet utilizzando una rete sicura; evitate reti aperte o gratuite. In genere, i moderni sistemi Wi-Fi a casa sono sufficientemente sicuri, ma potrebbero essere presenti installazioni meno recenti e meno sicure. Quando la connessione non è sicura, una persona che si trova nelle vicinanze può accedere alla rete e può non solo monitorare il vostro traffico, ma anche alterarlo. Il rischio aumenta per il fatto che un lungo periodo di utilizzo della rete domestica accresce la possibilità di intercettazione. Accertarsi di avere sempre attivato gli applicativi di criptografia, debitamente aggiornati
- evitate, per quanto possibile, lo scambio di informazioni critiche aziendali attraverso posta elettronica, smistata su reti non sicure
- per quanto possibile, usate risorse intranet aziendali per scambiare file di lavoro
- fate particolare attenzione a qualsiasi messaggio di posta elettronica, che fa riferimento al coronavirus, in quanto in questi messaggi si possono celare tentativi di phishing o di truffe informatiche di vario tipo. In caso di dubbio, prendete sempre contatto con il responsabile della sicurezza informatica aziendale
- i dati che vengono scaricati su archivi di memoria locali devono essere sempre crittografati, come protezione da furto o perdita dell'apparato
- mantenete sempre aggiornato ogni applicativo antivirus ed antimalware
- tutti i sistemi operativi e le applicazioni utilizzate devono essere sempre aggiornate
- attivate il salva schermo, se lavorate in un ambiente in cui anche i familiari possono osservare la vostra attività
- non condividete gli URL di incontri virtuali sui social media su altri canali pubblici.

3. Truffe informatiche collegate a COVID 19

Tutti gli enti che tengono sotto controllo la sicurezza digitale hanno registrato, in questo periodo, un drammatico aumento degli attacchi per phishing. Allo stato attuale, occorre diffidare di qualsiasi messaggio di posta elettronica che chieda di controllare e rinnovare le credenziali di accesso, anche se la richiesta sembra provenire da un mittente affidabile. Verificate la credibilità della richiesta, prima di cliccare su collegamenti sospetti o prima di aprire allegati sospetti; diffidate anche di messaggi di posta elettronica spediti da persone che conoscete, se le richieste sono insolite. Effettuate una verifica per telefono, se possibile.

Adalberto Biasiotti

www.puntosicuro.it