PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5417 di Venerdì 23 giugno 2023

11 modi pratici per mantenere un sistema informatico sicuro e protetto

L'Information Commissioner Office, vale a dire il garante per la protezione dei dati del Regno Unito, ha messo a disposizione un elenco di interventi di cybersicurezza, quanto mai attraente.

Il popolo anglosassone è ben noto perché, nello sviluppo di leggi, regolamenti e disposizioni varie, si attiene a criteri di chiarezza, incisività e accuratezza. Questo atteggiamento è confermato dalla recente pubblicazione di un documento sulla sicurezza informatica, afferente alla protezione dati personali, che siamo ben lieti di portare a conoscenza di tutti i lettori.

Il titolo di questo documento è "11 modi pratici per mantenere un sistema informatico sicuro e protetto". Vediamo insieme questi 11 passi.

La maggior parte delle piccole imprese detiene informazioni personali e sviluppa transazioni su dispositivi elettronici. È fondamentale per la reputazione e la gestione quotidiana dell'attività aziendale mantenere le informazioni al sicuro e lontane da occhi indiscreti. Non bisogna mai accontentarsi: una scarsa sicurezza può lasciare l'azienda, ed altri soggetti ad essa collegati, vulnerabile agli attacchi informatici, che colpiscono aziende di tutte le dimensioni.

Ecco alcuni passaggi pratici che tu e il tuo staff potete adottare per migliorare la sicurezza dei vostri dati.

1. Eseguire il backup dei dati

È necessario eseguire regolarmente il backup dei dati. Se utilizzi un dispositivo di archiviazione esterno, conservalo in un luogo diverso dal tuo posto di lavoro principale: crittografalo e, se possibile, bloccalo. In questo modo, in caso di effrazione, incendio o allagamento, ridurrai al minimo il rischio di perdere tutti i tuoi dati.

Controlla il tuo backup. Certo non vuoi scoprire che non ha funzionato, solo quando ne hai più bisogno. Assicurati che il tuo backup non sia connesso alla tua fonte di dati in tempo reale, in modo che qualsiasi attività dannosa non lo raggiunga.

2. Utilizzare password complesse e autenticazione a più fattori

Assicurati di utilizzare password complesse su smartphone, laptop, tablet, account e-mail e qualsiasi altro dispositivo o account, in cui sono archiviate informazioni personali. Devono essere difficili da indovinare. Il National Cyber Security Center (NCSC) consiglia di utilizzare tre parole a caso.

Ove possibile, dovresti prendere in considerazione l'utilizzo dell'autenticazione a più fattori. L'autenticazione a più fattori è una misura di sicurezza per assicurarsi che solo la persona autorizzata acceda ai dati. Richiede almeno due forme di identificazione separate, prima che venga concesso l'accesso. Ad esempio, si utilizza una password e un codice monouso, che viene inviato tramite messaggio di testo.

3. Sii consapevole di ciò che ti circonda

Ad esempio, se sei su un treno o in uno spazio di lavoro condiviso, altre persone potrebbero vedere il tuo schermo. Uno schermo per la privacy potrebbe aiutarti.

4. Fai attenzione alle email sospette

Tu e il tuo staff dovete sapere come individuare le e-mail sospette. Fai attenzione a segni rivelatori, come cattiva grammatica, richieste di agire con urgenza e richieste di pagamento. Le nuove tecnologie mostrano come gli attacchi via e-mail stiano diventando più sofisticati. Una e-mail di phishing potrebbe sembrare provenire da una fonte che riconosci. Se non sei sicuro, parla con il mittente. NCSC fornisce materiali di formazione utili per aiutare te e il tuo staff a riconoscere le e-mail sospette.

5. Installa la protezione antivirus e antimalware e tienila aggiornata.

Devi assicurarti che i dispositivi che tu e i tuoi dipendenti utilizzate a casa o quando lavorate fuori casa siano sicuri. Il software antivirus può aiutarti a proteggere il tuo dispositivo dal malware inviato tramite un attacco di phishing.

6. Proteggi il tuo dispositivo quando è incustodito

Blocca lo schermo quando sei temporaneamente lontano dalla scrivania, per impedire a qualcun altro di accedere al tuo computer. Se hai bisogno di lasciare incustodito il tuo dispositivo più a lungo, mettilo in un posto sicuro, fuori dalla vista.

7. Assicurati che la tua connessione Wi-Fi sia sicura

L'utilizzo di reti Wi-Fi pubbliche o di una connessione non sicura potrebbe mettere a rischio i dati personali. Dovresti assicurarti di utilizzare sempre una connessione sicura quando ti connetti a Internet. Se utilizzi una rete pubblica, considera l'utilizzo di una rete privata virtuale (VPN) sicura.

8. Limitare l'accesso a chi ne ha bisogno

Utenti diversi potrebbero aver bisogno di utilizzare diversi tipi di informazioni. Metti in atto controlli di accesso per assicurarti

che le persone possano vedere solo le informazioni di cui hanno bisogno. Ad esempio, il personale addetto alle retribuzioni od alle risorse umane potrebbe aver bisogno di vedere le informazioni personali dei lavoratori, ma il personale di vendita probabilmente no.

Se qualcuno lascia la tua azienda, o se è assente per un lungo periodo di tempo, sospendi il suo accesso ai tuoi sistemi.

9. Prestare attenzione quando si condivide lo schermo

La condivisione dello schermo in una riunione virtuale può mostrare agli altri il tuo dispositivo esattamente come lo vedi tu, incluse eventuali schede o documenti aperti. Prima di condividere lo schermo, devi chiudere tutto ciò che non ti serve e assicurarti che le notifiche e gli avvisi popup siano disattivati.

10. Non conservare i dati più a lungo del necessario

L'eliminazione dei dati non più necessari libererà spazio di archiviazione. Ciò significa anche che hai meno informazioni personali a rischio, se subisci un attacco informatico od una violazione dei dati personali.

11. Smaltire le vecchie apparecchiature informatiche e le registrazioni in modo sicuro

È necessario assicurarsi che non vengano lasciati dati personali su computer, laptop, smartphone o altri dispositivi, prima di eliminarli. Potresti prendere in considerazione l'utilizzo di un software di eliminazione o assumere uno specialista per cancellare i dati.

Adalberto Biasiotti

---

www.puntosicuro.it