ARTICOLO DI ELEARNINGNEWS

Year 3 - number 89 Wednesday 13 november 2019

La sicurezza informatica per l'e-learning

Oggi le aziende che offrono corsi in modalità e-learning devono assicurarsi che nessun terzo soggetto possa entrare in possesso dei dati riguardanti gli utenti, cosa che potrebbe mettere in pericolo la sicurezza informatica e la privacy.

Le violazioni e le perdite di dati mettono in pericolo la privacy degli utenti: nelle piattaforme e-learning sono disponibili molti dati riguardanti i corsisti (dati demografici, dati sanitari, data di nascita, indirizzi e-mail, numeri di telefono, profilo Facebook, nome e cognome) che è necessario proteggere anche in riferimento al "Regolamento generale sulla protezione dei dati" dell'Unione Europea (GDPR). Se la piattaforma e-learning subisse una perdita o violazione di dati, tutte le informazioni personali potrebbero infatti finire nelle mani di un criminale informatico, che potrebbe usarli per truffe, attacchi di phishing o semplicemente venderli per ottenere un profitto.

Il GDPR impone norme specifiche sul trattamento dei dati personali dei dipendenti nel contesto lavorativo.
Se la tua azienda ha uffici e dipendenti in tutta l'UE, dovresti conoscere le legislazioni nazionali specifiche dei paesi in cui la tua azienda è presente.

Nel caso specifico dell'e-learning, per essere conformi al GDPR è necessario esaminare attentamente il programma di conformità GDPR, l'Informativa sulla privacy e le Condizioni d'uso del LMS utilizzato e firmare un DPA (Data Processing Addendum) conforme al GDPR con il provider LMS.
Il DPA deve specificare in modo chiaro le istruzioni che il servizio LMS dovrebbe seguire e obbliga entrambe le parti a rispettare gli obblighi legali relativi al GDPR.

Sviluppare un piano di formazione GDPR sostenibile renderà la protezione dei dati un valore forte per la tua organizzazione: avere un piano di formazione continua ti permetterà di incorporare buone abitudini di protezione dei dati in tutta l'azienda.

Se invece sei utente di un corso in modalità e-learning, fortunatamente ci sono alcune cose che puoi fare per proteggere i tuoi dati:

1. Utilizzare un software di sicurezza su tutti i dispositivi

Gli hacker spesso sfruttano la mancanza di sicurezza del tuo dispositivo. Ti espongono a malware che rubano i tuoi dati sensibili o mantengono registri delle attività. Ecco perché dovresti usare programmi antivirus e antimalware. Assicurati di tenerli sempre aggiornati e pianificare scansioni regolari.

2. Utilizzare un servizio di rete privata virtuale (VPN)

Sono servizi online che possono aiutarti a nascondere il tuo indirizzo IP e crittografare il tuo traffico Internet, ciò significa che nessuno potrà monitorarlo, così sarà più difficile rintracciarti. Le VPN rendono facile bypassare i firewall.

3. Rendere privati tutti i tuoi account social

Il manager della tua azienda non ha bisogno di sapere dove hai festeggiato sabato scorso o quando vai a fare la spesa. Quindi, dovresti assicurarti che tutti i tuoi profili sui social media siano impostati come privati. In questo modo, solo le persone che conosci e di cui ti fidi potranno vedere i tuoi post e accedere ai tuoi dati.