Corso a distanza

Cyber Security e GDPR: conoscere e riprogettare la sicurezza informatica

Presentazione

Il corso parte dall'illustrazione del GDPR (General Data Protection Regulation, Regolamento Europeo 2016/679 sulla Privacy), ponendo l'attenzione soprattutto sul suo aspetto più innovativo e dirompente: il **Data breach (la perdita dei dati)** e **cosa fare per ridurne il rischio**. Nella prima parte, la trattazione si focalizzerà sulle **principali novità del GDPR** rispetto alla normativa precedente (il Codice Privacy D.Lgs. 196/2003), analizzando i punti e gli articoli più importanti del nuovo Regolamento. Nella seconda, il corso si pone l'obiettivo di creare consapevolezza ("awareness") sui principali rischi connessi alla Sicurezza Informatica, con particolare attenzione agli attacchi del Cybercrime e alla protezione dei propri dati e dei propri account. Il corso rappresenta quindi uno strumento per fornire la formazione aziendale prevista anche dal nuovo Regolamento Europeo Privacy (GDPR). Gli strumenti informatici sono importanti, ma il punto debole è sempre l'uomo (il fattore "H") che con il suo comportamento può rendere inefficace qualsiasi difesa. E proprio al fattore umano è dedicato questo corso.

Programma

Modulo 1
Struttura del General Data Protection Regulation (GDPR – Regolamento UE 2016/679)
Il Regolamento (UE) 2016/679 e i suoi precedenti
Le principali innovazioni e loro conseguenze operative
La privacy by design e by default
Le nuove forme di sicurezza da adottare
Il titolare ed il responsabile del trattamento
La nuova figura del responsabile della protezione dei dati personali
Le modalità di accesso ai propri dati personali
I nuovi diritti: diritto all'oblio, diritto alla portabilità dei dati, le notificazioni delle violazioni alle autorità nazionali ed agli utenti
L'istituto della one-stop-shop
L'apparato sanzionatorio
D.Lgs. n. 101/2018: adeguamento della disciplina nazionale in tema di privacy al GDPR

Modulo 2
Social Engineering, Phishing: le minacce più diffuse
Cos'è il Social Engineering.
Il phishing e lo spear phishing: esempi e casi pratici.
Come riconoscerli e come difendersi

Modulo 3
L'email non è uno strumento sicuro: gli attacchi attraverso la posta elettronica
Lo spoofing dell'e-mail
BEC, la Business email compromise: le truffe "The Man in the Mail" e "CEO fraud"

Modulo 4
I Ransomware
Cosa sono e come ci attaccano
La prevenzione: come proteggersi.
Sono stato colpito da un Ransomware: cosa fare ora?
Ransomware: aspetti giuridici (è reato pagare il riscatto?)

Modulo 5
Imparare ad usare le Password
Le regole per una Password sicura e gli errori comuni da evitare.
Le "domande di sicurezza".
I Password Manager.
L'autenticazione a due fattori: una protezione ulteriore.

Modulo 6
I malware su dispositivi mobili
Come vengono portati gli attacchi ai dispositivi mobili
I Social Media come mezzo di attacco sempre più usato.
La prevenzione del mobile malware: una corretta policy aziendale

Modulo 7
Mettere in pratica la Cyber Security in azienda
La Sicurezza Informatica come "Gioco di squadra".
Una corretta policy di Backup.
L'importanza degli aggiornamenti di sicurezza.
Il principio del minimo privilegio
Acquisire Consapevolezza: la miglior difesa è sempre l'uomo.

Specifiche tecniche per fruzione da PC

I corsi sono fruibili dalla piattaforma FAD dell'Associazione Italiana Leasing
http://media.assilea.it/moodle
Browser:
Chrome : **consigliato** tutte le versioni
Internet Explorer: Ver. 7 e 8;
Ver. 9 e 10 (visualizzazione compatibilità attiva);
Ver. 11
Safari: Ver. 5 o superiore;
Requisiti Browser:
Plug-in ***Adobe flash player:*** Ver. 10 o superiore
Esecuzione ***Javascript*** *consentita*
Salvataggio ***Cookie*** *consentita*
Blocco Popup *disattivato*

Referenti in Assilea Servizi

Ilaria Nanni - ***Area Formazione*** - Tel. 06 99703622
Dimitri Verdecchia – ***Area Formazione*** - Tel. 06 99703654