SEC-MAL - La sicurezza dei dati ai tempi del malware

ITCore Security - IT Security - Cyber Security

Durata:	Lingue:	Certificazione:
1 Giorno	**Italiano**	**-**

Descrizione del corso

Le implicazioni e i costi delle violazioni della sicurezza sono news da prima pagina e racchiudono tutto ci è che va dalla perdita di lavori, alla perdita di ricavi fino agli incubi per le pubbliche relazioni. Dato che il volume e la proliferazione dei dati, dal Cloud agli ambienti mobili, ai social network fino ai dati delle macchine, sono in continua crescita, gli approcci tradizionali alla sicurezza non offrono più da soli la soluzione unica per i dati sensibili, ma sono comunque alla base di tutto un processo generale che molti non affrontano nemmeno. Differenti ricerche citano condizioni che continueranno a dover essere affrontate dalle Organizzazioni per la tutela dei dati, affermando che aumenterà la loro responsabilità riguardo la protezione delle informazioni: Le violazioni sono in costante aumento, anno dopo anno (38%, PWC)&• è stata rilevata una crescita significativa del furto di Proprietà intellettuale (56%, PWC)&• I costi imputabili alle violazioni sono in continuo aumento (4 milioni di dollari per evento, Ponemon)&• I CdA considerano generalmente gli Amministratori Delegati e i Dirigenti responsabili per le eventuali violazioni (ricerca NYSE). Molte informazioni, spesso frammentate o solo accennate, se non a volte errate, che circolano senza alcun obiettivo se non la mera "vendita di servizi' portano un proliferare di disinformazione dilagante che deve essere affrontata partendo dalla cultura di base, per poi approfondire di volta in volta le tematiche necessarie alle rispettive realtà. Per questo motivo questo seminario ha l'obiettivo di porre fondamenti certi e strutturati di facile accesso agli appartenenti all'Ordine, in modo da poter formare una solida base di conoscenza e competenza in un ambito molto controverso

Programma

1. Introduzione alla gestione del dato informatizzato

- Salvataggio e archiviazione del dato
- Accesso al dato
- Backup e ripristino
- Uso interno ed esterno

2. I rischi inerenti i dati sensibili
   - Attacchi diretti all'infrastruttura
   - Virus e malware: cedere ai ricatti?
   - Violazioni fisiche nell'accesso ai dati
   - Distrazione e disinformazione dell'utente
   - Rischi legali connessi al dato (cenni GDPR)
3. Criteri principali di salvaguardia dei dati e della Business Continuity
   - Gestione degli accessi fisici
   - Gestione e archiviazione dei log
   - Sistemi di backup
   - La Business Continuity
   - Archiviazione e Disaster Recovery
4. Virus e malware di oggi
   - La nuova generazione di malware e virus
   - Ricatti, decrittazione e cancel'azione del dato
   - Wannacry, Pyeta, Cryptolocker
   - I riscatti e le Cryptovalute
5. Le difese da virus e malware
   - Antivirus e antimalware: i principali sistemi di difesa
   - Sistemi di antispam: abbassare il rischio diretto dell'utente
   - Soluzioni di protezione adattiva e predittiva
   - Il comportamento umano: l? dove i sistemi informatici non possono nulla
   - Human Endpoint Portection: l'uomo come sistema di protezione attivo