



Sicurezza Informatica

Web Dev

Security

Networking

Groupware

Il capitale delle aziende sono le proprie informazioni, le conoscenze acquisite, i clienti, i fornitori. Questi dati ormai sono sempre più in formato elettronico ed è diventato complesso proteggerli. Ci sono mezzi per trafugarli alla portata di tutti e gli accessi che le aziende mettono a disposizione sono moltissimi.

Inoltre la presenza su internet 24h su 24h mette a serio rischio queste informazioni a causa della mancanza di conoscenze tecniche e dell'inadeguata protezione, oltre che della mancanza di aggiornamenti alla propria struttura informatica e di un basso livello di controllo.

E' comune sottovalutare queste problematiche fino a quando informazioni delicate vengono trafugate o dati importanti vengono messi a disposizione di concorrenti.

Spesso chiediamo di soffermarsi a pensare quanto facilmente sarebbe possibile accedere all'elenco clienti / fornitori, a informazioni finanziarie riservate, a formule o informazioni vitali per aziende di produzione, a backup aziendali e dopo averlo fatto ci si rende conto a cosa si è stati esposti, ma se di questo ci si accorge prima ci si può ritenere già fortunati.



Molto più spesso si arriva a scoprire i propri punti deboli **solo dopo che il danno è stato fatto.** Dopo aver scoperto che qualcuno ha trafugato informazioni tra l'altro senza lasciare alcuna traccia. Si pensa che queste avvenimenti siano rari e solo "**da film di spionaggio**" ma con la diffusione informatica e l'accrescere delle conoscenze sono più comuni di quanto si pensi interessando dipendenti di passaggio ad altre realtà, ex dipendenti, malavita organizzata, concorrenti, ed altro.

Pensare che solo i grandi nomi come **Ferrari, Coca-Cola, Boeing, Ericsson** possono essere sottoposti a questi rischi è sbagliato, è come pensare che lasciando la porta di casa aperta nessuno entra perché "*tanto non c'è niente di importante da rubare*".

Come spesso facciamo presente, *“non si trova ciò che non si cerca”* di conseguenza difficilmente si è in grado di capire quale pericolo si corre. In situazioni reali ci si è resi conto di quanto informazioni sensibili come gare d'appalto, quotazioni dei propri clienti, e-mail riservate, formule chimiche, fornitori strategici, ecc. siano a disposizione di troppe persone, pochi sono i dati statistici in tal senso in quanto raramente le aziende colpite da questo tipo di danni lo dichiarano ritenendo che ormai *“i buoi sono scappati”* e per non dare una percezione di *“azienda poco sicura”*, di fatto non creando la conoscenza del problema e le relative possibili soluzioni.

Lo **spionaggio industriale** utilizza sempre più la tecnologia per assicurarsi l'accesso ad informazioni riservate e sono queste le situazioni in cui noi riusciamo a fermare e comunque ad individuare questo tipo di rischi.

Spesso arriviamo a problema accaduto, trovando le cause, cercando le possibili prove per un'azione legale, valutando gli eventuali rischi ancora presenti, istruendo il personale sui pericoli da *“Social Engineering”* (come ci piace definirlo l'ingegneria del carisma) e dal corretto utilizzo dei propri mezzi informatici, bloccando così futuri accessi o se è il caso valutando di lasciare la situazione invariata in modo da poter colpire in *“flagranza di reato”* o comunque per raccogliere tutto il necessario e scoprire esattamente di cosa si è venuti a conoscenza, per poi agire legalmente.

In caso di attività preventiva operiamo effettuando analisi, *“Penetration Test”* (tentativi di accesso autorizzato), e relazioniamo individuando i punti a rischio dove eventualmente intervenire con sistemi attivi di controllo, criptatura audio/dati, tracking e logging di dati riservati, è nostra opinione che anche la protezione indiscriminata di tutto sia sbagliata, in quanto può essere particolarmente costosa e rendere complessa la quotidiana operatività, è sufficiente proteggere i dati veramente importanti, inutile proteggerli tutti.

Operiamo anche per realtà investigative e forze dell'ordine come supporto informatico, effettuando indagini e perizie tecniche in caso di reati dove è richiesta un'analisi adeguata e intervenendo sul posto in supporto al personale investigativo.

Il Nostro referente commerciale:

