Gli attacchi aumenteranno

Abbiamo incontrato Carlo Del Bo, esperto di cybersecurity

Il nuovo regolamento europeo per la protezione dei dati è un passo avanti?
È un cambiamento positivo e radicale nella gestione della privacy. Finalmente vi è una regolamentazione della protezione dei dati personali. Il suo principio cardine è che i dati personali devono essere costantemente monitorati e in caso di data bridge, ossia in presenza di una violazione dall'esterno o dall'interno, vi è l'obbligo di notificarla alle autorità entro 72 ore.

Quali sono le aziende maggiormente a rischio di attacchi informatici?
Tutte, ma soprattutto le aziende che dispongono di un'ampia varietà di dati personali, come, ad esempio, gli ospedali e le case di cura. Queste strutture possiedono sia i dati relativi alle carte di credito che le schede dei pazienti come pure i dati personali.
Come possiamo immaginarci il futuro della sicurezza informatica?
Una cosa è certa: gli attacchi informatici aumenteranno. Non dobbiamo chiederci dunque se avverranno, ma quando. Nel mio lavoro eseguo spesso dei "vulnerability assessment" nei quali simuliamo un attacco a un'azienda per mettere alla prova la vulnerabilità della sua rete. Un programmatore o un ingegnere informatico, in ogni caso un tecnico, si cala nei panni di un hacker e cerca di entrare in un sistema informatico. L'azienda in genere non si accorge neppure che qualcuno è entrato nel suo sistema.
Quali misure concrete possono mettere in atto le aziende per proteggersi dagli attacchi informatici?
Il primo passo è fare un inventario, una mappatura, dei dati sensibili che l'azienda tratta. Mi riferisco ai dati personali relativi a collaboratori, clienti e fornitori. Va valutato il flusso delle informazioni, tenendo conto anche di ciò che accade al di fuori del perimetro aziendale. Pensiamo alla documentazione aziendale in possesso di un avvocato. Inoltre non va dimenticato che i dati sensibili non sono archiviati solo su supporti informatici, ma anche cartacei. Se metto in sicurezza la mia rete informatica, dovrò fare lo stesso fisicamente chiudendo a chiave la porta dell'archivio cartaceo. Terminato questo assessment, dovrà essere messo a punto un remediation plan che contenga le misure di messa in sicurezza unitamente a un supporto strategico per la mitigazione dei rischi. Ricordo inoltro che il GDPR impone il monitoraggio costante della tutela dei dati personali.
Sicurezza informatica e cybersecurity sono sinonimi?
Non confondiamo i termini. Con sicurezza informatica intendiamo l'insieme dei dispositivi che vanno installati in un sistema per ridurre il rischio di subire intrusioni dall'esterno. La cybersecurity è invece quel settore che studia l'impatto che il rischio informatico ha sul business. A questo livello si lavora maggiormente impostando determinate scelte strategiche. Per semplificare potremmo paragonare la cybersecurity alla criminologia e la sicurezza informatica alla polizia.
La Svizzera si adeguerà al GDPR?
Questa rivoluzione in atto nella protezione dei dati personali è un fiume in piena che non potrà essere deviato ai confini nazionali elvetici. La legislazione svizzera si avvicinerà alle linee guida del GDPR, anche se attualmente ci troviamo effettivamente in una sorta di limbo.
L'applicazione del GDPR sarà un onere importante per le aziende?
Non sarà certamente un'operazione a costo zero. Ma d'altro canto sono previste sanzioni importanti per chi contravviene il regolamento. A mio parere qui vi è anche una grande occasione di refresh per le aziende che potrebbero sfruttare le misure di protezione dei dati messe in atto come strumento di marketing. Ad oggi non esiste ancora una "certificazione GDPR" ma posso immaginare che in futuro vi saranno aziende che potranno fregiarsi di qualcosa di simile. Ma non mi limiterei solo a questi aspetti. Basti pensare ai settori Ricerca e sviluppo delle aziende che godranno anch'essi di una maggiore protezione rispetto allo spionaggio industriale.
L'introduzione del GDPR comporterà la creazione di nuovi posti di lavoro?
Sì e qui vedo un'ulteriore occasione di crescita. Nelle grandi aziende saranno create posizioni per DPO, Data Protection Officer, professionisti responsabili della sicurezza informatica che dovranno rendere conto direttamente alla direzione aziendale.

Carlo Del Bo

Carlo Del Bo è International Security Advisor per diverse multinazionali italiane ed estere. Laureatosi alla Criminal Justice dell'Università Northeastern University di Boston con una tesi su "Computer Crime", ha conseguito un Master in Security Management all'Università Bocconi e un Master in Business Intelligence. Dal 2017 è Executive Advisor di Gruppo Sicurezza SA, società di servizi e consulenza con sede a Savosa e specializzata in Security e Risk Management dove si occupa di Cyber, Crisis Management, Risk Assessment e consulenza internazionale.

I prossimi seminari di Boss Editore

"Lavoratori distaccati a 360°"
17.05.2018

"Notifiche e permessi di lavoro"
5.06.2018

Maggiori info:
www.boss-editore.ch
Seminari 2018

Attacchi informatici

Malware: indica un vasta categoria di codici nocivi quali virus, worm e cavalli di troia.
Phishing: è una metodologia di attacco che simula nella grafia e nel contenuto una comunicazione ufficiale e conosciuta.
DoS o DDoS: è una tipologia di attacco che ha lo scopo di saturare deliberatamente le risorse di un sistema informatico e bloccarlo.
Sql Injection: è una metodologia piu' complessa usata per attaccare i server che contengono informazioni di valore quali password-users o dati sensibili.
Man in the middle: di fatto "uomo nel mezzo" ovvero un attaccante che si inserisce nel traffico dati di due utenti e fa credere ad entrambe le parti che stiano interagendo tra loro.
Glossario a cura di Carlo Del Bo