VareseNews

Spionaggio industriale: cos'è, come difendersi

Pubblicato: Lunedì 20 Giugno 2022

In epoca di mercato globale, concorrenza, competitività, uno dei pericoli più insidiosi per le aziende è lo **spionaggio industriale**. Con questa espressione s'intende l'insieme delle pratiche (scorrette) volte a ottenere informazioni riservate su un'impresa. Clienti, brevetti, fornitori, procedure interne, qualsiasi dettaglio utile a concedere ai competitor un vantaggio.

Lo spionaggio aziendale è un reato **particolarmente odioso**. Non solo perché, subdolamente, vanifica lo sforzo di tutte quelle imprese che ogni giorno rischiano e innovano, ma anche perché mina la fiducia degli utenti nel sistema di mercato che ha nella libera concorrenza il suo pilastro.

I reati che si configurano sono molteplici: dalla **rivelazione del contenuto di documenti segreti** (art. 621), alla **rivelazione di segreto professionale** (art. 622), alla **rivelazione di segreti scientifici o industriali** (art. 623), all'**accesso abusivo a sistema informatico** (art. 615-ter).

A essere colpite non sono soltanto le grandi realtà hi-tech, ma tutte quelle imprese, anche piccole, che operano in settori delicati o che vantano importanti commesse o standard produttivi innovativi.

Come avviene lo spionaggio industriale

Difendersi non è semplice. Gli apparati di controllo (**microspie**, **microcamere**, **mini registratori**, **localizzatori GPS**) sono sempre più piccoli e sofisticati. I **software spia** agiscono senza lasciare tracce. Senza contare, poi, il fattore umano.

In linea di massima, si distingue tra **spionaggio interno** ed **esterno**. Il primo è reso possibile dall'infedeltà di un dipendente o un ex dipendente. Un caso eclatante, nel 2007, vide protagonista Nigel Stepney. Indispettito da una mancata promozione, l'ex coordinatore tecnico della Ferrari sabotò le vetture della Rossa e trasmise i progetti riservati della F2007 al capo progettista della McLaren, Mike Coughlan.

Lo spionaggio esterno avviene installando **dispositivi di controllo** oppure **intercettando le comunicazioni telefoniche e informatiche**. Nel 1999, una compagnia tedesca, la Enercon, tentò di lanciare negli USA un generatore per le turbine eoliche. In quell'occasione, scoprì che una sua rivale americana, la Kenetech, aveva già brevettato il prodotto. Si venne a sapere in seguito che la NSA aveva intercettato le comunicazioni di Enercon, passando poi le informazioni alla Kenetech.

Nulla vieta che le due modalità (complice interno e intercettazioni) siano combinate. Alcuni campanelli di allarme possono essere: una intrusione di personale non autorizzato nei locali dell'azienda; strane interferenze nel cellulare, lampeggiamenti improvvisi, batteria che si scarica troppo rapidamente, surriscaldamento; l'impressione di essere seguiti; la capacità dei competitor di prevedere le vostre mosse e battervi sul tempo.

Gli strumenti per difendersi: investigazioni aziendali, penetration test, bonifiche da microspie

Ferma restando l'importanza di alcune misure di base (manutenzione del sistema di allarme, valutazione scrupolosa dei curriculum dei nuovi assunti), lo spionaggio industriale si contrasta efficacemente con un'attività di **controspionaggio**.

Rientrano in questo filone anzitutto le **indagini aziendali**. Un investigatore privato potrà rendere conto delle attività sospette dei vostri dipendenti o ex dipendenti.

Ancora più importanti sono i **penetration test** e le **bonifiche elettroniche**. Con i primi si analizza la **sicurezza dei sistemi informatici**, più in generale, le strutture, i meccanismi, i processi di **conservazione dei dati sensibili**. I cyberattacchi sfruttano falle in sistemi operativi e reti. **Malware**, **ransomware**, **spyware** sono nemici temibili per la vita delle imprese. Eventuali vulnerabilità emerse nel penetration test vengono riportate al cliente in una apposita relazione.

La **bonifica elettronica** è la contromisura per eccellenza. Negli ultimi anni, il ricorso a questo tipo di attività è aumentato considerevolmente. Lo sviluppo tecnologico e la grande diffusione di apparati di controllo sono fattori di rischio per la privacy di cittadini e imprese.

Come spiegano gli esperti in **bonifiche elettroniche** di Doctorspy, la **bonifica da microspie** permette di individuare **microtelecamere**, **cimici audio**, **tracker GPS**, **microregistratori**, ogni apparato di controllo nascosto nei locali dell'azienda, nelle **auto**. Non solo: la **bonifica ambientale** rintraccia anche eventuali **software spia** installati su **cellulari** o **computer** aziendali.

L'attività avviene tramite l'utilizzo di **rilevatori** particolarmente sofisticati, impiegati da tecnici professionisti secondo una procedura più o meno standardizzata. Al termine della bonifica viene rilasciata una relazione tecnica che spiega il lavoro svolto e l'esito.

Imprese e sicurezza: lo stato delle cose in Italia

Le imprese italiane sono protette contro attacchi informatici? Non come dovrebbero. Secondo gli ultimi dati, la spesa per la cybersecurity in Italia è in aumento, sia nella pubblica amministrazione che nel privato. Il ritmo è del **10-12% l'anno**. Nel nostro paese, però, la spesa per la sicurezza digitale rappresenta appena lo **0,08% del Pil**. In Francia, Germania e Inghilterra è **più del doppio**.

In generale, dunque, la strada da fare è ancora tanta per le imprese italiane che vogliano mettersi al sicuro dai rischi di sottrazione dati e spionaggio aziendale. La crescita della consapevolezza intorno al problema della sicurezza non potrà che giovare.

Redazione VareseNews
redazione@varesenews.it