Il Sole 24 ORE

Data 30-01-2017
Pagina 9
Foglio 1

Information security. L'Osservatorio del Politecnico di Milano mette in evidenza i ritardi e i punti deboli del sistema italiano

Investito un miliardo in cyber-difese

Nel 2016 la spesa delle imprese è cresciuta del 5% ma mancano ancora strategie specifiche

Enrico Netti

Quasi un miliardo di euro, per la precisione 972 milioni, con un aumento del 5% sull'anno precedente. È quanto hanno investito nel 2016 le imprese italiane con almeno dieci addetti alla voce information security. Una frazione rispetto ai quasi 66 miliardi che rappresentano il mercato Ict nel nostro paese. A rivelarlo è la seconda edizione dell'Osservatorio Information security e privacy che giovedì verrà presentato a Milano.

Contro le cyberminacce si schierano risorse sufficienti? «Il tasso di crescita è in linea con il trend internazionale, ma non ci tranquillizza - risponde Alessandro Piva, direttore dell'Osservatorio Information security e privacy del Politecnico di Milano -. Solo una grande azienda su due ha un manager per la gestione della sicurezza informatica. Insomma, siamo ancora indietro». Un'impresa su sei dispone di un piano pluriennale di difesa con riferimenti al piano industriale e, guardando alle grandi società quotate, si arriva al 58 per cento. Cresce la consapevolezza verso le minacce digitali, ma solo in una società su tre viene varato un piano organico annuale, mentre in un altro 27% il budget viene stanziato all'occorrenza. In altre parole, troppo spesso manca una cabina di regia che organizzi difese efficaci in un'ottica di medio periodo.

In azienda i principali capitoli di spesa riguardano la tecnologia, i servizi di integrazione It, il software e i servizi esternalizzati, mentre i "cantieri aperti", a cui le grandi società stanno lavorando, spaziano dagli attacchi simulati ai sistemi aziendali, test indispensabili per saggiare le difese perimetrali, per finire con i molteplici aspetti della sicurezza delle informazioni. E un'impresa su sette ha già sottoscritto una polizza assicurativa contro i cyber-rischi e i danni causati a terzi.

Si lavora anche su cloud e dispositivi mobili, mentre per l'Internet delle cose, pilastro dell'Industria 4.0, si fa ancora troppo poco. Solo il 13% del campione ha adottato delle policy in merito e il 40% sta valutando le possibili azioni di difesa. Anche per i dispositivi *smart* si fa ancora troppo poco: appena il 10% delle organizzazioni interpellate adotta delle soluzioni It specifiche.

Cyberminacce sempre concrete - venerdì scorso la notizia dell'attacco riuscito ad Alphabay, marketplace del dark web che offre merci rubate e illegali -, ma invisibili, perché gli attacchi vengono scoperti troppo tardi. «Tra le aziende italiane quasi un attacco su tre va a buon fine e nel 66% dei casi viene scoperto dopo mesi, in media sei. Tra le criticità c'è la difficoltà di disporre di personale specializzato e le strategie di risposta offrono ampi spazi di miglioramento - osserva Paolo Dal Cin, Accenture security lead per Italia, Europa centrale e Grecia -. Per questo le imprese dovranno lavorare sempre di più e meglio sulla parte di definizione strategica e sulla prevenzione, puntando forte sull'innovazione».

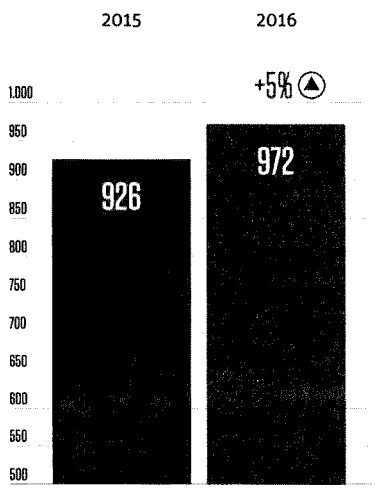
Oltre alla tecnologia c'è il fattore umano. «Il rischio di violazione può anche dipendere dall'uomo - afferma Stefano Minini, Risk & advisory services partner di Bdo Italia, multinazionale della consulenza -. Le aziende devono valutare, quindi, non solo i rischi di natura It e devono intervenire sui processi gestionali dello staff, sulla formazione del personale, su un sistema di controllo interno capace di identificare, prevenire e reagire alle diverse tipologie di rischio. Si tratta di investire sulla prevenzione».

Resta, infine, la parte di intelligence con l'analisi dei dati raccolti nel corso degli attacchi e altre attività sospette, passo propedeutico per poter anticipare le minacce secondo modelli predittivi e di risposta/reazione.

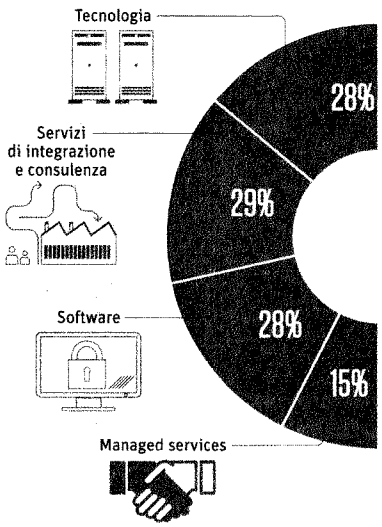
enrico.netti@ilsole24ore.com

Lo scenario

IL MERCATO...
Investimenti delle imprese italiane in sicurezza.
Dati in milioni



... E LE AREE DI INVESTIMENTO



LE CONTROMISURE
I progetti più diffusi nelle grandi imprese, risposte multiple in %

Protezione dei dati	51
Penetration test	51
Sicurezza delle reti	48
Difesa delle applicazioni	45
Protezione dei client	43
Gestione delle informazioni e degli eventi di sicurezza	38
Difesa della messaggistica	38
Controllo del traffico web	36
Gestione degli accessi	32
Intelligence per prevenire e monitorare le minacce	20
Protezione dati usati per le transazioni	19
Sicurezza sui social	16

COME INVESTONO LE PMI
I motivi che guidano la spesa, risposte multiple in %

Adeguamento normativo	48
Attacchi subiti	35
Nuove esigenze di business	31
Nuove esigenze tecnologiche	22

Fonte: Osservatorio information security e privacy, School of management del Politecnico di Milano

IL FATTORE UMANO
I principali interventi riguardano le tecnologie, anche se non va trascurata l'attenzione alla formazione del personale