Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 09/2016: 156.556
Diffusione 09/2016: 105.722
LettoriEd. II 2016 2016: 843.000
Settimanale - Ed. nazionale

Il Sole 24 ORE FOCUS

Dir. Resp.: Guido Gentili

12-LUG-2017
da pag. 14
foglio 1
www.datastampa.it

Le strategie. Da Confindustria Digitale un progetto per rendere gli Innovation Hub centri di informazione e implementazione della cybersecurity

Contro i danni più formazione e polizze

IL MONDO ASSICURATIVO
Le assicurazioni studiano modelli ad hoc che operano a valle e a monte del danno, che può essere proprio o contro soggetti terzi

Katy Mandurino

Saranno gli Innovation Hub sparsi in tutto il territorio nazionale, voluti dal piano Industria 4.0, ad avere il ruolo di centri di informazione e formazione per fronteggiare le problematiche della cybersecurity e dei rischi connessi al terrorismo. Il progetto è di Confindustria Digitale, specificatamente per aiutare le imprese – soprattutto le piccole, più impreparate e più vulnerabili – ad affrontare la gestione dei nuovi rischi virtuali.

«Nelle Pmi mancano figure professionali specifiche per questo tema e si fa fatica a trovare risorse da investire – spiega Giorgio Mosca, presidente Steering Committee Cybersecurity di Confindustria Digitale -. Come Confindustria Digitale stiamo lavorando perché all'interno dei nascenti Innovation Hub si possa informare sui modelli e sui metodi, che devono essere condivisi. La trasformazione digitale è un grande vantaggio se mette in collegamento le aziende e le società in modo sicuro». L'informazione e la formazione sono la chiave di volta per affrontare preparati i rischi della rete, che si configurano non solo sotto forma di attacchi veri e propri, come i ransomware, ovvero il "pizzo elettronico", ma anche, ad esempio, quando si tratta di sviluppare nuovi software a rischio virus, oppure quando il proprio business viene effettuato su piattaforme diverse che devono dialogare tra loro, oppure nel caso di un errore umano o di eventi che provocano un danno reputazionale. Nel 2016, sul totale degli attacchi web verificatisi a livello mondiale, il 72% riguardavano attacchi criminali, il 15% atti di hackeraggio, l'8% attacchi di spionaggio o sabotaggio e il 5% atti di cyber warfare.

«Dietro questi attacchi non c'è sempre una motivazione legata ai soldi, ma spesso sono manifestazioni di potenza - specifica Andrea Bono, general manager di Marsh, leader globale nell'intermediazione assicurativa e nella gestione dei rischi - con conseguenze dannose per la collettività». «L'evoluzione tecnologica - continua Bono - ha abituato cittadini e imprese a godere di incredibili comodità accompagnate da un drastico risparmio di tempo e fatica: dagli acquisti online alla gestione domotica della casa, dalle facilitazioni burocratiche all'efficientamento dei processi produttivi alla velocità di interazione, sia per lavoro che per svago. Ma il comprensibile eccesso di entusiasmo ha fatto sì che si perdesse l'attenzione sui rischi connessi alle opportunità. È questa la motivazione per cui oggi l'Italia è in ritardo di fronte alle problematiche della cybersicurezza, che si presentano in modo sempre più invasivo».

Una recente ricerca della Banca d'Italia, che per la prima volta ha indagato sull'approccio aziendale nei confronti della cybersecurity, dice che le imprese, soprattutto quelle più grandi, sono sempre più colpite da attacchi informatici, in particolare ransomware e azioni che sottraggono fondi, fenomeni la cui crescita è attestata anche da un report presentato al World Economic Forum di Davos da Marsh&McLennan Companies assieme a FireEye. «Si tratta di far passare nelle aziende una nuova cultura del rischio - dice Barbara Lucini, ricercatrice presso il centro di ricerca sul terrorismo dell'Università Cattolica di Milano -. Spesso le imprese si percepiscono fuori da queste problematiche; invece, bisogna lavorare molto sulla formazione, che diventa strumento di prevenzione, e sull'interpretazione degli atti terroristici».

Attorno a questi nuovi fenomeni si sta sviluppando anche il mercato assicurativo. Che opera non solo a valle del danno, coprendo la tipologia di fattori che riguarda i danni propri dell'azienda, come il mancato guadagno, le spese extra, l'estorsione, e i danni che come azienda possono esere causati a terzi - dalla distruzione di dati al coinvolgimento del network in attacchi a terzi, alla trasmissione di virus. Ma agisce anche a monte del possibile problema. «Oggi il panorama delle coperture è ampio - specifica il general manager di Marsh, Andrea Bono -. Come società operiamo anche nell'ambito preventivo della formazione del personale relativamente alla gestione dei rischi cyber. Siamo solo all'inizio: a fronte di un ammontare mondiale di premi assicurativi in questo campo di circa 3 miliardi di dollari (soprattutto negli Usa), i premi relativi all'Europa arrivano a circa 300 milioni di euro. Ma negli ultimi mesi la sensibilità è aumentata in modo esponenziale e nei prossimi cinque anni mi sento di prevedere un mercato europeo del valore da 1 a 3 miliardi».

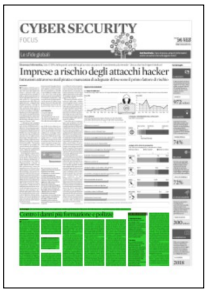
Si presume che sarà così, anche alla luce delle nuove normative europee che prevedono entro il maggio del 2018 che le imprese mettano in atto politiche per la sicurezza informatica con obblighi ben precisi.

«Il tema assicurativo è molto interessante - conclude Giorgio Mosca - perché aiuta a creare consapevolezza e perché genera modelli interpretativi fondamentali, che tuttora mancano».

CHE COSA SI RISCHIA

La tipologia del danno
Sono molteplici. Attacchi veri e propri, come i ransomware, ovvero il "pizzo elettronico", ma anche virus che attaccano nuovi software, oppure rischi connessi all'utilizzo di piattaforme diverse che devono dialogare tra loro, oppure errori umani o eventi che provocano un danno reputazionale.

Post-danno
Le società assicuratrici operano a monte del danno con la formazione del personale e i test, ma anche a valle, coprendo la tipologia di fattori che riguarda i danni propri dell'azienda, come il mancato guadagno, le spese extra, l'estorsione, e i danni che come azienda possono esere causati a terzi: dalla distruzione di dati al coinvolgimento del network in attacchi a terzi, alla trasmissione di virus


CYBER SECURITY
Imprese a rischio degli attacchi hacker