SEC MEDITERRANEA - PRESS MONITORING

TESTATA: IL SOLE 24 ORE
DATA: 28 marzo 2018
CLIENTE: DISTRETTO PRODUTTIVO DELL'INFORMATICA

NELL'ERA DEI DATI/1. DOMANI IN EDICOLA IL NUOVO FASCICOLO DELLA SERIE SULLA CYBERSICUREZZA

Il «fattore umano» decisivo per la privacy

Convegno del Sole a Bari: aziende sempre più attente alla difesa delle informazioni

di **Vincenzo Rutigliano**

La *cyber security* e la protezione dagli attacchi informatici non conoscono deroghe o isole felici. Lo sanno nel mondo della sanità che, insieme alla finanza, è il settore più colpito dagli attacchi informatici che hanno origine all'interno delle stesse organizzazioni. È così addirittura nel 70% dei casi, contro una media degli altri settori del 52%. Dunque la sanità - come è emerso a Bari nel corso della tappa pugliese del *roadshow* organizzato da Il Sole 24 Ore su "Cyber Security. L'evoluzione della sicurezza nell'ecosistema 4.0" - non è al riparo da questi attacchi che, nella maggior parte dei casi, sono provocati, secondo uno studio di IBM X-force condotto nel 2017, da azioni involontarie dei dipendenti delle organizzazioni sanitarie e da virus introdotti nei sistemi informatici dall'interno.

Contro questi rischi una buona *practice* viene dalla Itel di Ruvo, nel barese (radiofarmaci e servizi di medicina nucleare) che ha messo a punto un protocollo di sicurezza informatica collegato a Ehra, sistema di radioterapia di trattamento del cancro con il robot che posiziona il paziente rispetto al fascio di protoni che distruggono i tumori senza danneggiare i tessuti sani circostanti. Così le immagini diagnostiche di ciascun paziente, dapprima aggregate, vengono poi estese, e trasmesse a un calcolatore in remoto. Trattandosi di dati sensibili vengono trasmessi «in anonimato grazie a una chiave cifrata - spiega Michele Diaferia, ad di Itel – e poi tutto viene restituito a chi fa la protonterapia sbloccando la chiave». Per difendersi dagli attacchi esterni non bastano però solo gli strumenti tecnologici. È necessario puntare - sul fronte interno - soprattutto sulla formazione del personale, su *policy*, procedure e modelli organizzativi orientati alla gestione del rischio informatico, specie in quei settori, come l'*health care*, appunto, nei quali l'uso di servizi digitali, la trasmissione di dati sensibili, l'integrazione tra tecnologie informatiche (It) e operative (Ot) è in costante crescita. Dunque il fattore H (*Human*) è decisivo. Spesso l'anello più debole della catena di It sono proprio i dipendenti e dunque i loro errori. Per questo le imprese devono fare investimenti nella formazione e nelle politiche della sicurezza e se non c'è collaborazione tra i grandi *player* del settore si collabori almeno dentro i territori.

Come insegna il caso di Confindustria Bari e Bat che, in collaborazione con il Distretto pugliese dell'informatica, è al lavoro su questo fronte. «Le associazioni di categoria – spiega Salvatore Latronico, presidente del distretto - sono un interlocutore con cui definire e adottare codici di condotta appropriati. E noi come Distretto siamo impegnati nella definizione di modelli organizzativi che possano garantire la fornitura di prodotti e servizi sicuri». I modelli però sono da definire prima e non dopo, ad attacco avvenuto, quando la reazione è, in media, a due ore dal suo verificarsi. La cyber sicurezza interroga ovviamente tutto il sistema Paese perchè la sovranità si esercita anche proteggendo imprese e cittadini dai rischi di questi attacchi perché i *big data* crescono e attirano attività di hackeraggio nelle quali non vi sono hacker buoni e hacker cattivi, ma attaccanti e difensori. Il loro impatto economico è enorme, quasi mille miliardi di euro nel 2023.

Per questo la Ue ha raccomandato a tutti gli Stati membri di occuparsi della loro protezione perché al centro di una serie di tipologie di attacchi, come emerge dallo studio commissionato dalla Ue al Cini, il Cybersecurity National Lab guidato da Donato Malerba, direttore del dipartimento di Informatica dell'università di Bari, l'ateneo che ha istituito anche un corso di laurea sulla cyber sicurezza. Secondo Malerba vietato improvvisare: «Gli amministratori di *big data* dovrebbero documentare le scelte fatte e le soluzioni adottate e i cittadini devono essere consapevoli di quello che può accadere ai loro dati». Dunque «proteggere la rete nazionale è strategico», dice Maurizio Marcelli, responsabile Network Resilience di Tim –. E la sicurezza delle reti deve essere affrontata già in fase di progettazione delle infrastrutture e non dopo, quando i costi aumentano di 30 volte. Ed evitando frammentazioni». Che è proprio la sfida posta a tutta la PA italiana con 14mila *data center*. «Vanno ridotti e concentrati, costano molto - avverte Antonio Samaritani, dg di Agenzia per l'Italia Digitale –. Servono linee guida per i siti sicuri e le 58 amministrazioni collegate a Cert-PA devono essere modelli di accelerazione dell'aggregazione delle nostre comunità».