L’Italia digitale è un colabrodo informatico

- Arturo Di Corinto, 18.06.2020

Hacker's Dictionary. Aumentano in maniera esponenziali gli attacchi informatici: in Italia colpite Enel, Honda, Geox, Riscotel e la Zecca dello Stato. Ci vogliono più formazione e un impegno preciso delle aziende nella sicurezza informatica

Negli ultimi giorni un attacco cibernetico ha colpito Enel e Honda, bloccandone la rete informatica interna. L’azienda di scarpe Geox ha dovuto fermare produzione e logistica e lasciare a casa i lavoratori per colpa di un *ransomware* diffuso all’interno dei suoi sistemi. Anche la Camera di commercio di Roma è stata oggetto di un’incursione del gruppo Anonymous che è riuscito perfino a pubblicare una finta notizia sul suo sito web. Gli hacker sono anche penetrati nel sito dell’Istituto Poligrafico e Zecca dello Stato. Anche l’Associazione Nazionale delle Imprese Assicuratrici è finita preda degli hacktivisti al pari del Cicap, l’associazione per il contrasto alle pseudoscienze e così pure Riscotel, il portale per il calcolo dei tributi degli enti locali. Il 15 giugno invece centinaia di dati personali degli utenti iscritti alla community del Comune di Napoli sono stati diffusi senza autorizzazione.

Il successo di questi attacchi informatici dipende da vari fattori: errori nel software e nella sua configurazione; vulnerabilità del codice già note e mai risolte per mancanza di fondi, soprattutto nel settore pubblico; il lock-in tecnologico che rende le aziende dipendenti dalla stessa software house senza poter ingaggiare servizi alternativi per risolvere problemi di funzionamento. Più spesso la causa è però l’errore umano. La digitalizzazione forzata del nostro paese e la remotizzazione delle attività di svago e di lavoro ha aumentato a dismisura quello che si chiama il perimetro da difendere. Le persone si sono ritrovate a lavorare in casa coi bambini che strillano e la distrazione al computer si sa, costa cara. Poi c’è una dubbia cultura della sicurezza anche in ambito professionale se, come dimostrano gli Anonymous con le loro incursioni, chi gestisce sistemi digitali usa ancora come password la parola “admin” oppure una sequenza di numeri come “123456”.

Eppure il nostro quadro regolatorio oggi impone specifici obblighi alle imprese, soprattutto quando fanno parte delle 500 aziende presenti nell’elenco degli operatori dei servizi essenziali stilato dal Dipartimento Informazioni per la sicurezza, e che adesso pagano con cifre a sei zeri gli errori che fanno. Lo stesso accade per enti e imprese che non comunicano il danno subito dai propri utenti e clienti entro 72 ore, in ottemperanza della legge sulla privacy, la Gdpr, e che possono essere multate fino al 4% del proprio fatturato. In aggiunta lo Csirt, il nuovo Centro di risposta nazionale agli incidenti informatici, sembra funzionare bene, nonostante il meccanismo un po’ farraginoso per la segnalazione degli incidenti.

Da segnalare è anche lo sforzo di università e imprese private come Tim, Kaspersky, Ntt Data, che proprio nel periodo del *lockdown* pandemico hanno avviato seminari e corsi gratuiti sulla cybersecurity rivolti a tutta la popolazione e non solo ai loro impiegati. Ma non può bastare.

Insieme alla formazione del personale che deve imparare a riconoscere truffe e tentativi di frode online, tra le soluzione percorribili c’è quella del *Bug bounty*, programmi aziendali di caccia all’errore nei codici informatici che mettono in palio un premio per il primo che scova una falla di funzionamento. Dopo i *vulnerability assessment*, come gli *Sneaker Hacker* (hacker che lavorano come consulenti informatici aziendali) li chiamano in gergo, ci sono i penetration test, cioè l’esecuzione di attacchi autorizzati sui sistemi informatici per testarne la robustezza. In Italia ci sono aziende all’avanguardia che lo fanno. Voi che cosa aspettate?