23/05/2020

la Repubblica BARI

Pagina 14

EAV: € 1.480
Lettori: 29.750

Argomento: Exprivia: si parla di noi

Cybersecurity, i ritardi del Sud


pagina 14 Puglia Commenti

L'analisi

L'elogio della lentezza dei pranzi in famiglia: ci voleva la quarantena

Le idee

Paralisi Giustizia, sette soluzioni

L'intervento

Cybersecurity, i ritardi del Sud

L' intervento di Domenico Raguseo I n uno scenario di continua evoluzione tecnologica, in cui la mole di informazioni viaggia molto velocemente da un capo all' altro del mondo, si corre il rischio di non percepire la realtà per ciò che realmente è, finché non veniamo a contatto con le sue parti più nascoste. Questa distonia tra percezione ed effettiva consapevolezza di un fenomeno si è palesata anche con la nuova malattia del Coronavirus Una distonia ancora più evidente se si pensa ai fenomeni di crimine online, che viene avvertito come qualcosa esistente solo al di là del proprio pc. Non ci sorprendono allora alcuni dati nel Rapporto Clusit 2020, editato dall' Associazione Italiana per la Sicurezza Informatica, che ogni anno fotografa la situazione della cyber security e delle telecomunicazioni a livello nazionale e internazionale. Il Rapporto conferma nel 2019 una tendenza in crescita del 7% degli attacchi gravi a livello globale rispetto all' anno precedente, valutando come molto probabile l' ipotesi che una quota significativa di questi attacchi non sia ancora emersa, nonostante gli obblighi di notifica vigenti. Questo effetto di trasposizione tra mondo reale e virtuale è ancora più palese nei dati raccolti dall' Università degli Studi di Bari che, insieme al gruppo Exprivia, ha condotto uno studio sullo stato della cybersecurity nel Sud Italia, pubblicata sempre all' interno del Rapporto Clusit 2020. Dal sondaggio, che ha coinvolto oltre 212 tra aziende ed enti del Mezzogiorno, emerge che il 54,5% del campione, ritiene di non aver mai ricevuto attacchi informatici. Questo dato è secondo me uno dei più rilevanti, in quanto

rappresenta nel modo migliore la sfida simbolicamente lanciata dai criminali di ultima generazione. Tralasciando il fatto che molti non sanno di essere stati attaccati, solo il 10,6% del campione dichiara di aver subito un danno valutato come 'alto e molto alto'. In breve, se un criminale cattura un mio dispositivo, ma il danno che mi arreca è minimo, per quale motivo dovrei preoccuparmi? D' altra parte, l' obiettivo degli attaccanti è proprio questo: catturare i dispositivi migliorando le tecniche di 'offuscamento' e, quando possibile, rendere il dispositivo ancora più efficiente, ad esempio rimuovendo altri malware presenti per essere gli unici a trarre profitto dal dispositivo catturato. Gli attaccanti sanno benissimo, infatti, che ritardando la presa di coscienza dei rischi collegati al cybercrime, moltissime imprese continueranno a considerare la cybersecurity come qualcosa che non le tocca direttamente e il cui impatto sulla vita reale è tutto da dimostrare. Non deve pertanto sorprendere la moderata percezione circa le probabilità di subire un attacco informatico: solo il 32,7% del campione lo ritiene altamente possibile, il 34,5% sufficientemente probabile, il 25,5% poco probabile mentre il 7,3% ritiene addirittura nulla la possibilità che si verifichi. È da questo tipo di percezione che dobbiamo partire per scegliere strategicamente in cosa investire per rendere più sicure le nostre reti. La sfida che dobbiamo raccogliere, al fine di rendere l' intero ecosistema più sicuro, è che si può e si deve lavorare sulla consapevolezza. Non si tratta di qualcosa che interessa solo le aziende e gli enti, ma tutte le componenti del sistema affinché l' approccio al mondo digitale avvenga con coscienza e competenza. Questo va fatto anche con l' aiuto della scuola o con la formazione nelle aziende, come i corsi che la nostra azienda sta avviando con il rilascio di un certificato riconosciuto, con l' obiettivo di migliorare la conoscenza dei rischi da un lato, e di fornire dei suggerimenti su come ridurli dall' altro, attraverso uno stile di vita digitale più responsabile. Il Sud Italia sembra voler accettare questa sfida, tanto che quasi nove intervistati su dieci dall' Università di Bari ritiene che percorsi formativi di questo tipo siano necessari. (direttore CyberSecurity Exprivia)