30/03/2020

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 819
Lettori: 12.467

Link alla pagina web

Cyber security, tra percezione e consapevolezza: un gap da colmare soprattutto nel Sud Italia

Il processo di digitalizzazione corre veloce e tutti ne siamo consapevoli. Dobbiamo fare in modo, però, che questa consapevolezza non lasci indietro la presa di coscienza dei rischi relativi alla cyber security. Ecco le soluzioni per colmare questo gap, soprattutto nel Sud Italia In 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: da problema territoriale e distante, qualcosa che esiste solo dall'altra parte dello schermo del telefonino o della TV, si è trasformato in qualcosa di drammaticamente reale.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. Se ne parla in tanti eventi con eccellenti oratori, in molti programmi televisivi, molte riviste iniziano a darne notizia, ma rimane sempre qualcosa che non ci intacca, distante milioni di chilometri e che ci ha raggiunto solo perché le informazioni viaggiano veloci. Il crimine potrebbe essere vero o forse no.Indice degli argomenti Cyber security, tra percezione e consapevolezza: i numeriPrendere coscienza dei rischi collegati al cyber crimeCyber security, tra percezione e consapevolezza: quali investimentiCyber security: lavorare sulla consapevolezzaCyber security, tra percezione e consapevolezza: i numeri Non ci sorprenderanno 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|Italtel, ha condotto uno studio sullo stato della cyber security nel Sud Italia, pubblicata sempre all'interno del Rapporto Clusit 2020.Al sondaggio, effettuato utilizzando Google forms e diffuso tramite i social network più comuni, hanno risposto 212 tra aziende ed enti; un campione composto per il 54,5% da piccole imprese (fino a 50 dipendenti), il 18,2% da medie (da 51 a 250 dipendenti) e il 27,3% da grandi imprese (oltre 250 dipendenti).È altamente probabile che chi ha risposto al sondaggio sia in qualche modo attivo nell'ecosistema digitale, rappresentando proprio quei gruppi di persone che ascoltano le informazioni sulla cyber security in televisione ritenendole vere e a volte false, ovvero con un livello sproporzionato di allarmismo. WHITEPAPER Cybersecurity: come superare efficacemente le vulnerabilità delle tecniche di Intelligenza Artificia Sicurezza Scopri come Scarica il WhitepaperDall'analisi realizzata dall'Università di Bari emerge che il 54,5% del campione costituito da piccole aziende non ritiene di aver mai ricevuto un attacco. Questo dato è, secondo me, uno dei più rilevanti, in quanto rappresenta nel modo migliore la sfida simbolicamente lanciata dai criminali di ultima generazione.Infatti, l'Italia ha accelerato il suo percorso di digitalizzazione sensibilmente e il Sud Italia ha avuto un ruolo considerevole, sia a livello accademico che industriale. Considerando che per sviluppare un attacco di tipo DDoS che raggiunge i 100 Gbps i criminali necessitano di milioni di dispositivi catturati precedentemente, come è possibile che ad aver ricevuto un attacco informativo sia solo un numero di aziende così esiguo?Prendere coscienza dei rischi collegati al cyber crime Tralasciando il fatto che molti non sanno neanche di essere stati attaccati, solo il 10,6 % dichiara di aver subito un danno valutato come "alto e molto alto". Questo perché, in genere, siamo istintivamente motivati a spendere in funzione di un presumibile ritorno di investimento (ROI, Return of Investment). 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 obfuscation e quando possibile rendere il dispositivo ancora più efficiente, come 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 cyber crime, tutti continueranno a considerare la cyber security

come qualcosa che non li tocca direttamente, qualcosa di cui si parla o cui si legge on line, il cui impatto sulla vita reale è tutto da dimostrare.Non deve pertanto sorprendere la percezione circa la probabilità di un attacco informatico: solo il 32,7% del campione lo ritiene altamente possibile e il 34,5% sufficientemente probabile, mentre il 25,5% lo ritiene poco probabile e solo il 7,3% ritiene addirittura nulla la possibilità che si verifichi.Questo stride con quanto rilevato da Fastweb, nello stesso Rapporto Clusit 2020, che nel 2019 in Italia ha raccolto ed esaminato attraverso il proprio Security Operations Center oltre 43 milioni di attacchi informatici transitati sulla sua infrastruttura.Come fanno riflettere i numeri forniti sempre dalla Polizia Postale che segnala 6.854 casi a livello nazionale solo di cyber crime finanziario (phishing, vishing, smishing, Business Email Compromise, Sim-Swap).Sempre dalla Polizia Statale emerge una fotografia sulle forme di aggressione in rete con numeri da capogiro, ma di cui continuiamo a non avere reale percezione: basti pensare alle 196.000 segnalazioni di truffe on line o ai 460 casi di cyberbullismo per cui sono stati indagati 136 minori, passando per l'adescamento di minori online per cui, ad esempio, sono stati incriminati 189 soggetti, sempre sul territorio italiano.È ovvio che i numeri forniti dalla Polizia Postale indicano i casi di persone che hanno avuto il coraggio o la volontà di denunciare e segnalare. I numeri, invece, forniti da Fastweb ci dicono quello che è stato scoperto, che ovviamente è molto più grande, consegnandoci una percezione del tutto diversa della realtà e facendoci immaginare uno scenario apocalittico.Cyber security, tra percezione e consapevolezza: quali investimenti Ed è da questo tipo di percezione che dobbiamo partire per scegliere strategicamente in cosa investire per rendere più sicure le nostre reti. Secondo lo studio sullo stato della cyber security nel Sud Italia, gran parte degli investimenti sono in "protect", ossia sono spese che pianifico "una tantum" per avere la coscienza a posto; e solo l'8,7 % del campione dice di avere un SIEM, cioè una tecnologia per implementare il processo di "security information and event management" e che implica un'attività di osservazione e rilevamento continua e costante ("detect").Tra l'altro, dobbiamo considerare che il campione investigato dall'analisi dell'Università di Bari non tiene in considerazione tutte quelle persone, enti o società che sono inconsapevolmente all'interno dell'ecosistema digitale, ossia persone che considerano la cyber security come un bene intrinseco di cui si occuperà sempre qualcun'altro. E non dobbiamo credere che questa categoria, con lacune di cultura digitale, sia una minoranza; spesso è esattamente il contrario.Cyber security: lavorare sulla consapevolezza Per cui la sfida che dobbiamo raccogliere, al fine di rendere l'intero ecosistema più sicuro, è che in

ambito cyber security 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. Va fatto con l'aiuto della scuola e con la formazione nelle aziende, con corsi che da un lato migliorino la conoscenza dei rischi e dall'altro forniscano dei suggerimenti su come ridurli attraverso uno stile di vita digitale più responsabile.Il Sud Italia sembra voler accettare questa sfida, infatti l'89,1% degli intervistati ritiene che i corsi di formazione di questo tipo siano necessari. Il campione pertanto vuole comprendere se il "rumore" sulla cyber security è giustificato e perché. WHITEPAPER Mobile security: come proteggere gli smartphone dai malware Sicurezza Scarica il WhitepaperIl processo di digitalizzazione oramai corre veloce e tutti ne siamo consapevoli. Dobbiamo fare in modo che questa consapevolezza non lasci indietro la presa di coscienza dei rischi relativi alla sicurezza informatica.@RIPRODUZIONE RISERVATA