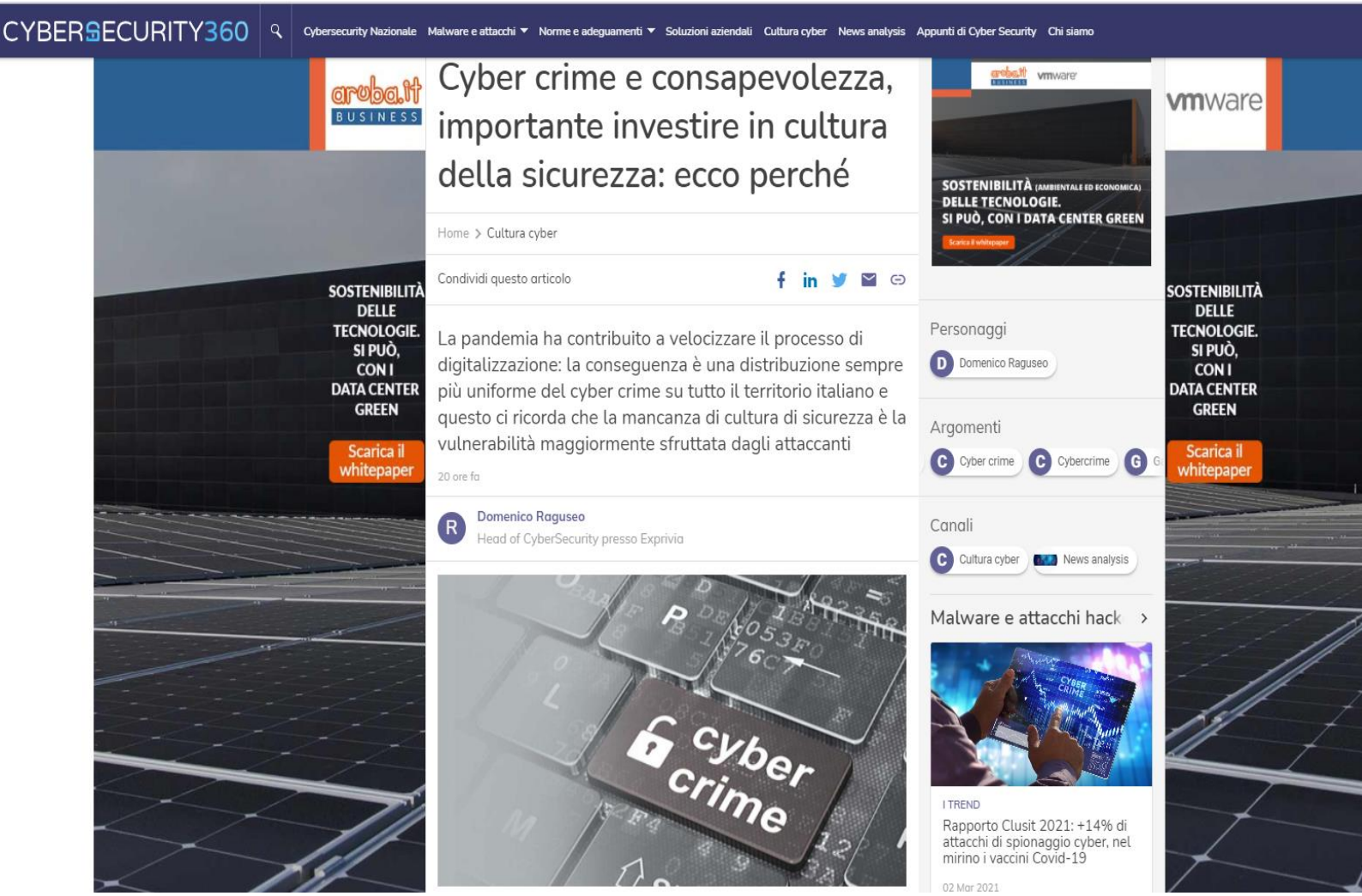
29/04/2021

cybersecurity360.it

Argomento: Exprivia: si parla di noi



29/04/2021

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 702
Utenti unici: 1.633

https://www.cybersecurity360.it/cultura-cyber/cyber-crime-e-consapevolezza-importante-investire-in-cultura-della-sicurezza-ecco-perche/

Cyber crime e consapevolezza, importante investire in cultura della sicurezza: ecco perché

La pandemia ha contribuito a velocizzare il processo di digitalizzazione: la conseguenza è una distribuzione sempre più uniforme del cyber crime su tutto il territorio italiano e questo ci ricorda che la mancanza di cultura di sicurezza è la vulnerabilità maggiormente sfruttata dagli attaccanti Gli investimenti effettuati nel settore privato sono spesso conseguenti a studi sul ritorno di investimento (ROI, Return of Investment) e influenzati dalla percezione del rischio. Non essendoci nella cyber security un ROI oggettivo (si potrebbe valutare il danno in funzione di un attacco, ma non un ROI su un investimento specifico), la percezione diventa un elemento fondamentale.Nel Rapporto Clusit dal 2021, Exprivia, in collaborazione con Dipartimento di Informatica della Università di Bari, ha svolto uno studio che associa i dati di incidenti, attacchi e violazioni privacy (raccolti dall'Osservatorio Exprivia sulla CyberSecurity utilizzando fonti pubbliche), a quella che è la percezione della popolazione sul cyber crime.La ricerca si focalizza sul Mezzogiorno e, seppur rilevi una maggiore presenza del fenomeno del cyber crime nel nord e centro Italia, le differenze tra le tre aree non risultano significative.L'Italia nel 2020 ha subìto, infatti, una forte accelerazione del processo di digitalizzazione che ha interessato tutte le regioni e la conseguenza diretta è che anche il fenomeno del cyber crime si è distribuito abbastanza uniformemente su tutto il territorio italiano. Figura 1 – Distribuzione geografica di attacchi, incidenti e violazioni privacy nel 2020 in Italia.Indice degli argomenti Cyber crime e consapevolezza: il fenomenoLa percezione Cyber crime e consapevolezza: il fenomeno Attacchi e incidenti risultano seguire il trend di utilizzo degli strumenti digitali e quindi riportano un calo nel periodo estivo e un picco nei momenti di maggiore produttività per le imprese e per la PA. WHITEPAPER Quali sono stati i casi di cybercrime più aggressivi degli ultimi anni? Scoprilo nel white paper Cybersecurity Scopri come Scarica il WhitepaperLa pandemia da Covid-19 è causa, seppur indirettamente, di tale fenomeno. La Covid-19 ha, infatti, accelerato il processo di trasformazione digitale e la conseguenza è stato un aumento del fenomeno criminale.Non associate alla pandemia, invece, sono le segnalazioni fatte dal Garante Privacy per le violazioni del GDPR. Infatti, le segnalazioni di violazioni della privacy sono state pressoché costanti durante tutto il 2020. Di GDPR non se ne è parlato molto nel corso dell'anno, ma il 2020 è stato uno anno critico anche per le violazioni della privacy. Senza pandemia, probabilmente, se ne sarebbe parlato molto di più. Figura 2 – Breakdown tra attacchi, incidenti e violazioni privacy Figura 3 – Attacchi, incidenti e violazioni privacy nel 2020 in sud ItaliaAltro tema relativamente collegato alla pandemia è

il numero di dispositivi collegati tramite IPv4 su internet che risultano essere aumentati vertiginosamente nel corso del 2020. Siamo a quasi otto milioni di dispositivi con un aumento del 12% nell'ultimo quarto del 2020 e molti di questi dispositivi risultano privi di meccanismi di autenticazione.Non si parla solo di IT classica, ma anche di telecamere, Smart TV, stampanti, PLC e via dicendo. La pervasività dell'IT, associata alla possibilità di integrare tramite la rete strumenti intelligenti che comunicano tramite protocolli spesso non proprietari e che si interfacciamo con applicazioni su ambienti open per servire anche infrastrutture critiche, è un tema che deve essere affrontato in maniera strutturale sia in termini di governance (chi gestisce in azienda i dispositivi IoT? Chi gestisce gli elementi IT a supporto di infrastrutture critiche o industriali?), che di certificazione dei dispositivi introdotti sul mercato. Insomma, Bruce Schneier scriveva "click here to kill everybody". Oggi il problema è ancor più evidente. Figura 4 – Distribuzione dei dispositivi IoT nelle regioni italiane 2020Con riferimento alle metodologie utilizzate per gli attacchi, nel Mezzogiorno osserviamo la netta predominanza del phishing. Figura 5 – Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel sud Italia 2020In termini di mercati, il settore maggiormente colpito è la Pubblica Amministrazione, fermo restando che i tradizionali crimini finanziari continuano a mietere impietosamente vittime. La percezione I dati sono stati raccolti attraverso una survey focalizzata sul Mezzogiorno, ma che ha registrato input da tutta Italia.Nel rapporto Clusit, pertanto, è possibile visionare dati che fanno riferimento a tutto il territorio italiano. Quando si parla di cyber crime, il territorio italiano non si può dividere tra zone di diverso colore, su questo tema le differenze tra regioni sono davvero lievi.Parlando di percezione, dobbiamo evidenziare come quanto qui descritto sia una visione molto ottimistica della realtà. Infatti, nella maggioranza dei casi, chi ha risposto alla survey aveva già una certa sensibilità sul tema.Tra coloro che hanno sensibilità sul tema, la percezione è di non aver ricevuto un attacco.Insomma, se ne parla tanto, ma se si chiede ai diretti interessati risponderanno che ne hanno sentito parlare, ma non sono mai stati coinvolti direttamente in attacchi. La pandemia ed il cybercrime sembrano viaggiare su binari paralleli per gli specialisti di settore.La percezione dell'uomo medio italiano è però diversa da quella di specialisti del settore, anzi direi diametralmente opposta. A rendere lo scenario più preoccupante è che in molti ritengono che in caso di incidente, i danni possano essere considerati praticamente trascurabili.Quanto alla consapevolezza, rispetto al 2019 si nota un sensibile aumento della stessa. Il 50% del campione afferma, infatti, di aver seguito dei corsi a riguardo. E alla domanda se i corsi siano stati utili e necessari, il campione non ha dubbi: i corsi sono necessari. Sostanzialmente, gli intervistati non ritengono probabile un attacco o un incidente, ma ritengono comunque opportuno investire in conoscenza e questa è sicuramente una buona notizia.Laddove la mancanza di cultura di sicurezza è la vulnerabilità maggiormente sfruttata dagli attaccanti, il fatto che ci sia consapevolezza della necessità di maggiore informazione, anche in assenza di una forte percezione del rischio, è il dato in assoluto più rassicurante. WEBINAR WEBINAR - La nuova era del Cybercrime: quali strumenti e strategie di difesa ti servono davvero? Sicurezza Cybersecurity Iscriviti al