05/03/2020

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 819
Lettori: 12.467

Link alla pagina web

Cyber attacchi, ecco le minacce peggiori: il report Clusit 2020

Nel 2019 sono stati messi a segno 1.670 attacchi informatici, dato che rappresenta il +7,6% rispetto al 2018 e il +91.2% sul 2014, con una prevalenza di minacce legate al cyber crime: la situazione emerge dalla presentazione in anteprima del rapporto Clusit Va sempre peggio e le vittime continuano ad aumentare. Sono stati 1.670 gli attacchi cyber messi a segno nel 2019, con una percentuale di crescita del 7,6% sul 2018 e del 91,2% rispetto al 2014. Il cyber crime si attesta come principale causa d'attacco, tra i mezzi il più utilizzato è il malware.È questa la grave situazione emerge dai dati del rapporto Clusit 2020, presentato in anteprima alla stampa oggi in attesa dell'incontro pubblico via streaming del 17 marzo e del Security summit di maggio. L'attenzione sul tema cyber security "è in vertiginosa crescita, anche per via dell'aumentare degli incidenti – commenta Alessio Pennasilico, information&cyber security advisor di P4I e membro del Comitato tecnico scientifico Clusit -. Diventano quindi particolarmente rilevanti i dati che pubblichiamo sugli attacchi", per analizzare la situazione e individuare idonee contromisure.Indice degli argomenti Il report Clusit 2020Cyber security, gli attacchi più importanti del 2019 Tecniche di attacco e severity 2019Le rilevazioni del SOC FastwebSicurezza informatica nel Sud ItaliaI trend del mercato della sicurezzaIl report Clusit 2020 Per l'associazione "il 2020 è un anno particolare, il ventesimo dalla fondazione – spiega il presidente di Clusit Gabriele Faggioli, Ceo di P4I -. Abbiamo raggiunto i 600 iscritti, di cui 320 organizzazioni e 280 soci individuali". Il nuovo rapporto Clusit si apre con una panoramica sugli attacchi cyber più importanti del 2019, per proseguire con l'analisi affidata a Fastweb sullo scenario italiano in relazione a cyber crime e incidenti rilevati. A seguire, un'analisi del mercato italiano della sicurezza IT, lo stato della cyber security nel Sud Italia e un focus sui trend in

materia di email security. Seguono le rilevazioni della Polizia Postale, Guardia di finanza, Cert Nazionale e Cert PA. Un ampio capitolo è dedicato al cyber crime nel settore finanziario in Europa, a cura del Cert di Banca d'Italia.Il report si chiude con focus su argomenti di attualità come business continuity e resilienza aziendale, i rischi legati alle app mobile italiane, la sicurezza nel settore healthcare, l'impatto del deepfake e le tendenze IT che potranno impattare sui professionisti in Italia quest'anno. Chiude il rapporto il focus sulla industrial security con i dati a cura degli Osservatori del Politecnico di Milano. In generale, emerge dal report "crescite sia relative ai tentativi di attacco sia degli incidenti che si verificano e degli impatti sulle organizzazioni", commenta Pennasilico. In particolare, tra gennaio e dicembre 2019 ci sono stati in media 139 attacchi cyber al mese, a livello mondiale, cioè il +47,8% in più del periodo 2014-2018, durante il quale la media degli attacchi mensili era di 94.Cyber security, gli attacchi più importanti del 2019 Andrea Zapparoli Manzoni, del Comitato direttivo di Clusit, spiega che "è stata rilevata un'accelerazione sulla media degli attacchi, con il +48% degli attacchi gravi nel triennio 2017-2019. In particolare, nei mesi di luglio, agosto, settembre, ottobre e dicembre ci sono stati maggiori picchi". Un trend significativo: "Normalmente in estate ci sono meno attacchi, in questo caso invece c'è stato un incremento", segnale di come le organizzazioni criminali siano strutturate in modo da poter garantire attacchi tutto l'anno. Per ragioni di tipo normativo (in particolare l'obbligo di disclosure), le vittime degli attacchi cyber nel 2019 sembrano essere state soprattutto americane. Tuttavia, "non è la realtà dei fatti, significa che lì la disclosure sta funzionando". In Europa invece il dato sembra in diminuzione, anche se si attendono gli effetti delle nuove normative nonostante "il GDPR e la direttiva NIS indicano che dobbiamo segnalare gli incidenti alle autorità, non pubblicamente. Eppure la public disclosure aiuterebbe a proteggerci meglio, il suo valore non è stato ancora recepito".La categoria Target multipli è stata quella più colpita nel 2019, superando anche quest'anno il settore Gov che fino a tre anni fa era al primo posto. Al terzo posto c'è il settore healthcare, quarto online services e cloud, quinto ricerca ed educazione: "La maggior parte degli attacchi gravi sono su queste prime cinque categorie. Questo potrebbe indirizzare una serie di politiche per attrezzare questi settori in modo specifico", racconta Zapparoli Manzoni. Nel 2019, l'83% degli attaccanti appartiene alla categoria cyber crime, al contempo sono diminuiti gli attacchi legati all'hacktivism e sembrano rimanere stabili le categorie cyber espionage e information warfare. Confrontando i dati, emerge che "le misure che devono essere adottate dalle vittime sono diverse, perché differente è la minaccia che imcombe.

Verso i target multipli, la percentuale di attacchi riconducibile al cybercrime è dell'84%. Nell'healthcare, settore le cui strutture sono attaccate perché fragili e spesso costrette a pagare in caso di ransomware per tutelare la continuità e dunque la salute dei pazienti, la percentuale di episodi legati al cyber crime sale al 94%", fa notare l'esperto. Confronti importanti, perché "Ciascun settore ha trend diversi per cui dovrebbe modulare le risposte in base alle minacce prevalenti".Tecniche di attacco e severity 2019 WHITEPAPER Cosa fare per gestire i Micro Data Center in maniera ottimale? Datacenter Datacenter Infrastructure Management Scarica il WhitepaperTra le tecniche più utilizzate per danneggiare le organizzazioni, il malware è quella preferita: è stato utilizzato nel 44% degli attacchi, con una crescita del +24% sull'anno scorso. Seguono le tecniche sconosciute, poi social engineering e phishing, con una crescita del + 81,9% sul 2018. Al quarto posto ci sono lo sfruttamento delle vulnerabilità e al quindi posto gli attacchi APT. Tra gli attacchi malware, il ransomware rappresenta il 46%, mentre i cryptomines sono diminuti. Vengono sempre attaccate singole organizzazioni, ma anche milioni di persone insieme, con un aumento degli attacchi più generalizzati rispetto a quelli targettizzati. Il ransomware "è arrivato a spingere Stati come la Louisiana a richiedere la dichiarazione di emergenza nazionale, ma le singole vittime non hanno avuto impatti gravi rispetto ad altre categorie", sottolinea Zapparoli Manzoni.Per comprendere l'impatto di queste tecniche, è utile l'analisi della severity. Nel report Clusit gli attacchi sono stati suddivisi in tre fasce per valutare la gravità degli incidenti, ed è emerso che gli attacchi con impatto medio sono stati la maggioranza, con il 46% dei casi. I più gravi hanno rappresentato il 28% dei casi e quelli di livello critico il 26%. Tra i target, le infrastrutture critiche sono quelle che hanno subito soprattutto attacchi di livello critical, seguite dalla categoria Gov. Considerando invece le tecniche, gli attacchi di tipo APT/Multiple threats sono stati soprattutto di livello critico.Le rilevazioni del SOC Fastweb Fastweb ha contribuito al report Clusit con l'analisi della situazione italiana relativamente al cyber crime e agli incidenti, segnalando i dati degli attacchi rilevati dal proprio Security Operations Center. L'analisi si basa su oltre 43 milioni di eventi di sicurezza. Emerge la crescita del cyber crime, tuttavia i dati rivelano che la PA ha adottato misure tali da contenere gli attacchi alle proprie strutture. Infatti, risulta che gli attacchi verso la Pa siano calati del -23%. Tra i settori merceologici più coinvolti, nel 2019 è emersa una new entry: il settore Gaming, che ha registrato il +25%, con picchi di attacchi a ottobre e novembre 2019.L'analisi di Fastweb indica che nel 2019 c'è stata circa una vittima di cyber crime al secondo. Gli attacchi DDOS sono cresciuti del +12% sul 2018. La

maggior parte degli attacchi, precisamente l’83%, arriva dagli Usa, dove si trova la maggioranza dei Centri di comando e controllo che diramano gli attacchi. Il 13% di tali centri sono invece ospitati in Europa, diminuiscono invece nel mondo asiatico -7%.Sicurezza informatica nel Sud Italia Il rapporto Clusit 2020 include anche un’analisi sullo stato della sicurezza informatica nel Sud Italia, a cura dell’Università degli Studi di Bari e di Exprivia Italtel. Dal campione di aziende raccolto, il 34,5% di queste imprese dichiara di aver subito attacchi informatici nel corso del 2019, mentre solo il 10,9% dei soggetti si ritiene incapace di difendersi. Il 69% degli intervistati si dice poco o per niente consapevole circa i rischi conseguenti ad un attacco informatico.I trend del mercato della sicurezza IDC Italia invece ha analizzato la situazione e le prospettive del mercato italiano della cyber security. È emerso che sono soprattutto le grandi organizzazioni a investire in sicurezza IT, in particolare nel settore manifatturiero, dove cresce la consapevolezza dell’importanza del tema relativamente a Industria 4.0 e alle tecnologie legate all’intelligenza artificiale. I dati IDC indicano che entro il 2025 il 25% della spesa in servizi di sicurezza delle aziende italiane sarà destinata a creare e mantenere un “trust framework”. Invece, il tema dello “skill shortage” rimane critico.@RIPRODUZIONE RISERVATA