COMUNICATO STAMPA

CYBERCRIME: NEL 2022 PEGGIORA LO STATO DELLA SICUREZZA INFORMATICA IN ITALIA

L'Osservatorio Cybersecurity di Exprivia nel 2022 registra 2.600 fenomeni legati al cybercrime, quasi il doppio rispetto al 2021. Hacker sempre più capaci di andare a segno e causare incidenti informatici, che per la prima volta da quando viene diffuso il report superano gli attacchi.

14 febbraio 2023 – Se il 2021 era stato un annus horribilis per la sicurezza informatica in Italia, il 2022 è stato anche peggiore. Infatti, per la prima volta dal 2020, quando è nato l'**Osservatorio Cybersecurity di Exprivia** sulle minacce informatiche in Italia, il numero di incidenti informatici (ovvero gli attacchi andati a buon fine) supera quello degli attacchi: circostanza resa possibile dal crescente lasso di tempo tra il momento dell'attacco e l'incidente, da tecniche sempre più sofisticate usate dagli hacker e dalla poca consapevolezza sui rischi legati alla rete da parte di imprese e cittadini.

È quanto emerge dall'**ultimo 'Threat Intelligence Report'** di **Exprivia** che prende in considerazione 118 fonti aperte (siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media) e che, nel 2022, registra **2.600** fenomeni legati al cybercrime, di cui **1.236** attacchi, **1.261** incidenti e **103** violazioni della privacy; un numero quasi doppio rispetto ai **1.356 del 2021** e più che quadruplicato rispetto ai **605 del 2020**.

Solo nel trimestre ottobre-dicembre 2022 si sono verificati **547** eventi, con una progressiva crescita nel mese di dicembre (che da solo ne conta 257), diventando così il terzo mese dell'anno per numero di fenomeni dopo marzo e maggio.

"Con il sorpasso degli incidenti sugli attacchi nel 2022 possiamo affermare con certezza che alcuni degli incidenti sono l'effetto di azioni ostili intraprese dagli hacker nel biennio precedente **- commenta Domenico Raguseo, direttore Cybersecurity di Exprivia***. Considerare un attacco come un'azione che inizia e finisce nel corso di qualche minuto o qualche giorno è, infatti, un grande errore. In molti casi si tratta di una guerra non dichiarata da parte di un attaccante che prima studia debolezze e vulnerabilità della propria vittima, quindi decide quando e come sferrare il colpo finale. Alcuni attacchi possono durare anni e, spesso, è difficile ricondurre un incidente a un attacco specifico".*

Nel rapporto stilato dal Gruppo ICT pugliese – impegnato nel promuovere la cultura sulla sicurezza informatica – il **cybercrime** si conferma nel 2022 la motivazione principale che porta gli hacker a compiere azioni malevoli con oltre 2.000 fenomeni, registrando un aumento del 73% rispetto al 2021.

A partire dal 2022, con il conflitto russo-ucraino, si è aggiunto alla lista delle motivazioni anche il **cyberwarfare** (guerra cibernetica) con ben **157** fenomeni registrati; di particolare importanza l'**hacktivism** (attività criminali al fine di promuovere una causa politica o sociale) aumentate del **139%** rispetto al 2021.

Anche il settore **Finance**, con picchi importanti per tutto il 2022 e, in particolare, nella prima metà dell'anno, conserva il suo primato tra i settori più colpiti con **939** casi (il 36% del totale e più del doppio rispetto al 2021 quando erano stati 428). Secondo gli esperti dell'Osservatorio questo numero è legato al fatto che le aziende finanziarie, gli istituti bancari, le piattaforme di criptovalute, gestendo importanti quantità di denaro, siano un obiettivo attraente per gli attaccanti. Segue il settore **Software/Hardware –** tra i bersagli preferiti durante la pandemia **–** con **343** casi, in lieve flessione rispetto allo scorso anno quando erano stati 388, mentre l'**Industria** è al terzo posto con ben **280** fenomeni, seguita da **Pubblica Amministrazione** (passa da 120 a **260** casi) e **Retail** (da 118 a 172) che si confermano settori tra i più vulnerabili.

Tra le tipologie di danno rilevate nel 2022 primeggia ancora il **furto di dati** con il 70% dei casi sulla totalità dei fenomeni registrati; a netta distanza, ma da non sottovalutare, **danno economico** e **service interruption** (rispettivamente il 10% e l'11% del totale). Tra le tecniche più utilizzate, mantiene il primato il **phishing-social engineering** con **1.133** casi di adescamento in rete o via mail verso utenti distratti o poco consapevoli, quasi il doppio del 2021 quando erano stati 627, rappresentando, quindi, il 43% del totale dei casi nel 2022.

Il report di Exprivia rileva, infine, una diminuzione dei dispositivi IoT esposti in rete nell'ultimo trimestre dell'anno (-8%), mentre l'indice sul rapporto tra dispositivi sicuri e non, elaborato dall'Osservatorio, evidenzia una maggiore vulnerabilità nel Sud Italia. Per la prima volta, invece, il rapporto tra servizi digitali analizzati e vulnerabilità identificate sembra vedere tutto il territorio nazionale muoversi con la stessa velocità.

COMUNICATO STAMPA

Exprivia

Contatti

Exprivia SpA

Investor Relations
Gianni Sebastiano
gianni.sebastiano@exprivia.it
T. + 39 0803382070 - F. +39 0803382077

Ufficio Stampa

Sec Mediterranea
T. +39 080/5289670
Teresa Marmo
marmo@secnewgate.it - Cell. +39 335/6718211
Gianluigi Conese
conese@secnewgate.it - Cell. +39 335/7846403

Sec and Partners
T. +39 06/3222712
Martina Trecca
trecca@secnewgate.it - Cell. +39 334/1019671
Andrea Lijoi
lijoi@secnewgate.it - Cell. +39 329/2605000