COMUNICATO STAMPA

CYBERCRIME: È DICEMBRE IL MESE PEGGIORE DEL 2020

L'Osservatorio Cybersecurity di Exprivia registra nell'ultimo trimestre dell'anno una crescita dei reati informatici quasi cinque volte superiore rispetto al primo.
La finanza tra i settori più colpiti, soprattutto per l'incremento dei pagamenti cash-less.
Primeggia l'adescamento tramite email e social network. Presi di mira i dispositivi medicali.

24 febbraio 2021 – Dopo mesi altalenanti, tornano a crescere a fine anno i **reati informatici in Italia**; con un picco a dicembre, il 2020 si conferma un anno complesso anche per quanto concerne la sicurezza in rete.

Da quanto emerge nell'ultimo **rapporto del 2020 sulle minacce informatiche in Italia** elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo **ottobre-dicembre** si sono registrati 237 crimini informatici, in crescita del 60% sul trimestre precedente e quasi del 400% rispetto al periodo gennaio-marzo, quando furono solo 49. È marzo il mese che segna lo spartiacque nella dinamica del cybercrime: con l'iniziò della **pandemia** e, con essa, della diffusione dello **smart working**, si è assistito a un'impennata tra attacchi informatici, violazioni della privacy e incidenti in tutti i settori dell'economia e della pubblica amministrazione.

L'Osservatorio di Exprivia - impegnata nel diffondere la cultura della sicurezza informatica – segnala che i fenomeni, oltre che **all'enorme numero di dispositivi connessi in rete**, sono legati alla crescita esponenziale delle **transazioni digitali**, tra cui gli acquisti e le operazioni bancarie online, soprattutto nell'ultima parte dell'anno. In particolare, secondo il rapporto - che ha analizzato oltre 50 fonti di informazione pubbliche - il mese di **dicembre** è, con 96 eventi criminali, quello che ha registrato il **numero record nell'anno**.

"Se da un lato la pandemia ha accelerato la digitalizzazione nel nostro Paese, dall'altro la sicurezza della rete è stata messa a dura prova - **afferma Domenico Raguseo, direttore Cybersecurity Exprivia.** *A stupirci maggiormente è che la vulnerabilità più sfruttata dagli attaccanti sia il fattore umano. È necessario quindi per tutti noi – aggiunge Raguseo - prendere consapevolezza dei rischi che si corrono in rete, iniziando a diffidare delle anomalie. Ad esempio, dai video o dalle gif inattesi che riceviamo sulle app di messaggistica istantanea, dagli errori di sintassi contenuti nelle e-mail sospette, dai domini non veritieri degli indirizzi di posta o dall'improvvisa velocità con cui navighiamo sul pc. Siamo noi i primi a poterci proteggere dagli attaccanti".*

In tutto il 2020, oltre il 60% degli eventi criminali ha provocato il **furto dei dati**, superando di gran lunga sia le **violazioni della privacy** (13% dei casi) – quasi **triplicate dall'inizio dell'anno** – che le **perdite di denaro** (10%).

Tra le tecniche più sfruttate dai cyber-criminali durante il 2020 primeggia il **phishing-social engineering con il 43% dei casi**, che colpisce in maniera particolare utenti distratti o con poca conoscenza delle modalità di adescamento tramite e-mail o social network. Seguono, gli **attacchi unknown** (24% sul totale degli eventi), ossia nuove metodologie sperimentate dagli hacker per non essere rilevati dai meccanismi di difesa tradizionali, e i **malware** (23%), il cui utilizzo è quadruplicato nel corso dell'anno.

Nel 2020 la **Pubblica Amministrazione** e il settore **Finance** sono stati gli **ambiti più vulnerabili e maggiormente attaccati dai cybercriminali,** rispettivamente con 91 e 81 eventi registrati. Dati che fanno riflettere, considerando l'accelerazione subita dalla **digitalizzazione dei servizi nella PA,**

dall'utilizzo di applicazioni bancarie e dai pagamenti digitali. E proprio nell'ambito finanziario, particolarmente vulnerabile a causa dell'esposizione di dati sensibili spesso senza adeguata protezione, si evidenzia un aumento esponenziale dei fenomeni durante l'anno, dal singolo episodio registrato tra gennaio e marzo si passa a 41 nell'ultimo trimestre, la metà di tutti i reati verificati nel 2020 nel settore.

A seguire, **con 41 episodi**, il settore **Education**, preso di mira a causa del massiccio ricorso alla didattica a distanza di scuole e università. Non è da meno il settore dell'**Industria** che dopo aver registrato picchi incrementali durante tutto l'anno, conta solo **nell'ultimo trimestre 17 eventi criminali, quasi il 50% dell'intero 2020**, causati da una crescita di dispositivi collegati alla rete, molti privi di autenticazione, e anche da tanti episodi di spionaggio industriale.

Sotto i riflettori dell'Osservatorio Cybersecurity di Exprivia gli episodi di cybercrime riguardanti la **Sanità** che, duramente colpito nei mesi centrali dell'anno, non è sul podio per il numero degli eventi subiti ma merita attenzione soprattutto per la **criticità** degli stessi, se si pensa al valore dei **dati sanitari rubati e utilizzati nel 'dark web'.** Dall'analisi degli esperti Exprivia, inoltre, emerge che nell'ultimo anno i **dispositivi medicali** sono stati esposti a molteplici vulnerabilità, a partire da quelli personali utilizzati da medici e pazienti per l'assistenza a distanza. I cyber criminali, infatti, si impossessano del **controllo di un dispositivo bloccando il servizio** o manomettendo le funzionalità, con il fine di acquisire informazioni sensibili.

Gli esperti di Exprivia sottolineano, infine, che nell'intero anno sono aumentati di quasi otto volte gli **attacchi informatici** rispetto al primo trimestre gennaio-marzo **(da 25 a 199)**, mentre gli **incidenti**, ovvero gli attacchi andati a buon fine, hanno avuto un andamento altalenante con un picco tra aprile e giugno (46) e un calo nei mesi seguenti, fino a ridursi del **40%** tra il secondo e il quarto trimestre dell'anno. Probabilmente le tecniche di attacco sono sempre più complesse e risulta più difficile identificare in maniera efficace i cyber-criminali e quindi dare contezza degli incidenti.

Oltre al report, sul sito di Exprivia www.exprivia.it è presente anche l'elenco dei corsi organizzati per la formazione nell'ambito della sicurezza e della gestione dei rischi a livello informatico.

Exprivia

Exprivia è a capo di un gruppo internazionale specializzato in Information and Communication Technology in grado di indirizzare i driver di cambiamento del business dei propri clienti grazie alle tecnologie digitali.

Con un consolidato know-how e una lunga esperienza data dalla presenza costante sul mercato, il gruppo dispone di un team di esperti specializzati nei diversi ambiti tecnologici e di dominio, dal Capital Market, Credit & Risk Management all'IT Governance, dal BPO alla CyberSecurity, dai Big Data al Cloud, dall'IoT al Mobile, dal networking alla collaborazione aziendale sino al mondo SAP. Il gruppo affianca i propri clienti nei settori Banking&Finance, Telco&Media, Energy&Utilities, Aerospace&Defence, Manufacturing&Distribution, Healthcare e Public Sector. L'offerta comprende soluzioni composte da prodotti propri e di terzi, servizi di ingegneria e consulenza.

A seguito dell'acquisizione dell'81% del capitale sociale di Italtel, storica società italiana che oggi opera nel mercato ICT con un forte focus nei mercati Telco & Media, Enterprises e Public Sector, oggi il gruppo conta circa 3.600 professionisti distribuiti in oltre 20 paesi nel mondo.

Exprivia S.p.A. è quotata in Borsa Italiana nel mercato MTA (XPR).

Contatti

Exprivia SpA

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

Ufficio Stampa

Sec Mediterranea
T. +39 0805289670
Teresa Marmo
marmo@secrp.com
Cell. +39 3356718211

Gianluigi Conese
conese@secrp.com
Cell. +39 3357846403

Sec and Partners
T. +39 063222712
Martina Trecca
trecca@secrp.com
Cell. +39 3339611304

Andrea Lijoi
lijoi@secrp.com
Cell. +39 3292605000