COMUNICATO STAMPA

CYBERSECURITY: PRIMO REPORT DEL 2023 DI EXPRIVIA

CALANO I FENOMENI DI CYBERCRIME IN ITALIA MA PEGGIORA LA SICUREZZA DEI DISPOSITIVI MEDICALI

Nel periodo gennaio-marzo diminuisce del 44% il numero di casi rispetto al trimestre precedente. Aumenta però il rischio per apparecchi radiologici, dispositivi cardiologici, microscopi connessi in rete. Il furto dei dati torna al primo posto tra i danni causati dagli hacker.

25 maggio 2023 – Il 2023 si apre con una complessiva **diminuzione delle minacce informatiche** rispetto ai mesi precedenti, ma i **dispositivi esposti in rete aumentano** e sono **poco protetti**, in particolare quelli utilizzati in **ambito medico**.

È quanto emerge dal nuovo **'Threat Intelligence Report' elaborato dall'Osservatorio Cybersecurity** di **Exprivia** che prende in considerazione 122 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media.

Secondo il rapporto stilato dal gruppo ICT pugliese, tra gennaio e marzo **calano del 44% i fenomeni di cybercrime**, con **308** casi rispetto ai **547** dell'ultimo trimestre dello scorso anno e con il mese di marzo che registra, da solo, quasi la metà dei casi (137). Rispetto allo stesso periodo del 2022, gli attacchi si sono addirittura dimezzati (-53%), gli incidenti sono diminuiti di oltre il 70% e le violazioni della privacy del 37%.

Nello specifico, nei primi tre mesi dell'anno si sono verificati **192 attacchi**, **104 incidenti** – ovvero attacchi andati a buon fine – e **12 violazioni della privacy**.

"È vero che la quantità di fenomeni rilevati rispetto al passato è decisamente inferiore, tanto che non si registrava un numero di incidenti così basso da settembre 2021 **- commenta Domenico Raguseo, direttore Cybersecurity di Exprivia.** *Tuttavia, non dobbiamo assuefarci al crimine informatico, soprattutto nel momento in cui i dispositivi connessi alla rete aumentano. Di pari passo, infatti, cresce il rischio di incorrere in minacce che interrompono servizi critici come quelli legati al mondo della salute. Questi risultati devono essere uno stimolo per comprendere come contrastare il fenomeno; l'unica strada è continuare a investire nella sicurezza informatica".*

Dal rapporto si evince che sul territorio italiano aumentano **del 13% i dispositivi IoT connessi in rete (circa otto milioni)** con maggiore probabilità di essere attaccati dagli hacker e, in particolare, nel Sud Italia. Secondo l'indice di valutazione elaborato dall'Osservatorio di Exprivia, è peggiorata anche la sicurezza dei dispositivi medicali intelligenti, ad esempio apparecchiature per radiografie e

risonanze, microscopi, o dispositivi cardiologici indossabili e connessi. In leggera flessione anche il livello di sicurezza dei servizi esposti in rete, sempre più vulnerabili a causa dell'aumento delle attività digitali, dai pagamenti online all'invio delle ricette dematerializzate: gli attaccanti ne compromettono la reperibilità o la disponibilità, causando inefficienze dei sistemi.

Per gli esperti dell'Osservatorio Cybersecurity di Exprivia, impegnata nel promuovere la cultura sulla sicurezza informatica anche attraverso corsi di formazione, il settore maggiormente preso di mira dagli attaccanti nel primo trimestre dell'anno è stato quello **Software/Hardware** (società ICT, di servizi digitali, piattaforme di e-commerce, dispositivi e sistemi operativi) con ben 99 casi. Al secondo posto, quello della **Pubblica Amministrazione** con 89 casi, in crescita del 59% rispetto al periodo ottobre-dicembre dello scorso anno, quando i casi erano stati 56; al terzo posto, con 31 fenomeni, il settore **Finance** (aziende finanziarie, istituti bancari o piattaforme di criptovalute) che perde il primato e segna un calo del 79% rispetto all'ultimo trimestre del 2022 (quando se ne contavano 150). Seguono **Industria** e **Retail**, rispettivamente con 22 e 14 fenomeni.

Nel primo trimestre dell'anno il **furto dei dati** torna al primo posto tra le principali tipologie di danni causati dagli hacker, con il 65% dei casi totali (201 fenomeni sui 308 totali); un dato comunque in calo di oltre il 50% rispetto alla rilevazione precedente (424). Il furto dei dati consiste nell'archiviazione o nel trasferimento illegale di informazioni personali, finanziarie o proprietarie come password, codici software, algoritmi e processi causando gravi conseguenze per le persone o le organizzazioni colpite. Ex aequo, al secondo posto, l'**interruzione di servizio**– (l'arresto del normale funzionamento della rete, di un'applicazione o di un servizio software) con il 15% dei casi, e la richiesta di **denaro** con il 13%; a seguire la **violazione della privacy** (4%), ossia la divulgazione di dati da parte di soggetti terzi senza il consenso dell'interessato.

Tra le tipologie di attacco, primeggia il **phishing/social engineering**, ovvero l'adescamento in rete o via mail di utenti distratti o poco consapevoli, con il 47% dei casi totali (145 fenomeni rispetto ai 193 del trimestre precedente); calano anche gli attacchi tramite **malware**, al secondo posto con 88 casi rispetto ai 170 registrati tra ottobre e dicembre 2022.
Secondo il rapporto, il **cybercrime** si conferma la principale minaccia per la sicurezza in rete in Italia, con oltre l'80% dei casi (255) rispetto al totale. A notevole distanza l'**hacktivism** (attività criminali al fine di promuovere una causa politica o sociale) con il 13% (40 casi), e il **data breach** (violazioni di sicurezza che comportano distruzione, perdita, modifica, accesso o divulgazione non autorizzata dei dati personali) con il 4% degli eventi rilevati.

COMUNICATO STAMPA

Exprivia

Il Gruppo Exprivia, specializzato in Information and Communication Technology, è tra i principali protagonisti della trasformazione digitale.

Forte di un bagaglio di competenze maturate in oltre 30 anni di presenza costante sul mercato nazionale e internazionale, Exprivia impiega circa 2.400 persone in sei Paesi nel mondo avvalendosi di un team di esperti in diversi ambiti della tecnologia e della digitalizzazione: dall'Intelligenza Artificiale alla Cybersecurity, dai Big Data, al Cloud, dall'IoT al BPO, dal Mobile al Networking e alla Collaboration, presidiando interamente il mondo SAP.

Quotata in Borsa Italiana dal 2000 nel mercato Euronext (XPR), Exprivia supporta i propri clienti nei settori Banking, Finance&Insurance, Aerospace&Defence, Energy&Utilities, Healthcare e Public Sector, Manufacturing&Distribution, Telco&Media. La capacità progettuale del gruppo è arricchita da una solida rete di partner, soluzioni proprietarie, servizi di design, ingegneria e consulenza personalizzata.

La società è soggetta alla direzione e coordinamento di Abaco Innovazione S.p.A.

www.exprivia.com

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
teresa.marmo@secnewgate.it - Cell. +39 335/6718211
Gianluigi Conese
gianluigi.conese@secnewgate.it - Cell. +39 335/7846403

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