LE APERTURE PERICOLOSE


Cybersecurity

LE APERTURE PERICOLOSE

PRIVATI CITTADINI E AZIENDE SEMBRANO ESSERE ACCOMUNATI IN ITALIA DALLA CATTIVA ABITUDINE DI TRASCURARE ACCORGIMENTI IN APPARENZA BANALI IN MATERIA DI SICUREZZA INFORMATICA. IL RISULTATO È IL PROLIFERARE DEGLI INCIDENTI E ATTACCHI, AGEVOLATO IN TEMPI DI PANDEMIA DAL PIÙ AMPIO RICORSO ALLO SMART WORKING

Nel corso del terzo trimestre del 2020 l'Osservatorio CyberSecurity di Exprivia, multinazionale attiva a tutto tondo nel mercato informatico, ha rilevato nel nostro Paese qualcosa come 62 attacchi di phishing e social engineering e altri 37 malware. Ha inoltre identificato ben 6,935 milioni di indirizzi IPv4 esposti in Rete. Fra questi, 123 mila e 723 sono telecamere o smart TV, stampanti, firewall, router o tecnologie di ambito sanitario e ben 5.685 sono relativi a sistemi di controllo industriale. I dati sommariamente riassunti qui sono da considerarsi ideale complemento di quanto visto al termine del secondo quarto dell'anno. Analizzando 40 fonti di informazione pubbliche era risultato allora che tra il primo trimestre dell'anno - quando gli attacchi, incidenti e violazioni privacy erano stati 49 - e il secondo (171) si era potuto osservare un incremento superiore al 250% che ha toccato il suo picco massimo a giugno con 86 attacchi, incidenti e violazioni privacy. Già in quella circostanza l'Osservatorio di Exprivia aveva individuato alcuni dei responsabili del boom. «L'aumento dello smart working, una maggiore connessione ai social network durante l'emergenza e la riapertura delle industrie subito dopo il lockdown», cioè. «La maggior parte degli attacchi sono da mettere infatti in relazione all'emergenza-coronavirus e oltre il 60% degli episodi ha

provocato come danno il furto dei dati con una crescita a Carminatitripla cifra rispetto al primo trimestre (+361%), superando di gran lunga sia le violazioni della privacy (11% dei casi) sia le perdite di denaro (7%)». Dai riscatti alle criptovalute L'attività dei cybercriminali sembra andare di pari passo con quella delle imprese. «Proprio in coincidenza con il rientro in azienda di settembre», ha detto il direttore CyberSecurity di Exprivia Domenico Raguseo a Stampi, «le incursioni sono risultate in ascesa e hanno toccato il loro secondo record annuale. Inoltre, è interessante notare che fra luglio e settembre non c'è stata proporzione diretta fra attacchi veri e propri e incidenti, magari perché molti incidenti non sono stati segnalati». Gli obiettivi sono noti, almeno in parte: la sottrazione di dati sensibili, a cui si aggiungono numerose segnalazioni di violazioni dell'Autorità Garante a seguito di ispezioni compiute per verificare la conformità al GDPR. «Trojan e ransomware sono i principali codici maligni in circolazione», ha detto Raguseo, primi sono dei software che si travestono da applicazioni sicure ma che contengono malware estremamente pericolosi, ad esempio programmi che consentono il controllo del dispositivo da parte dell'attaccante. Gli altri constano di azioni che mirano a bloccare i servizi di una società, ente o organizzazione sino al pagamento di un riscatto. Fra gli illeciti attivabili tramite trojan c'è la trasformazione dei computer in cripto-miner che direttamente (scaricando degli eseguibili) o indirettamente (tramite java script inseriti nel browser, tecnica questa chiamata criptojacking) generano criptovaluta a beneficio dell'attaccante e non del possessore del dispositivo. C'è però anche dell'altro: cresce il fenomeno del phishing, una truffa banale a testimonianza della poca cultura in tema di sicurezza IT». Quali che siano le armi a disposizione dei pirati, certo è che le cifre sono quanto mai preoccupanti. Accanto a quelle squadernate in apertura spiccano quelle relative ai protocolli privi di autenticazione trovandone 8.694 come ad esempio opzione anonymous impostata a TRUE o autenticazione disabilitata su SAMBA. Sono inoltre 5.685 i dispositivi industriali (Industrial Control Systems, conosciuti come ICS) esposti su internet, di cui 416 sono PLC (Programmable Logic Controller). Se si pensa al fatto che questi sistemi sono chiamati a gestire impianti e aziende di grandi dimensioni e ne interessano anche l'indotto, la gravità della situazione emerge in tutta la sua chiarezza. «I quasi 7 milioni di dispositivi citati», ha argomentato poi Raguseo, «sono tutti potenziali ostaggi di un attaccante, compresi quelli industriali. Stiamo parlando di dispositivi utilizzabili per lanciare attacchi nei confronti di terze parti, grazie a botnet create per dar vita a un at attacco di tipo DDoS (Distributed Deny Of Service) che consiste nel bombardare un servizio con volumi che possono raggiungere i 300 Giga Bit al

secondo. In un panorama globalizzato qual è quello odierno, il pericolo non è quindi limitato alla sola Italia, anche perché a livello globale i dispositivi non protetti sono centinaia di milioni: 400 milioni sono quelli esposti su Internet, di cui 100 milioni in Europa».L'anno della svolta La scarsa cultura cui l'intervistato ha fatto riferimento si può spiegare con un esempio. Chiunque ha consapevolezza che pur vedendo per strada una porta di casa aperta sa che oltrepassarla costituirebbe reato. Non così su Intenet, dove la sensibilità è molto minore e gli usci vengono spalancati e attraversati con una inconcepibile leggerezza che interseca il mondo fisico. Secondo Raguseo è infatti difficile da accettare che molti installino, per l'abitazione o il capannone, dei sistemi di videosorveglianza, ma li proteggano con pasword e ID sin troppo facili da indovinare o addirittura senza proteggere il dispositivo con userid e password. Strano, insomma, ma tristemente vero. «È sulla consapevolezza», ha dichiarato il direttore CyberSecurity di Exprivia, «che bisogna lavorare, perché l'attacco in sé è solo la punta di un iceberg fatto di superficialità e incoscienza. Fra il 2020 e il 2021 è più che mai necessario, da parte dei governi come da parte delle industrie, investire per colmare le lacune generate da un approccio troppo leggero non solo alla protezione delle informazioni, ma piuttosto alla digitalizzazione tout court». Laddove in passato l'informatica era asservita all'automazione, ora è andata ben oltre e ha di fatto assunto il controllo totale su una molteplicità di operazioni critiche, per esempio negli aeroporti o nelle stazioni, senza dimenticare la sanità o il manifatturiero, il mondo dei servizi. Industria 4.0 è sotto questo aspetto un esemplare punto di non ritorno. E tutto è accaduto con una rapidità impressionante, eccessiva nell'opinione di Domenico Raguseo, tale da coglierci per molti versi impreparati e indifesi. La pandemia da Covid-19 stessa ha portato con sé una rivoluzione, sospinta soprattutto dall'affermazione su larga scala del cosiddetto smart working. «Ha accelerato», ha detto Raguseo, «il percorso virtuoso della digitalizzazione, ma l'accelerazione si è focalizzata su priorità che non erano la CyberSecurity. Mi aspetterei che le aziende e le persone investano in consapevolezza ma, soprattutto, che i servizi forniti debbano essere sicuri. L'ultimo quarto dell'anno sarà forse il più pericoloso. Spero che aziende e istituzioni continuino a investire in CyberSecurity, non solo in connettività e automazione». La vulnerabilità, fuori e dentro casa Opinione del direttore è che il lavoro a distanza sia veicolo di problemi per le imprese, più che per i loro addetti. «Lavorare a casa», è la sua visione, «può significare trasferire la poca attenzione alla sicurezza dei singoli individui anche al di fuori delle mura domestiche. Si dovrebbe disporre di strumenti e barriere protettive adeguati, mentre come spesso accade si utilizzano pc condivisi

col resto della famiglia: il che, per l'azienda può esser motivo di rischi e allarmi. In più, il collegamento fra persona e sede passa dai router domestici e questo sancisce l'impossibilità di garantire un livello di sicurezza non soltanto adeguato, ma anche uguale per tutti i dipendenti connessi remotamente». In realtà, qualche rimedio ci sarebbe. «Si può provvedere», ha suggerito Raguseo, «a una messa in sicurezza di reti, strumenti e accessi da remoto mediante la segmentazione o micro-segmentazione delle connessioni, con policy che non tengano conto dei soli IP-address ma di tutte le risorse coinvolte nelle operazioni. Proteggere i dispositivi», ha concluso, «è un fattore essenziale. Mettere al sicuro un laptop significa salvaguardare il business. E questo è praticabile con applicazioni antivirus e anti-malware aggiornate o soluzioni EDR - Endpoint detection response - sugli account attivi e le risorse aziendali in genere. Non da ultimo, segnalare immediatamente ogni malfunzionamento e verificare che tutte le anomalie siano segnalate e bloccate sin dal principio».