Ransomware in crescita globale del 15% nel 2019, +195% nel Regno Unito: è l'era del banditismo informatico

Difendere il proprio ecosistema digitale ed informatico non è cosa facile oggi. Che siano aziende, amministrazioni pubbliche, organizzazioni internazionali, o piccole realtà, fino alla nostra casa, ogni dispositivo collegato in rete è una porta che favorisce un attacco.
Nell'ultimo **Rapporto** SonicWall, relativo alle minacce informatiche rilevate in 200 Paesi di tutto il mondo nel primo semestre 2019, si evidenzia un'escalation nell'utilizzo di diversi strumenti *cyber crime*, soprattutto il nuovo *ransomware as a service*, il *malware open source* e il tradizionale *cryptojacking*.

"*Le imprese continuano la loro battaglia di monitoraggio dei modelli con cui si sviluppano gli attacchi informatici – il passaggio ai cocktail malware e ai vettori delle minacce in evoluzione – cosa che rende estremamente difficile difendersi*", ha dichiarato **Bill Conner**, Presidente e CEO di SonicWall.
"*Nella prima metà del 2019 la nostra tecnologia Real-Time Deep Memory Inspection (RTDMI) ha scoperto **74.360 varianti di malware** fino a quel momento sconosciute. Per essere efficienti, le imprese devono sfruttare tecnologie innovative come l'**apprendimento automatico**, in modo da poter intervenire in anticipo contro le strategie di attacco che mutano costantemente*".

Solo per dare alcuni dati riportati dallo studio: nei primi

sei mesi del 2019 gli attacchi malware rilevati sono stati 4,8 miliardi, più di 8,3 milioni gli attacchi ***phishing*** e decine di migliaia di virus finora mai conosciuti.
Prendiamo i *ransomware*, i temibili attacchi che vanno tanto di moda e che vengono utilizzati dai *cyber* criminali per bloccare un dispositivo e chiedere un riscatto per ripristinarne l'accesso.
Mentre il volume di *malware* globale è calato del 20%, è stato osservato un concomitante **aumento del 15% di attacchi ransomware a livello mondiale, che hanno raggiunto un incremento pari al 195% nel Regno Unito**. Gli stessi ricercatori attribuiscono questi dati alla preferenza che i criminali informatici stanno dando ai kit ***ransomware-as-a-service* (RaaS)** e ***malware open-source***, il che costituisce una novità.

Anche l'***Internet of Things*** o IoT diventa dispensa malware a passo di record e mentre aziende e consumatori continuano a collegare apparecchi a internet senza idonee misure di sicurezza, i dispositivi IoT vengono sfruttati in misura crescente dai cibercriminali per distribuire payload di malware. **Nella prima metà del 2019 è stato rilevato un aumento del 55% di attacchi IoT,** vale a dire più dei primi due trimestri dell'anno precedente.

Più crescono i ***bitcoin***, maggiori le minacce portate dalle pratiche di *cryptojacking*, cioè tecniche tese a forzare sistemi informatici a minare *cryptocoin* sfruttando la potenza di calcolo inutilizzata di processori, SoC e acceleratori grafici, di aziende, come di singoli utenti a casa.
Nei primi sei mesi dell'anno il volume di cryptojacking ha toccato quota 52,7 milioni, con un aumento del 9% rispetto all'ultimo semestre del 2018. Questa crescita è parzialmente imputabile all'aumento del prezzo di *bitcoin* e *Monero*, il che fa sì che tale fenomeno continui ad essere redditizio per i

cibercriminali.
Una delle cause di una così alta incidenza è che i siti web compromessi non sono stati puliti dopo l'infezione, per quanto il servizio *Coinhive* (programma di punta per il mining i criptovalute) non esista più da marzo 2019 e l'URL sia stato abbandonato.

https://www.key4biz.it/ransomware-in-crescita-globale-del-15-nel-2019-195-nel-regno-unito-e-lera-del-banditismo-informatico/266882/

Data breach, per le imprese italiane un costo medio di 3,13 milioni di euro

Non solo aumenta il numero di attacchi informatici alle aziende di tutto il mondo, ma anche il valore complessivo del danno e quello medio per singola organizzazione. Il rapporto annuale "***Cost of a Data Breach***" (Costo di una violazione di dati) sponsorizzato da IBM Security e condotto dal Ponemon Institute si concentra sia sulle imprese a livello globale, sia di singoli mercati, come ad esempio quello italiano.

"*Il cybercrime è fonte di guadagno per i criminali informatici e a questo corrispondono perdite significative per le aziende colpite*", ha affermato **Wendi Whitmore**, Global Lead di IBM X-Force Incident Response and Intelligence Services.
"*Considerando che l**e organizzazioni hanno dovuto affrontare la perdita o il furto di oltre 11,7 miliardi di dati solo negli ultimi 3 anni**, le imprese devono essere pienamente consapevoli dell'impatto finanziario che una violazione dei dati può avere sui loro profitti e, quindi, concentrarsi su come è possibile*

ridurre questi costi”.

Del campione globale fanno parte 26 aziende italiane, intervistate nell’arco degli ultimi otto anni, i cui dati si possono riassumere come segue: **3,13 milioni di euro è il costo totale medio della violazione dei dati subite dalle aziende italiane,** che rappresenta un aumento del 9,36% rispetto all’anno precedente; 130 euro è il costo pro capite per record smarrito o rubato, con un aumento del 3,13% rispetto all’anno precedente; la causa principale, pari al 46% delle violazioni dei dati, è da ricondurre ad attacchi malevoli o criminali.

Aumenta anche il **tempo medio necessario per identificare la violazione dei dati, che nell’ultimo anno è passato da 199 a 213 giorni**, è quello per contenere la violazione dei dati, che è passato da 56 a 70 giorni.

A livello mondiale, invece, **il costo della singola *data breach* è di 3,92 milioni di dollari in media**, in aumento del 12% negli ultimi cinque anni. Un trend frutto di diversi fattori in gioco, tra cui: “*impatto finanziario pluriennale delle violazioni, aumento delle regolamentazioni e aumento del complesso processo di risoluzione degli attacchi criminali*”.

Un attacco, però, non si esaurisce nel momento del suo impatto iniziale. Come ha spiegato bene lo studio IBM: “***il 67% dei costi della violazione di dati viene registrato entro il primo anno, il 22% nel secondo anno e un altro 11% si estende oltre i due anni*** *dall’attacco. I costi sono risultati più elevati nel secondo e terzo anno per le aziende operanti in ambienti altamente regolamentati, come la sanità, i servizi finanziari, l’energia e l’industria farmaceutica*”.

> *Data breach, per le imprese italiane un costo medio di 3,13 milioni di euro*

Procuratore generale Usa: ‘Non escludo legge per obbligare le big tech a creare backdoor per l’Intelligence’

Ieri, in un discorso a New York, il procuratore generale degli Stati Uniti **William Barr** ha invitato le società tecnologiche a fare di più per aiutare le autorità federali a ottenere l’accesso ai dispositivi con un ordine legittimo.

Barr, che conduce anche l’indagine antitrust aperta nei confronti dei big tech, ha affermato che i consumatori dovrebbero accettare i rischi che le backdoor di crittografia comportano per la loro sicurezza informatica personale per garantire che le forze dell’ordine possano accedere alle comunicazioni crittografate.

Il direttore dell’**FBI Christopher Wray** ha dichiarato che il numero di dispositivi a cui non è stato possibile accedere è inferiore a un quarto dei 7.800 telefoni e tablet dichiarati.

La messaggistica crittografata è aumentata negli ultimi anni, arrivando ai dispositivi e servizi di **Apple**, **Facebook**, **Instagram** e **WhatsApp**, una risposta, non sicura al 100%, della Silicon Valley all’abuso di accesso da parte dei servizi di intelligence a seguito delle rivelazioni di **Edward Snowden** nel 2013.

Amnesty International: ‘Le app di messaggistica più usate al mondo, che utilizzano la crittografia di default, non sono sicure al 100%’

Una risposta non sicura perché, secondo **Amnesty International**, che l’anno scorso ha testato le 11 app di messaggistica più usate al mondo per verificare l’utilizzo della crittografia di default, WhatsApp, Messenger, Telegram, Snapchat e Skype non garantiscono una privacy al 100%. Con le cinesi WeChat e QQ il voto è 0/100. (Leggi il report di Amnesty International)

“Un rischio accettabile, non stiamo parlando dei codici di lancio nucleari’

Ora le forze dell’ordine Usa affermano che la crittografia impedisce l’accesso alle comunicazioni di cui hanno bisogno per perseguire i criminali.

Il Governo chiama questo “*oscuramento*” perché non riesce ad accedere nelle comunicazioni crittografate, e rimane un punto di discussione chiave da parte delle autorità.

Nelle osservazioni, Barr ha affermato che “*il significato del rischio dovrebbe essere valutato in base al suo effetto pratico sulla sicurezza informatica dei consumatori, nonché alla sua relazione con i rischi netti che l’offerta del prodotto rappresenta per la società”.*

Il procuratore generale degli Stati Uniti ha suggerito dunque che *“il rischio residuo di vulnerabilità derivante*

dall'integrazione di un meccanismo di accesso lecito è materialmente maggiore di quelli già presenti nel prodotto non modificato".

Il rischio, ha detto, è accettabile perché *"stiamo parlando di prodotti e servizi di consumo come messaggistica, smartphone, email e applicazioni voce e dati"* e *"non stiamo parlando di proteggere i codici del lancio nucleare della Nazione".*

Il procuratore generale ha affermato che è "*insostenibile*" che i dispositivi offrano una crittografia non "craccabile", offrendo allo stesso tempo l'accesso zero alle forze dell'ordine.

Barr è l'ultimo di una serie di procuratori generali a denunciare l'incapacità delle forze dell'ordine di accedere alle comunicazioni crittografate, nonostante il respingimento da parte delle società tecnologiche.

Sono "*scandalose, sbagliate e pericolose",* così il senatore dell'Oregon **Ron Wyden** (D-OR) ha commentato le richieste del procuratore generale: *"Se diamo a Barr e a questo Presidente /Trump) il potere, senza precedenti, di violare la crittografia su tutta la linea, ed entrare così nei dettagli più intimi della vita di ogni americano – abuserebbero dei poteri",* ha concluso il senatore.

Stessa richiesta da parte di Uk, ma non accettata dai big tech

Gli Stati Uniti non solo gli unici ad avanzare questa proposta ai big tech.

All'inizio di quest'anno anche le autorità britanniche hanno proposto un nuovo meccanismo di backdoor, il cosiddetto "protocollo fantasma", che avrebbe consentito alle forze dell'ordine di accedere alle comunicazioni crittografate come se fossero parte di una conversazione privata. **Apple**, **Google**,

Microsoft e **WhatsApp** hanno respinto la proposta.

Barr non ha escluso di sostenere una legge per costringere le aziende tecnologiche a costruire backdoor per l'Intelligence. La sua iniziativa è stata subito bocciata da **Gen Michael Hayden**, l'ex direttore della CIA e della NSA, che su Twitter, ha scritto: '*Non proprio. Ed ero il direttore dell'Agenzia di Sicurezza Nazionale'.*

> *Procuratore generale Usa: 'Non escludo legge per obbligare le big tech a creare backdoor per l'Intelligence'*

Cyber sicurezza, negli ultimi due anni le imprese italiane sono aumentate del 300%

Nei giorni scorsi il Governo ha approvato un disegno di legge in materia di perimetro di sicurezza nazionale cibernetica. Il testo introduce disposizioni volte ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.
Questo perché la realtà in cui viviamo vede crescere

costantemente il numero di minacce alla sicurezza informatica, non solo per noi cittadini e utenti di rete, ma anche per le aziende e per le stesse Istituzioni, che si vedono obbligate ad aumentare i livelli di difesa soprattutto delle infrastrutture strategiche nazionali.

Per affrontare questa nuova sfida, da una parte **crescerà la spesa globale in prodotti e servizi di cyber sicurezza, valutata tra il 2017 ed il 2021 in più di 1.000 miliardi di dollari**, secondo stime del "*Cybercrime Report 2019*" di Cybersecurity Ventures, dall'altra, però, il **calcolo dei danni economici** provocati dai cyber criminali andrà lievitando in maniera evidente, con la possibilità concreta di raggiungere la cifra stratosferica di **6.000 miliardi di dollari**.

Sebbene la percezione dei rischi legati ai crimini informatici nel nostro Paese sia ancora molto bassa, tale scenario riguarda da vicino anche noi e negli ultimi anni si è assistito ad una crescita molto significativa del numero di imprese che offrono strumenti e servizi per combattere questa nuova minaccia.
Tra la fine del 2017 e i primi tre mesi del 2019, **le imprese italiane che offrono servizi nel campo della sicurezza informatica o della cybersecurity sono aumentate di oltre il 300**%, passando da poco meno di 700 a oltre 2.800 unità.

Il dato è relativo ad un'elaborazione Unioncamere-InfoCamere e a questo 'balzo' nel numero degli operatori si è accompagnato anche un aumento ancora più marcato (quattro volte) nel numero degli **addetti, che sono passati nello stesso periodo da 5.600 a 23.300 unità (+316%)**, corrispondenti ad una media di 8 addetti per azienda al 31 marzo di quest'anno.

Cyber sicurezza, negli ultimi due anni le imprese italiane sono aumentate del 300%

007 russi hackerati. Ecco i 4 progetti su cui lavorano gli agenti di Mosca

La società informatica **SyTech**, fornitore dei servizi segreti russi dell'**Fsb**, è stata vittima dell'attacco di un gruppo anonimo di hacker, che avrebbero sottratto circa 7,5 terabyte di informazioni riservate, secondo quanto ricostruito dalla **Bbc**. Tra i documenti trafugati, condivisi con alcuni organi di stampa, vi sarebbero le prove dei quattro progetti su cui lavorano gli 007 russi.

- "Nautilus-S", si tratta di una operazione di de-anonimizzazione del software **Tor**, usato per navigare anonimamente in rete. L'operazione è probabilmente fatta per tracciare e spiare gli avversari interni del regime.
- "Nautilus", è un'operazione che era in corso al momento dell'hackeraggio, di esfiltrazione e raccolta illegale di dati dai social network (i social network "esfiltrati" sarebbero **Facebook**, **LinkedIn**, ecc..) .
- L'Internet sovranista. Il terzo si chiama "Hope", una serie di attività preparatorie alla separazione dell'Internet russa (**Runet**) dal resto dei network degli altri paesi. I provider potrebbero esser costretti a staccarsi da tutti i server stranieri, poggiando solo sul **DNS**, il dominio russo. Quest'ultima è un'iniziativa nota da tempo, dopo che a febbraio di quest'anno Mosca ha approvato delle leggi per dotare il Paese di un proprio Internet parallelo.
- Spiare le imprese. Il quarto si chiama "Mentor", consiste in una raccolta dati prelevati ad aziende che operano in Russia. Una forma di attività che rientra

nello spionaggio industriale di Stato.

I dettagli dell’attacco hacker

L’**Fsb** (acronimo inglese per Federal Security Service of the Russian Federation) è una delle principali agenzie d’intelligence al mondo, insieme all’**Fbi** statunitense e all’**Mi5** britannico. Tra le sue competenze, sono comprese quelle per l’ambito cibernetico e per lo spionaggio internazionale.

Gli hacker – che agiscono sotto lo pseudonimo di “0v1ru$” – hanno rivendicato l’attacco su Twitter il 13 luglio, pubblicando lo screenshot di una pagina del sito di SyTech da loro modificata, per mostrare la capacita’ di agire sui sistemi della societa’.

Successivamente i criminali informatici hanno condiviso le informazioni trafugate al collettivo hacker Digital Revolution, che le ha inviate ad alcune testate giornalistiche. Secondo la Bbc, si tratterebbe del più importante furto di informazioni mai subito dai servizi russi, anche se nessun segreto di Stato è stato rivelato.

007 russi hackerati. Ecco i 4 progetti su cui lavorano gli agenti di Mosca

Il Consiglio dei Ministri ha approvato il ddl cybersecurity: le 5 novità

Il Consiglio dei ministri, su proposta del **Presidente Giuseppe Conte**, ha approvato un disegno di legge in materia di perimetro di sicurezza nazionale cibernetica.

Il testo introduce disposizioni volte ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

A questo scopo, il disegno di legge prevede, tra l'altro:

- la definizione delle finalità del perimetro e delle modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, dei sistemi informativi e dei servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica per i quali si applicano le misure di sicurezza e le procedure introdotte;
- l'istituzione di un meccanismo teso ad assicurare un *procurement* più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;

- l’individuazione delle competenze del Ministero dello sviluppo economico – per i soggetti privati inclusi nel perimetro – e dell’Agenzia per l’Italia Digitale (AgID) – per le amministrazioni pubbliche;
- l’istituzione di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti;
- lo svolgimento delle attività di ispezione e verifica da parte delle strutture specializzate in tema di protezione di reti e sistemi nonché, per quanto riguarda la prevenzione e il contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti.

Il Ddl prende il posto del decreto Golden Power sul 5G, sul quale il Governo ha cambiato idea: non sarà più convertito in legge, così i suoi effetti decadranno.

https://www.key4biz.it/il-consiglio-dei-ministri-ha-approvato-il-ddl-cybersecurity/266221/

Swascan e le vulnerabilità di Huawei

Finanza Agevolata è la rubrica a cura di **Sercam Advisory** dedicata agli aggiornamenti sui bandi pubblici (europei, nazionali, regionali) aperti o in prossima apertura. Per consultare tutti gli articoli clicca qui.
Lo scorso 8 luglio gli esperti **Swascan** avevano identificato una serie di criticità sull’infrastruttura e sulle web app **Huawei**.

Huawei, in un comunicato rilasciato il 15 luglio, ha dichiarato che "*le vulnerabilità scoperte da Swascan scoperte sono irrilevanti per i prodotti e le soluzioni vendute da Huawei. Sono rilevanti solo per le potenziali vulnerabilità del sistema IT*". Abbiamo chiesto a **Pierguido Iezzi**, Co-Founder di Swascan, chiarimenti sulla vicenda.

Key4biz. ***Dott. Iezzi perché è arrivata questa precisazione da Huawei?***

***Pierguido Iezzi*.** Posso supporre che la dichiarazione sia stata necessaria per fornire un chiarimento. La precisazione di Huawei era già indicata nel comunicato stampa che era stato concordato e autorizzato dalla stessa Huawei. L'attività di *Responsible Vulnerability Disclosure* era riferita alla digital infrastructure.

Key4biz*. Le vulnerabilità scoperte da Swascan non appartengono allora alle web app?*

Pierguido Iezzi. Come indicato nel comunicato le criticità erano riferite a web app e server dell'infrastruttura IT. Da parte nostra ringraziamo Huawei per averci autorizzato alla pubblicazione. E' l'ennesimo attestato di stima e serietà professionale che è stata riconosciuta al Team di Swascan.

Un attestato che si aggiunge a quella di altri big del settore IT come **Adobe, Microsoft e Lenovo.**

Quando a maggio abbiamo contattato Huawei, l'attenzione che ha dimostrato verso le nostre scoperte, unitamente agli scambi di e-mail, le valutazioni, le attività di remediation e i tempi di risoluzione sono stati tra i più seri, professionali e trasparenti che abbiamo potuto sperimentare in prima persona.

La filosofia alla base dei *Responsible Vulnerability Discosure*

è quella di portare maggiore attenzione sull'importanza di una collaborazione reale, vera, efficace ed efficiente tra i software vendor e le aziende di CyberSecurity.

Molto probabilmente è stato proprio questo approccio ad essere premiato e non dovrebbe lasciare perplessi che sia una azienda italiana a fare queste scoperte.

Non dobbiamo dimenticare che la scena dell'hacking italiano ha delle eccellenze di primo piano a livello internazionale sia come aziende che come singoli.

Riprendendo una dichiarazione dell'amico e socio **Raoul Chiesa** *"Sono italiani molti hacker white-hat che contribuiscono alla lotta ai malware e alle altre minacce cyber. Siamo creativi, abbiamo quella capacità alquanto rara all'estero di 'pensare e vedere le cose in un altro modo. Questo si traduce in centinaia di hacker etici i quali, nel corso degli anni, hanno sviluppato software, identificato vulnerabilità, calcato le scene delle più importanti conferenze hacker internazionali"*.

L' hacking italiano non è sempre riuscito a fare squadra e sistema per consolidare questa leadership nel settore.

L'aspetto positivo è che le cose stanno cambiando. La maturità degli attori e la fiducia professionale sta prendendo il sopravvento sul campanilismo dei singoli.

https://www.key4biz.it/falla-sistemi-huawei-la-precisazione-di-swascan/265900/

Cybersecurity, la Difesa

investe poco: solo 500 milioni in 16 anni contro 1,4 miliardi della Francia nel 2018

“La sicurezza cyber costituisce un settore strategico nevralgico per la protezione delle infrastrutture critiche istituzionali di un’amministrazione che opera a garanzia degli interessi nazionali del Paese”, si legge nel Documento programmatico pluriennale (**Dpp**) della Difesa, relativo al triennio 2019-2021*. “Il crescente livello della minaccia cibernetica, impone, quindi, di proseguire con il programma di potenziamento dei livelli di sicurezza”,* è scritto nel documento governativo. Peccato che a questa strategia non corrisponda un’adeguato investimento economico.

Nel Dpp, pubblicato di recente dal Ministero della Difesa, si nota che il Governo per rafforzare la cybersecurity ha aggiunto soltanto un milione di euro per ciascuno dei tre anni, come previsto da un emendamento della legge di Bilancio 2019. Per un totale di 500 milioni di euro fino al 2033. Quanti sono, pochi o molti soldi investiti per tenere al sicuro le infrastrutture critiche dell’Italia? Per capirlo basta confrontare la cifra con quanto stanziato dagli altri Stati, a partire da quelli europei.

1,4 miliardi per la cybersecurity stanziati in Francia solo nel 2018

La Francia nel gennaio 2018 hanno inserito nella Finanziaria 4,8 miliardi per la Ricerca e Sviluppo, di cui 1,4 miliardi per quella relativa alla cybersecurity. Nella legge di programmazione militare 2019-2025 si prevede una spesa

complessiva di 78 miliardi per la costituzione di una cyber-armata di 6mila addetti. La strategia francese si distingue in Europa per proattività perché si pone in chiave non solo difensiva, ma anche offensiva, laddove si individuino possibili pericoli per la sicurezza nazionale. Quanto alla Gran Bretagna, ha un National Cyber Security Programme con una dotazione di circa 1,5 miliardo di euro.

L'altro parametro di riferimento per capire il valore dei fondi stanziati dall'Italia per la cybersecurity il documento redatto ogni anno dall'agenzia **Onu** per le telecomunicazioni, il *Global Cybersecurity Index*, che misura il grado di sicurezza informatica di 175 Paesi. L'Italia si posiziona nel 2018 al 25esimo posto. In miglioramento dal 31esimo del 2017, ma dietro tutti i Paesi europei avanzati e alle spalle di emergenti come Lituania, Georgia e Croazia.

L'esigua cifra investita dall'Italia stride un po' con quanto dichiarato dal ministro della Difesa, **Elisabetta Trenta**, quando a luglio scorso nell'illustrare in Parlamento le linee programmatiche del Dicastero, ha posto grande attenzione alla cybersecurity: *"La minaccia cyber è un imprescindibile fattore di rischio per il Paese. È necessario continuare ad investire in tecnologia per contrastare in maniera efficace la cyber guerra".*

https://www.key4biz.it/cybersecurity-la-difesa-investe-poco-solo-500-milioni-in-16-anni-contro-14-miliardi-della-francia-nel-2018/265445/

Cybercrime, scoperta vulnerabilità sull'infrastruttura Huawei

Gli esperti **Swascan** hanno identificato una serie di criticità sull'infrastruttura e sulle web app **Huawei**.

Secondo quanto riporta l'azienda – la prima piattaforma cloudbased
di Cybersecurity Testing italiana – dal *Responsible Vulnerability Disclosure* sono emerse alcune vulnerabilità di livello critical che, se sfruttate da Hacker criminali, avrebbero potuto impattare la Business continuity, la sicurezza di dati e informazioni degli utenti e la regolare attività dei servizi.

La società italiana, che grazie al suo Team era già stata in grado di svelare, tra le altre, le vulnerabilità di **Adobe**, **Microsoft** e **Lenovo** ha contattato i corrispettivi **Huawei** per informarli delle vulnerabilità identificate e per impostare una collaborazione volta all'attività di remediation di queste falle.

"*Nel mondo della Cyber security si sta affermando finalmente il principio della collaborazione. I rischi aumentano di n volte di anno in anno e a fronte di questo si è reso necessario un Paradigm Shift culturale oltre che tecnologico. La nostra esperienza con Huawei dimostra che se recepiti correttamente questi valori possono essere un'ulteriore colonna portante per creare un Cyber Security Framework efficace ed efficiente*", ha dichiarato **Pierguido Iezzi**, Co-Founder di Swascan.

In dettaglio le vulnerabilità appartenevano alle seguenti categorie CWE:

• **CWE-119** (Improper Restriction of Operations within the Bounds of a Memory Buffer): Il software esegue operazioni su un buffer di memoria, ma può leggere o scrivere in una posizione di memoria che si trova al di fuori del confine previsto del buffer. Se la memoria accessibile dall'attaccante può essere efficacemente controllata, può essere possibile eseguire codice arbitrario, come nel caso di un buffer overflow standard. Se l'attaccante può sovrascrivere la memoria di un puntatore (di solito 32 o 64 bit), sarà in grado di reindirizzare un puntatore di funzione al proprio codice dannoso. Anche quando l'attaccante può modificare solo un singolo byte, l'esecuzione arbitraria del codice è possibile. A volte questo è dovuto al fatto che lo stesso problema può essere sfruttato ripetutamente con lo stesso effetto. Altre volte è perché l'aggressore può sovrascrivere dati critici per la sicurezza specifici di un'applicazione – come un flag che indica se l'utente è un amministratore.

• **CWE-125** (Out-of-bounds Read): Il software legge i dati oltre la fine, o prima dell'inizio, del buffer previsto. In genere, questo può consentire agli aggressori di leggere informazioni sensibili da altre posizioni di memoria o causare un crash.

• **CWE-78** (OS Command Injection): Il software costruisce tutto o parte di un comando OS utilizzando input influenzati dall'esterno da un componente upstream, ma non neutralizza o neutralizza in modo errato elementi speciali che potrebbero modificare il comando OS previsto quando viene inviato a un componente a valle.

Gli aggressori potrebbero eseguire comandi non autorizzati, che potrebbero essere utilizzati per disabilitare il software o per leggere e modificare dati per i quali l'aggressore non ha il permesso di accedere direttamente.

Poiché l’applicazione mirata esegue direttamente i comandi al posto dell’aggressore, qualsiasi attività dannosa può sembrare che provenga dall’applicazione o dal proprietario dell’applicazione.

L’esperienza di cooperazione tra Swascan e Huawei riafferma quanto sottolineato da Pierguido Iezzi: per far fronte alle emergenti minacce dei Criminal hacker c’è bisogno di una doppia azione: lato azienda è necessaria un’infrastruttura informatica sicura e un personale qualificato, unita però alle competenze e agli strumenti che solo gli esperti di Cyber Security possono dare

https://www.key4biz.it/cybercrime-scoperta-vulnerabilita-sulli nfrastruttura-huawei/264347/

Blue OLEx 2019, ieri la prima esercitazione Ue in caso di cyber crisi

Si è svolta ieri a Parigi l’**esercitazione** congiunta dell’Agenzia dell’Unione europea per la sicurezza informatica (*European union agency for cybersecurity* o Enisa), della Commission europea e i rappresentanti di 23 Stati membri, denominata “***Blue OLEx 2019***”.
La prima in Europa di questo genere, organizzata in due giorni (2-3 luglio), per un test di alto livello concentrato tutto sul livello operativo, per meglio definire il **quadro generale di risposta coordinata dei partner europei ad una crisi informatica improvvisa**.

#NISCooperationGroup è al lavoro su #BlueOlex19,

> *un'esercitazione di alto livello con i Paesi Ue, #ENISA ed #EUCommission. Presente anche l'Italia con il #DIS. Obiettivo: rafforzare la capacità degli Stati in caso di crisi cibernetica in Europa. #cybersecurity #sicurezzanazionale pic.twitter.com/kTOeiYKGab*
>
> *— Sicurezza Nazionale (@SicNazionale) 2 luglio 2019*

All'esercitazione hanno preso parte i rappresentanti di alto livello delle autorità nazionali per la cibersicurezza e **per l'Italia cera il Dis, Dipartimento informazioni per la sicurezza**.
L'operazione è stata condotta nel quadro della direttiva sulla sicurezza delle reti e dell'informazione, che ha istituito la cooperazione operativa e tecnica tra gli Stati membri tramite la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT).
I risultati della prova, oltre alle prime indicazioni sul momento, aiuteranno a **sviluppare le procedure operative standardizzate previste nel quadro della raccomandazione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza dell'UE** e degli Stati membri, adottata nel 2017.

L'***incident response***, o quadro di risposta della crisi informatica in Europa, più conosciuto con il termine "***Blueprint***", serve proprio a fronteggiare una crisi cibernetica improvvisa e prevede un livello tattico di azione (per risolvere e analizzare il problema), uno più operativo (per il coordinamento della risposta e una prima valutazione dei danni) e uno strategico (per il coinvolgimento diretto dei decisori politici nazionali e a livello di Unione in fase decisionale).

> *Exciting 2nd day at #BlueOlex19 together with @ANSSI_FR , @EU_Commission, @dsn, @Cybersec_EU and the #NISGroup. Working together to develop mechanisms that could efficiently manage*

> *a cyber crisis affecting EU Member States! https://t.co/U4AxqBhuZT pic.twitter.com/pz4zFih9N6*
>
> *— ENISA (@enisa_eu) 3 luglio 2019*

Il *Blue Olex 2019* è servito e servirà proprio a testare il livello di risposta che l'Unione è in grado di mettere in campo nel più breve tempo possibile e nel modo più efficace appunto a livello operativo, tattico e strategico.
Un modello di risposta in fase di sviluppo ed implementazione che consentirà alla politica di adottare le decisioni migliori a cui poi sarà dato seguito a livello tecnico coinvolgendo i CERT nazionali in cooperazione con il CERT-EU e l'ENISA.

Sempre ieri, intanto, **l'Italia ha appena dato seguito ad un altro punto chiave previsto dalla cosiddetta Direttiva europea Nis** (*Network and information security*) sul rafforzamento delle risposte da parte degli Stati membri ad un attacco cibernetico.
A livello nazionale, le Autorità competenti all'attuazione della normativa Ue (i Ministeri dello sviluppo economico, delle infrastrutture e dei trasporti, dell'economia e delle finanze, della salute, dell'ambiente e della tutela del territorio e del mare, in collaborazione con Regioni e Province autonome di Trento e di Bolzano), hanno elaborato le **linee guida per la gestione dei rischi e la prevenzione e mitigazione degli incidenti** che hanno un impatto rilevante sulla continuità e sulla fornitura dei servizi essenziali.

> *Blue OLEx 2019, ieri la prima esercitazione Ue in caso di cyber crisi*