Cisco scopre backdoor in alcuni suoi dispositivi. Allora dovrebbe scattare il ban per la società Usa?

Il primo maggio scorso, la statunitense **Cisco** ha risolto con 40 *patch* una vulnerabilità di sicurezza in alcuni dei suoi dispositivi di rete che avrebbe potuto essere sfruttata dai malintenzionati per accedere alle apparecchiature IT e spiare gli utenti.

"*Una vulnerabilità nella gestione delle chiavi SSH per il software Switch della modalità ACI (Application Centric Infrastructure) Cisco Nexus serie 9000 può consentire a un utente malintenzionato remoto non autenticato di connettersi al sistema interessato con i privilegi dell'utente root",* ha dichiarato Cisco, nella nota in cui mette a disposizione l'aggiornamento del software.

Ma la notizia non ha destato scalpore come quella riportata da *Bloomberg* il 30 aprile: il gruppo **Vodafone** ha riscontrato vulnerabilità in alcuni apparati forniti da **Huawei**, ma le problematiche in Italia, *"sono state tutte risolte tra il 2011 e il 2012 e non abbiamo prove",* ha sottolineato Vodafone*, "di accessi non autorizzati".*

L'agenzia ha poi aggiunto una considerazione smentita da Vodafone. È falso, invece, ha aggiunto l'operatore, "*quanto riportato da Bloomberg che afferma come tali vulnerabilità avrebbero potuto 'aver dato a Huawei l'accesso non autorizzato alla rete fissa della compagnia in Italia'.*

Smascherata la campagna Usa contro Huawei

Dunque, se il *Telnet* riscontrato da Vodafone 7-8 anni fa in alcuni apparati di Huawei, risolto e per giunta non accessibile da Internet, è una ragione sufficiente per gli Stati Uniti per bannare Huawei dalle reti in Occidente, allora anche dopo la scoperta di Cisco della vulnerabilità nel Cisco Nexus serie 9000 dovrebbe spingere i Paesi europei ad escludere la società Usa dalle sue infrastrutture di Tlc? E non è la prima volta che l'americana Cisco risolve 'backdoor' nei suoi dispositivi. Nel 2018 sono state trovate 5 backdoor nei router di **Cisco**. Il principale fornitore mondiale di apparecchiature di rete e di software aziendali ha poi rimosso 4 mesi dopo una serie di backdoor dai suoi prodotti

Ovviamente i bug se risolti appena riscontrati non sono un valido motivo né per far scattare un allarme sulla sicurezza dei dispositivi e delle infrastrutture né per escludere un fornitore di telecomunicazioni da un mercato. Anzi le individuazioni di 'backdoor' sono la controprova della sicurezza delle apparecchiature costantemente verificate dagli operatori. Occorre, però, capire quando ci si trova di fronte a notizie enfatizzate solo per avvalorare la propaganda Usa secondo la quale Huawei agisce come agente di spionaggio della Cina e quindi rappresenti un rischio per la sicurezza nazionale dei Paesi che utilizzano le sue apparecchiature. Non a caso nessun Paese europeo si è lasciato convincere dall'amministrazione Trump bannando Huawei e non l'hanno fatto per due motivi principali:

- I prezzi offerti dalla Tlc cinese sono particolarmente accessibili dal punto di vista economico rispetto ai competitor.
- Bannare Huawei in Europa significherebbe sviluppare la rete 5G e poi la commercializzazione dei servizi almeno con due anni di ritardo rispetto agli Usa. Ecco qual è

l’obiettivo non dichiarato della campagna americana.

Per saperne di più: 5G

Cisco scopre backdoor in alcuni suoi dispositivi. Allora dovrebbe scattare il ban per la società Usa?

Intelligenza artificiale, quali rischi si corrono nei sistemi esperti?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

McKinsey, in un recente articolo[1], avverte di possibili rischi nell’uso della Intelligenza Artificiale (AI). Se da una parte riconosce i vantaggi e la positiva percezione da parte degli imprenditori, dall’altra avverte che la AI è come una spada a doppio taglio: può ad esempio provocare – come accaduto in alcuni casi – che, dopo una elaborazione di grandi moli di dati, siano sorti problemi di privacy, svelando dati riservati o trattando i dati senza il preventivo consenso del cliente, o, piuttosto, in un modo non sicuro; in altri casi, si sono ottenute informazioni fuorvianti che hanno originato decisioni errate (ad esempio, derivanti da eccesso di fiducia nelle funzioni predittive della manutenzione; ecc.).

Perché cito questo articolo? Al di là del fatto che ho trovato spunti interessanti, mi ha ricordato una delle mie prime esperienze nella realizzazione di sistemi esperti, finalizzati

al trattamento di grandi moli di dati confidenziali. Quella volta mi andò benissimo (un successo inatteso), ma mi suonò come un avvertimento per il futuro (come molti sanno, le banche hanno da lunghissimo tempo delle apposite applicazioni atte ad assistere chi deve controllare la *compliance* alla normativa ed alla regolamentazione corrente).

Racconto brevemente l'episodio.

Il sistema esperto era finalizzato ad individuare eventuali possibili impiegati disonesti (per fortuna sono molto pochi, ma il danno di immagine che provocano è deleterio). Ciò che giunse inatteso, fu che il risultato fu assai apprezzato dalle filiali per un'altra ragione, diversa dalle finalità originarie!

Ero all'epoca responsabile dell'IT auditing in **BNL** e fra i nostri obiettivi vi era quello di aiutare l'Ispettorato (così si chiamava all'epoca) nell'individuare possibili frodi.

Una delle più antipatiche, vedeva un impiegato (spesso ricattato per il vizio del gioco o per altri vizi) prelevare quanto a lui necessario dai conti di persone anziane o altre che avevano comunque una discreta giacenza e prelevavano il denaro di rado. Il caso tipico era quello della persona pensionata che prelevava il minimo indispensabile, non aveva assegni, non faceva bonifici, ecc..

Dopo aver ascoltato gli ispettori che ci hanno illustrato le modalità operative generalmente seguite, abbiamo disegnato l'applicazione; questa, di notte, consultava tutti gli archivi necessari e, se trovava possibili comportamenti rientranti nelle casistiche a noi descritte, evidenziava la filiale ed il conto potenzialmente interessato.

Il Direttore della prima filiale da noi interpellata, mi

chiamò entusiasta! Aveva convocato un cliente il cui conto, normalmente interessato da versamenti e raramente da prelevamenti, da qualche giorno evidenziava cospicui prelevamenti tramite assegno. Tutto combaciava con le caratteristiche di una potenziale frode: aveva cambiato l'indirizzo per l'invio dell'estratto conto; aveva chiesto un carnet di assegni; aveva comunicato i dati di un delegato; e così via. Il quadro rientrava nella casistica da noi ipotizzata.

Il cliente ringraziò per essere stato convocato in quanto la banca finalmente dimostrava un interesse nella sua persona: ciò non era avvenuto fino ad ora, e, non solo, era stato addirittura maltrattato con il tasso creditore; infatti, gli era stato negato il tasso di interesse promesso e, di conseguenza, lui – per ripicca – aveva aperto il conto in un'altra banca e aveva iniziato a trasferire i soldi!

Una applicazione nata per individuare i ladri era invece ambita dalle filiali per analizzare comportamenti anomali dei clienti.

Da allora sono passati tanti anni, e le applicazioni nell'analisi della clientela hanno fatto passi enormi. Oltre a crescere in numero e qualità, devono affrontare grandissime moli di dati assai diversi, di diversa provenienza, di diversa frequenza di aggiornamento, ecc.

Questa mia breve testimonianza, molto semplice e quindi facilmente comprensibile da tutti, è per affermare che le applicazioni, finalizzate ad assistere il personale operativo e di business, spesso progettate per una determinata finalità, poi possono essere utili anche per altri fini, inizialmente non previsti.

Ma, attenzione! Come ci ricorda McKinsey, si tratta di una spada a doppio taglio: l'altra faccia della spada può essere invece una minaccia alla protezione dei dati personali o alla

continuità del business.

Non bisogna quindi trascurare una attenta analisi degli obiettivi e dei possibili output; non bisogna essere presi dalla fretta di mettere l'applicazione in produzione, ma esaminarne i contenuti e le fonti con estrema attenzione coinvolgendo nell'esame tutte le funzioni aziendali potenzialmente interessate.

Anthony.wright@anssaif.it

---

[1] https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

https://www.key4biz.it/intelligenza-artificiale-quali-rischi-si-corrono-nei-sistemi-esperti/256324/

Cloud Microsoft, scoperto database non protetto con informazioni di 80milioni di famiglie Usa

E' stato scoperto su un server cloud gestito da **Microsoft** un archivio di 24 gigabyte contenente i dati personali di 80 milioni di famiglie statunitensi.

L'archivio, non protetto, conteneva nomi, cognomi, date di nascita, indirizzi di residenza, genere, stipendio e stato civile di circa 80 milioni di famiglie USA (in totale in

America le famiglie sono 128 milioni).

Nel database erano presenti inoltre dettagli sulla tipologia di abitazione delle famiglie coinvolte, con tanto di coordinate geografiche per localizzarla su una mappa, e un'indicazione che specificava se si trattasse di un edificio di proprietà o in affitto.

Considerata la natura dei dati e il nome attribuito ad alcuni campi del file come "member_code" e "score", il sospetto è che potesse appartenere a qualche grande realtà del **settore immobiliare.**

Fonte: vpnMentor

Il leak scoperto da vpnMentor

La falla è stata scoperta da una coppia di ricercatori israeliani del team di **vpnMentor** che ha affermato di aver scoperto il database non protetto mentre lavorava ad un progetto di mappatura web.

Chi possiede i dati sul server non è noto. Tuttavia, il misterioso hacker ha deciso di dettagliare tutte le informazioni per famiglia, anziché per singoli individui.

"*Questo database aperto è una miniera d'oro per ladri di identità e altri aggressor*i", ha dichiarato **vpnMentor**. Ad esempio, il tesoro di informazioni potrebbe aiutare gli hacker a rivolgersi ai ricchi o alle persone in base all'età.

La buona notizia è che il server è stato messo al sicuro. "*Abbiamo notificato al proprietario del database e stiamo prendendo le misure appropriate per aiutare il cliente a*

rimuovere i dati fino a quando non può essere adeguatamente protetto“, ha detto Microsoft in una dichiarazione. Tuttavia l’azienda, ha rifiutato di nominare il cliente.

I potenziali pericoli per la privacy

L’accesso al tuo nome completo può aiutare gli hacker a indovinare il tuo indirizzo email. Molte persone usano nome.cognome@gmail.com come loro indirizzo email, quindi identificare la email è molto facile.

Questo scenario è solo la punta dell’iceberg. Gli indirizzi possono facilmente portare a numeri di telefono, rendendo le persone facili bersagli per le truffe di phishing. Le date di nascita e i codici postali sono risposte comuni alle domande di sicurezza. E la longitudine e la latitudine significano che le abitazioni possono essere individuate per eventuali furti.

https://www.key4biz.it/cloud-microsoft-scoperto-database-non-protetto-con-informazioni-di-80milioni-di-famiglie-usa/256182/

Hackerato il sito dell’Archivio di Stato. Raoul Chiesa: “L’Italia ‘Cyberdebole’ per le gare al

risparmio”

Anche il sito dell’**Archivio di Stato** è stato hacherato con oltre 5mila user e password violate e diffuse sui social. Tra gli account anche manager di **Eni** e della **Juventus**. A rivendicare il cyber attacco, sferrato la scorsa settimana, sono stati gli hacktivisti di **LulzSec Italia** con questo messaggio su **Twitter**: “*Ops, pensiamo ci sia un problema, date un occhiata a questi 5465 utenti con password in chiaro”.*

“*Banalmente mi sembra di tipo Sql injection”,* ha spiegato **Raoul Chiesa**, uno dei primi hacker etici italiani, celebre con lo pseudonimo di “Nobody”, intervistato da Valentino Di Giacomosul quotidiano *Il Mattino*. “*In due parole significa”,* ha aggiuntol’informatico torinese *“che se il programmatore scrive male il codice software anche se non hai una password ti puoi accreditare e accedere al sito come amministratore. Ormai è un tipo di attacco così semplice, diffuso da più di 10 anni, ci sono persino dei programmini sul web che riescono automaticamente a compiere queste incursioni. È incredibile che nel 2019 possano esserci ancora queste vulnerabilità strutturali su siti dello Stato dove transitano dati e informazioni che impattano non solo sulla sicurezza nazionale, ma anche su quella delle nostre imprese e dei cittadini in generale. Bisognerebbe investire di più, ma non c’è la volontà di farlo”.*

Come mai allora questa vulneralità su alcuni siti dello Stato?

Per una ragione economica e per una mancanza di cultura in cybersicurezza, ha detto Raul Chiesa nel corso dell’intervista. In particolare il problema iniziale è *“nelle gare di appalto affidate a chi fa il prezzo più basso”* e non a chi fornisce le migliore competenze e gli strumenti più efficaci nel settore: *“Il problema è che quando lo Stato fa*

delle gare di appalto per la creazione di questi portali si cerca sempre di rivolgersi a chi fa il prezzo più basso”, ha detto Chiesa. *“Dopodiché chi si è aggiudicato la gara fa partire una serie di subappalti a catena: poi alla fine chi realmente opera per costruire il sito magari è un ragazzo che prende 30 euro al giorno e non si può pretendere che oltre ad essere un esperto di grafica possa essere pure capace ad impostare determinati sistemi di sicurezza per rendere meno vulnerabile il sistema”,* ha sottolineato l’esperto di sicurezza informatica a livello internazionale. Infine Raul Chiesa lancia anche un messaggio alle Istituzioni per rendere i siti web dello Stato a prova di cybersecurity: *“Non esiste la consapevolezza della minaccia a tutti i livelli: dallo Stato, alle imprese, fino ai semplici cittadini. Eppure in Italia siamo molto bravi, ma i migliori programmatori fuggono all’estero proprio perché qui non abbiamo un’adeguata cultura della sicurezza informatica”.*

Una sottovalutazione che mette in pericolo la sicurezza nazionale su tutti i fronti, anche in campo militare. “L’Italia”, spiega il sottosegretario alla Difesa con delega alla cybersecurity, **Angelo Tofalo**, *“è ancora indietro rispetto alla consapevolezza della minaccia. Noi per la prima volta abbiamo messo al centro dell’agenda questa tematica, come ministero abbiamo costituito un gruppo di progetto per creare un nuovo Comando sulla cyber con alla guida un Generale a tre stelle. Tutti gli uffici della Difesa saranno messi insieme per migliorare lo scambio informativo tra i vari apparati”*. Da oltre un anno il **Cisr** (Comitato interministeriale per la sicurezza della Repubblica) ha dato la delega alla cybersecurity al vicedirettore del Dis, **Roberto Baldoni**.

Hackerato il sito dell’Archivio di Stato. Raoul Chiesa: “L’Italia ‘Cyberdebole’ per le gare al risparmio”

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

Seduto al tavolino di un bar accanto gli uffici di **Italiaonline** ad Assago, un hacker ha rubato credenziali di accesso alle caselle di posta elettronica di 1 milione e 400.000 clienti dei servizi di **Libero Mail** e di **Virgilio Mail.**

Sono questi gli esiti della vicenda raccontata dal *Corriere della Sera dell'attacco hacker avvenuto nel milanese,* messo a punto da un hacker 24enne.

Il criminale informatico, secondo la ricostruzione del Corriere, sarebbe entrato nelle rete Wifi dell'azienda attraverso l'uso di un computer portatile e di una grande antenna, usando la password di un dipendente e avrebbe iniziato l'attacco, riuscendo a violare **1 milione e 400mila dati.**

Sulla vicenda, secondo il quotidiano, sta indagando la **Procura di Milano** e sta svolgendo una apposita ispezione il **Garante per la privacy,** avvisato del Data Breach da Italiaonline come impone il GDPR, il nuovo regolamento europeo.

L'azienda ha fatto sapere che il sistema antintrusione ha funzionato dichiarando che "*allo stato attuale, non ci sono utenti che abbiano segnalato accessi indesiderati alla propria posta*".

Il rischio, invece, si palesa per chi usa la stessa password

della posta elettronica per accede ad altre piattaforme, quali conti bancari: in questo caso è necessario cambiare immediatamente tutte le parole chiave, per evitare che i pirati informatici si introducano nella piattaforma bancaria.

Consigli sulle password

Avere password differenti per ogni account, email o conti correnti è una buona regola per non essere vittime di criminali informatici e dover fare i conti con furti di dati. E allora ecco qualche semplice consiglio su come ricordare password complesse, in modo da poter ricordare tutte le password più importanti.

1. Creare una “static string” (quella parte di password che resta sempre uguale)

1. Pensare ad una frase, al testo di una canzone, alle citazioni di un film, ad una filastrocca o a qualcosa di simile, che sia facile da ricordare;
2. Prendere la prima lettera delle prime tre o prime cinque parole;
3. Aggiungere, tra una lettera e l’altra, un carattere speciale (ad esempio: #, @, / e simili).
4. Da questo momento in poi, è possibile basare tutte le proprie password uniche su questa singola stringa di caratteri.

2. Sfruttare la potenza dell’associazione di idee

1. In caso di necessità di una password per uno degli account online in uso (ad esempio per Facebook, Twitter, eBay, per l’online banking, per lo shopping online o i siti di videogiochi…), si deve prendere nota della prima

parola che si associa ad un determinato sito o ad una certa piattaforma.
2. Ad esempio, se si sta creando una password per l'account di Facebook, si potrebbe associare al social media il colore blu, presente nel logo. Basterebbe, quindi, aggiungere la parola "blu", magari in lettere maiuscole, alla fine della "static string" creata in precedenza

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

---

Cybercrime, cosa si vende nel dark web?

Cosa succede quando la parte di nascosta del web, dove hanno luogo le transazioni più sregolate decide di rinfrescare la sua impostazione commerciale?

Le implicazioni per la cybersecurity sono sicuramente molte, un tempo il **Dark web**, per definizione, era un luogo dove la sola parola garanzia era impronunciabile: le transazioni avvenivano in un contesto di massima insicurezza, senza alcuna certezza. Oggi, mimando il successo dell'on-line retail il Dark web si è dotato di uno dei componenti chiave del successo della sua controparte legale, le garanzie. Non solo, queste piattaforme distorte di eCommerce operano su piattaforme che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto, il tutto incorniciato con un'interfaccia intuitiva e responsive facilmente navigabile. Non mancano neppure elementi di customer care come FAQ, chat di supporto e dettagliate pagine di aiuto.

La valuta principale di scambio non è il dollaro e neppure lo yen, qui la fanno da padrone le cripto valute grazie alle loro caratteristiche che permettono grande anonimato e scarsa tracciabilità.

Tra la merce a disposizione al primo posto per numero di inserzioni regnano ancora gli stupefacenti, ma a breve distanza troviamo innumerevoli *hacking tools* e pacchetti di dati sensibili illegalmente ottenuti. Siamo dinnanzi a una *regolarizzazione* della delinquenza e le implicazioni per la cybersecurity sono molte.

Cybercrime commodity: i must have

Ma quali sono i programmi più popolari in vendita all'interno di queste piattaforme? Alcuni esempi delle categorie più popolari:

Tra i vari malware offerti sulle piattaforme, i più pericolosi sono sicuramente i Remove Access Trojan. Questa variante di software dannoso può mettere in condizione il pirata informatico di prendere totalmente il controllo del pc della sua vittima. Questo la rende scoperta e vulnerabile nei confronti di una pletora di potenziali crimini: dal furto di dati sensibili – dalle carte di credito, Paypal, dati di homebanking – al vero e proprio furto d'identità, ma i RAT sono anche usati per accedere alle webcam integrate che vengono sfruttate a fini di ricatto. Attenzione però, non sono solo i personal computer a essere aperti al rischio di questa infezione, alcune varianti di malware sono state in grado di contagiare anche nei dispositivi mobile che utilizzano l'OS Android.

Anche in questo caso fioriscono le offerte di programmi più o

meno differenti. I target più frequenti di questi programmi, utilizzati per sottrarre password, sono i siti social e di svago come Facebook e Spotify.

Il **phishing** è sicuramente uno dei vettori di cyberattacco più diffusi, quindi non c'è da stupirsi se all'interno del Dark web esistono centinaia di inserzioni in vendita per pagine che in maniera camaleontica replicano siti di brand affermati come Netflix, Facebook, Twitter…

Oltre ai metodi già citati sono disponibili una pletora di opzioni di Hacking in vendita a prezzi inferiori ai 10 dollari: i keyloggers – software in grado di catturare tutto ciò che viene digitato sulla tastiera del PC -, vari software in grado violare reti Wifi e connessione Bluetooth e malware progettati per sottare Bitcoin.

Così come il mercato delle tecnologie IT ha sviluppato offerte in grado di soddisfare l'utente finale secondo tutte le sue necessità allo stesso modo anche il Dark Web ha sviluppato pacchetti omnicomprensivi per aspiranti truffatori. In particolare, questo è stato osservato nel mercato della falsificazione di documenti ufficiali. Sono stati creati veri e propri template Photoshop – completi di dettagliate istruzioni per l'uso – che coprono tutto il ventaglio dei documenti: carte d'identità, patenti, passaporti, bollette, fatture… Questi template sono usati in combinazione con i cosiddetti "Fullz", termine proprio dello slang degli hacker, che indica il pacchetto completo dei dettagli personali (nome, codice fiscale, data di nascita, numero di conto corrente bancario…) sottratti alla vittima di furto d'informazioni e ugualmente disponibili sul Dark web. Il risultato dell'unione di questi dati con i template (venduto appunto come soluzione completa) viene usato principalmente per commettere frodi bancarie. Ciò, in breve, è significativo di quanto si sia evoluto questo mercato "underground": il criminale intenzionato a commettere una frode può effettivamente acquisire un pacchetto completo di strumenti e istruzioni per

l’uso atte a questa attività criminale.

Cybercrime commodity: un epidemia in procinto?

Quelli elencati non sono altro che alcuni semplici esempi dell’enorme business che è il cybercrime oggi. Di certo è un’utopia l’augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono portare significativi benefici atti a scongiurare questi attacchi e mantenere la propria sicurezza. Un consiglio è quello di utilizzare, laddove possibile, un sistema autenticazione a due fattori, che assicura un’ulteriore barriera di protezione anche nel caso in cui venga sottratta la password. Un altro facile accorgimento riguarda l’igiene delle password: una sicura non deve essere scontata, non deve richiamare al tuo nome/data di nascita o a quello dei tuoi cari, non deve essere eccessivamente corta e deve includere caratteri speciali. Il cambio di paradigma necessario per assicurarsi maggiore protezione non è solo tecnico, ma anche culturale: lo sforzo combinato deve avere luogo lungo tutta la filiera digitale per educare ed educarsi sull’importanza della sicurezza online è la vera strada per rendere inefficaci, se non solo per gli hacker più esperti, tutti gli strumenti che pullulano sulle piattaforme presenti nel Dark web.

La battaglia deve essere combattuta su due fronti: tecnico e culturale. Si è reso imperativo l’acquisto di skill, anche basilari, per affrontare le criticità della cybersecurity. Una buona strada per raggiungere questo obiettivo è quella di intraprendere corsi di formazione. Il mercato ha, fortunatamente risposto a questa necessità ed è oggi possibile prendere parte a corsi tailor made per ogni tipo di livello richiesto, dalle basi di Cybersecurity awareness a sessioni su argomenti più avanzati come l’Ethical Hacking.

Sul lato più “company”, uno dei migliori metodi, per business e provider di servizi web, di comprendere a quali rischi possono essere soggetti i propri domini, app, etc… è quello di eseguire un Vulnerability Assessment test: si tratta di un’analisi di sicurezza effettuata per identificare tutte le vulnerabilità potenziali di sistemi, pagine web, network e applicazioni. Come fare per effettuarne uno? Sono disponibili molti strumenti automatizzati.

Questi tools effettuano controlli approfonditi su ogni sistema o applicazione e riconoscono le vulnerabilità presenti. Un altro aspetto importante da considerare è la velocità di scansione. La celerità di questi tool rende possibile la scansione di un perimetro molto ampio in un periodo di tempo relativamente breve, fornendo, inoltre, un buon livello di dettaglio, questo per garantire la massima efficienza nell’intervenire e correggere eventuali falle di cybersecurity presenti nel sistema.

https://www.key4biz.it/cybercrime-cosa-si-vende-nel-dark-web/255313/

Backup dei dati: lo fa solo il 18% delle persone, la metà di noi archivia la propria vita nei device

Si parla ormai in maniera sempre più diffusa e dettagliata di cosa sia una minaccia informatica e di quanto è fondamentale proteggere i nostri apparecchi elettronici e i nostri dati, ma ancora poco di tecniche e di best practice.

Ad esempio, è più importante istallare un buon antivirus o magari fare periodicamente un back up dei dati contenuti nei nostri device? Magari è bene fare entrambe le cose, ma appare evidente che mentre un antivirus lo compriamo prima o poi, molta meno attenzione rivolgiamo alla pratica del backup.

Nonostante numerosi studi statistici hanno dimostrato, nel tempo, che ogni minuto 113 telefoni cellulari vengono persi o rubati, per un totale di oltre 162,000 unità al giorno, con l'84% degli intervistati che dichiara di aver perso i propri dati almeno una volta nella vita, ancora oggi, secondo un nuovo studio Kingston Technology Europe, **il 55% dei rispondenti afferma di effettuare il backup dei propri dispositivi solo quando capita**, mentre **il 13% non sa nemmeno cosa sia**.
Per fortuna, si evidenzia nel documento, **il 18% dichiara di eseguire il backup almeno una volta al mese**.

Dal sondaggio emerge che episodi in realtà frequenti come attacchi hacker, smarrimento e manomissione di dispositivi, vengono percepiti come poco probabili, mentre le cause di perdite dati più verosimili sono attribuite a fattori quali furto e malfunzionamento dell'hardware.

Backup, questo sconosciuto, in pochi lo conoscono e sempre in pochi, nel caso sanno più o meno cosa sia, hanno in mente cosa si deve fare: il 41% si affida al proprio intuito; il 25% prova a portare a termine l'operazione, ma senza garanzie sul risultato; **il 19% non saprebbe nemmeno da dove iniziare; solo il 15% eseguirebbe un backup ad occhi chiusi.**

Altro dato su cui riflettere leggendo il Report Kingston, soprattutto alle luce di questi ultimi risultati è che **il 47% delle persone afferma che all'interno dei propri device è custodita praticamente tutta la propria vita** (tra cui ricordi,

agenda, contatti, password, dati sensibili, documenti di varia natura).

Nello specifico, il 39% dichiara che perdere i dati contenuti nei dispositivi mobili sarebbe "*la fine del mondo*", il 35% riconosce nel misfatto un problema, ma comunque risolvibile, dopo il disagio iniziale, mentre il 25% afferma che se si dovesse svegliare la mattina e scoprire che i propri device sono completamente vuoti, "*andrebbe totalmente nel panico*".

Tra i dati a cui più teniamo e che proprio non vorremmo perdere: fotografie e video si posizionano al primo posto (61%), seguiti da password e accessi ai vari siti e account (17%), documenti vari (14%) e contatti della rubrica (8%).

> *Backup dei dati: lo fa solo il 18% delle persone, la metà di noi archivia la propria vita nei device*

Cybercrime, quali sono le tecniche d'attacco alla luce del Clusit 2019

Nello scorso anno il 95% dei cyberattacks è durato meno di 3 ore, ma di essi il 2% si è protratto oltre le 24 ore consecutive, come riportato dal Rapporto **Clusit** 2019.

Importante allora è la **Cyber resilience**, cioè la "*capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso*", spesso nelle situazioni di **Zero-day attach** cioè un "*attacco compiuto sfruttando vulnerabilità non ancora*

note/risolte”.

Altro dato importante è valorizzare e comprendere la COMPONENTE UMANA (come accade nei malware dove il maggior impatto è dato dal*Man-in-the-browser*).

Ancora, molto sviluppata è la **Social engineering** che è la “*tecnica di attacco basata sulla raccolta di informazioni mediante studio/interazione con una persona*”.

Infatti la “***User Behavior Analytics (UBA)*** *o analisi comportamentale dell’utente, aggiunge un ulteriore elemento per il calcolo del valore di rischio della singola transazione, e mira ad individuare prontamente le azioni dei cyber criminali che cercano di impersonificare la vittima, autenticandosi con le sue credenziali. Lo fa analizzando una grande quantità di dati e informazioni sul comportamento online dell’utente, generati dai sistemi e dalla rete, e finora ignorati. Questi elementi, disponibili già oggi, consentono di aggiungere contesto all’utente e al dispositivo usato nella transazione, e contribuire a misurare in maniera accurata il livello di rischio di ciascuna operazione*”.

Compartecipazione della vittima

L’elemento che ha contribuito al successo delle principali campagne di malware dell’anno è stata la compartecipazione della vittima, che spesso ha aperto ed eseguito gli allegati malevoli ricevuti via mail. Questo nella noncuranza delle più elementari norme di precauzione, e dei messaggi di avvertimento generati dalle versioni più recenti dei prodotti di produttività, come Office.

Il fenomeno è più grave di quanto si possa immaginare. All’atto pratico, non solo la vittima ha aperto per curiosità

una mail che nella maggior parte dei casi non attendeva, ma si è anche fidato delle informazioni fallaci che ha visto a schermo, ed ha collaborato attivamente con l'attaccante abilitando l'esecuzione delle macro all'interno dei documenti o dei file.

Anno nuovo, modus operandi nuovo (webinject)

Una nuova tattica è emersa nella seconda parte del 2018. In almeno due campagne studiate da **IBM Security,** i malware sono stati usati per seguire e osservare le attività online della vittima senza alcun intervento, lasciandogli effettuare il login e la navigazione all'interno del sito bancario, intervenendo però con webinject al momento dell'effettiva operazione dispositiva, sostituendo le coordinate bancarie del beneficiario.

I webinject permettono di alterare ciò che viene visualizzato all'interno del browser. In questo modus operandi i **webinject** mostrano a video le coordinate bancarie del destinatario, ma all'invio della transazione passano al sito bancario altre coordinate bancarie. La frode diventa trasparente nei confronti della banca, e difficile da individuare per l'utente non attento. La vittima inserisce anche il secondo fattore di autenticazione (solitamente inviato via SMS), e riceve poi segnalazione della avvenuta transazione con l'importo effettivamente immesso, che vede tra le operazioni effettuate. Quello che un occhio attento non nota però è che le coordinate del beneficiario sono state sostituite con altre coordinate di pagamento, spesso appartenenti ad un money mule, oppure a conti controllati dagli attaccanti e usati per far transitare le somme

Email security

Circa il 10% delle mail contiene un link, il link malevolo resta un efficace sistema di attacco, in crescita rispetto all'anno precedente. Rispetto all'invio del malware in allegato offre maggiori possibilità di evasione dei sistemi di email security, soprattutto quando la mail è inviata da un account legittimo (abusato) e il link punta ad un sito legittimo che è appena stato compromesso.

Tecniche di attacco utilizzate

È utile riportare le tecniche di attacco più comuni:

- **DOS (Distributed Denial of Service)**

Un attacco **DoS (Denial of Service)** è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio.

DNS Reflector attack è un attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive) inviando a questi ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza (IP spoofing).

- **I servizi VOIP (Voice Over Internet Protocol)**

I VOIP rappresentano una modalità di trasmissione di voce e traffico multimediale su reti IP dove **le comunicazioni vocali vengono convertite, pacchettizzate e trasmesse sotto forma di traffico dati**.

Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere dato che può sfruttare le sinergie con la rete dati. D'altra parte questo meccanismo è caratterizzato da possibili **vulnerabilità** (tipiche di una classica rete IP) e può ampliare la superficie d'attacco alla quale le Aziende sono esposte.

Le particolarità e vulnerabilità dello specifico protocollo possono infatti rappresentare un ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di **Social Engineering** e intercettazione fino a possibili interruzioni di servizio **(DoS e DDoS)** e **Service Abuse** (dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale)."

Una blacklist è una lista dove vengono inseriti e catalogati indirizzi IP classificati come fonte di e-mail di SPAM.

Ci sono diversi motivi per cui si può essere inseriti nelle liste nere, di seguito cercheremo di analizzare i principali:

- Invio di e-mail massive dal proprio indirizzo.
    - Nel testo o nell'oggetto delle e-mail inviate sono presenti caratteri e simboli in genere utilizzati nelle mail di SPAM

Il pc è infetto da virus che invia autonomamente e ciclicamente email infette.

- **Il fenomeno del Carding**

Con il termine Carding si identifica principalmente lo scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.

- **Attacchi tramite malware**

Le modalità di attacco da parte dei malware bancari rimane quella di tipo **Man-in-the-browser**, mediante **injection** di codice malevolo all'interno delle pagine web dei portali di **home banking**. La **web injection** può essere effettuata sulla pagina di login, allo scopo di rubare le credenziali di accesso al portale.

Quando l’utente visita l’home banking della propria banca il malware si attiva e resta in attesa che l’utente si posizioni nella pagina di login o di esecuzione dei bonifici. Appena il malware riesce ad entrare in possesso di una sessione valida tra il cliente e il portale della banca allora inizia la procedura per eseguire una frode mediante due possibili tecniche. In un primo caso il bonifico viene fatto partire in maniera automatizzata e in modo trasparente all’utente non appena quest’ultimo esegue il login sul portale della banca; di solito il bonifico necessita di un codice OTP per poter essere inviato quindi il malware richiede, mediante una tecnica di socia engineering, un secondo codice OTP durante la procedura di autenticazione.

Nel secondo caso l’operazione di bonifico iniziata da un cliente della banca viene intercettata dal malware e il destinatario viene modificato prima di inviare la richiesta al server della banca senza che l’utente se ne renda conto. Il cliente rimane ignaro di quanto accaduto poiché il malware altera la struttura grafica delle sezioni interne del portale della banca per nascondere il bonifico fraudolento, ad esempio nelle pagine di conferma e successivo resoconto delle disposizioni effettuate. In alcuni casi il malware blocca le connessioni al provider di posta elettronica sul computer della vittima e rimuove ogni riferimento a numeri o chat di assistenza sul sito web della banca; in questo modo il malware ha più tempo a disposizione prima che la vittima riesca a contattare la banca per segnalare anomalie e bloccare la transazione fraudolenta.

- **Phishing / Social Engineering**

Tra i **numerosi toolkit di phishing che consentono di realizzare velocemente delle pagine di raccolta delle credenziali** ci sono quelli che emulano un portale di webmail dell’organizzazione a cui viene inviata la mail malevola.

La pagina che richiede le credenziali cerca di apparire come

un portale di webmail dell'organizzazione mostrando in modo dinamico nel titolo il nome del dominio dell'indirizzo email della vittima.

In "altri tipi di phishing viene preso come obiettivo una persona in particolare o un impiegato di una azienda specifica. Tale modalità fa sì che lo **spear phishing** diventi ancora più efficace e quindi pericoloso: **il cybercrime raccoglie informazioni relative alla vittima in modo tale che questa possa essere ingannata**. È infatti molto complesso distinguere un'e-mail di **spear phishing** ben ideata da una normale, per questo è più facile che le vittime cadano nella trappola".

You have new mail waiting

In molti casi analizzati, i malware sono stati **inseriti come allegati all'interno di conversazioni realmente avvenute tra la vittima e un interlocutore noto**. All'atto pratico, la vittima riceve una risposta ad un messaggio già scambiato, oppure un nuovo messaggio da una controparte nota, e il messaggio contiene un allegato malevolo. Questo modus operandi mira ad aumentare la fiducia della vittima nei confronti dell'allegato ricevuto, inducendolo ad aprire il file senza porsi troppe domande.

- Un esempio di mail riconducibile al *phisihing* è quello rappresentato nella figura sottostante. "*Si può notare che la mail prende di mira utenti italiani e, come numerosi casi simili riscontrati durante l'anno in diverse campagne, simula proprio l'invio di notifiche di atti giudiziari.*"

- La mail di phishing può anche non contenere un link ma rimandare a un file allegato, [vedi figura sottostante].

Si tratta di un documento Word (in altri sample vengono utilizzati anche file Excel) che, se aperto, presenta un messaggio di errore e invita l'utente ad attivare l'esecuzione delle macro per poter procedere alla lettura del documento.

Il secondo passaggio è "*l'abilitazione dei contenuti da parte dell'utente comporta l'esecuzione delle macro configurate nel foglio Excel, che subdolamente avvia una connessione a un server remoto compromesso per effettuare il download di un eseguibile. Il file scaricato è il malware vero e proprio che viene eseguito, sempre dalla macro e attraverso l'uso di PowerShell, sull'host ormai infetto*."

- "***Numerosi casi relativi alle campagne osservate*** *durante l'anno appena trascorso e aventi come obiettivo solo l'Italia,* ***erano veicolati via PEC*** *e cioè un canale normalmente considerato affidabile*".

In tal senso una campagna di phishing particolarmente strutturata si è sviluppata nella prima metà dell'anno, provando a ingannare l'utente con un riferimento ad un finto rimborso INPS. La campagna era organizzata in modo da raccogliere prima i dati personali dell'utente vittima – codice fiscale e numero di telefono, [VEDI FIGURA sottostante] – e successivamente invitando l'utente a selezionare la propria banca – tramite cui ottenere il rimborso, [VEDI FIGURA sottostante] – prima di reindirizzarlo al finto sito web dei numerosi istituti bancari coinvolti per il furto vero e proprio delle credenziali di login.

- **PowerShell di Windows**

È il metodo di attacco con cui iniettare il malware all'interno di processi Windows in esecuzione in memoria e senza la necessità di scaricare file in locale, evadendo molti degli antivirus.

Applicazioni infette negli app store

Usare solo app scaricate da store ufficiali è certamente una pratica virtuosa, ma non risolve del tutto il problema.

BankBot è un malware Android, inserito all'interno di applicazioni apparentemente legittime, e con capacità di controllare lo schermo attraverso overlay. Il malware rimane silente all'interno dell'applicazione infetta fino a che l'utente non lancia sullo smartphone una delle app per accedere ai servizi di banking. A questo punto BankBot, prende il controllo dello schermo per catturare le credenziali utente.

Ma come fa il malware a finire su Play Store, raggirando i controlli di sicurezza? L'analisi

delle app infette con BankBot ha accertato che tutto comincia con una applicazione benigna, nei casi analizzati un'app contenente video comici o tutorial di cucito, caricata sul Play Store. Dopo che un certo numero di utilizzatori hanno scaricato e installato l'app, si invia un aggiornamento che istruisce l'app a scaricare altro codice, questa volta contenente il malware, attraverso una connessione HTTP

diretta, dall’app a un server Internet predisposto.”

Furto di credenziali di piattaforme a supporto delle cripto-valute

Ormai tutti i principali malware, parallelamente agli obiettivi bancari, implementano tattiche per il furto di cripto-valuta.

Soluzioni per la Cyber Security

È indubbio che qualsiasi siano le soluzioni messe in campo dai fornitori di servizi finanziari, queste devono essere supportate da continua osservazione e ricerca dell’evoluzione delle tattiche di attacco. In un contesto mutevole come quello descritto, una soluzione non supportata da team di ricerca specializzati nell’analisi del malware, rischia di divenire presto obsoleta e inefficacie. Le soluzioni adottate devono altresì essere in grado di continue riconfigurazioni sulla base delle mutate forme di attacco. Ad esempio un SIEM deve adesso poter individuare utilizzi malevoli della PowerShell.

Indubbiamente, anche l’intelligenza artificiale e le capacità cognitive inserite all’interno delle singole soluzioni, saranno leve importanti nel campo della lotta al cybercrime nel settore finanziario.

L’uso dell’intelligenza artificiale nelle soluzioni di sicurezza offerte sul mercato si sta orientando su tre macro aree. Anzitutto nell’analisi predittiva con sistemi in grado di identificare autonomamente nuove frodi.

Su questo aspetto vede essere sviluppata l’area della *Intelligence Consolidation*, “che sfrutta le capacità di interpretazione del linguaggio naturale, analizzando e apprendendo dall’enorme quantità di informazioni, per lo più in forma non strutturata e prodotte continuamente nel campo

della sicurezza.

Molto utile la ***“Security bulletins”*** cioè “report, grafici, conferenze, notizie di agenzia, tweet, advisories e altre fonti, che altrimenti rischierebbero di finire ignorate in quanto non fruibili dalle soluzioni di sicurezza finora usate.”

Infine, l’Intelligenza Artificiale si pone come *trusted advisor* a supporto del lavoro degli analisti umani, per una più veloce risposta alle minacce e agli attacchi.

Non quindi una tecnologia che sostituisce il security analyst, ma piuttosto una tecnologia a supporto del security analyst, di cui incrementa sensibilmente la produttività.

Sviluppo di un sistema di *cyber threat intelligence*

L’attività di **CTI** è usualmente espletata da specifiche unità in seno a **CERT** (Computer Emergency Response Teams) o **CSIRT** (Computer Security Incident Response Teams). Uno scenario maturo prevede la gestione, suddivisa e coordinata, di attività tattiche di CTI e attività strategiche di CTI all’interno di un’unica struttura preposta.

Fondamentale il ruolo dei Security Operation Center (SOC) e di tutte le figure che in essi operano, come i Security Analyst, i Security Manager e i Network Specialist. A queste figure, con ruoli diversi, sono demandati i compiti controllo e investigazione sulle minacce, attacchi e vulnerabilità che colpiscono l’organizzazione, la sua infrastruttura, le applicazioni e i dati.

In questo contesto una piattaforma di **Threat Intelligence** è lo strumento fondamentaleper l’investigazione degli eventi di sicurezza, consentendo di verificare e confrontare allarmi, log, file binari, con una fonte autorevole e aggiornata, con

lo scopo di confermare o escludere una potenziale minaccia.

Inoltre la piattaforma di **Threat Intelligence** permette la condivisione di informazioni tra membri dello stesso team, oppure all'interno di team estesi accomunati dalla stessa necessità investigativa.

Per l'analisi tecnica di possibili *intrusions*, è utile l'impiego di **framework** strutturati come la **cyber kill chain (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions)** e il **diamond model (Adversary, Infrastructure, Victim, Capability)**.

Per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere è efficace l'utilizzo della *course of action matrix* (composta da due azioni passive – **Discover** e**Detect** – e cinque attive – **Deny, Disrupt, Degrade, Deceive, Destroy**).

Per approfondire

https://www.key4biz.it/cybercrime-quali-sono-le-tecniche-dattacco-alla-luce-del-clusit-2019/255031/

Data breach, quasi la metà delle aziende non si è adeguata al GDPR. Ecco perché vittime di attacchi

IBM Security ha annunciato i risultati di uno studio globale che esplora la preparazione delle aziende in relazione alla loro capacità di resistere e ripristinare l'operatività in

seguito a un attacco cyber.

Condotto dal **Ponemon Institute** e sponsorizzato da **IBM Resilient**, *“2019 Cyber Resilient Organization”* è lo studio annuale sulla resilienza informatica, arrivato alla quarta edizione, che evidenzia la capacità di una azienda di mantenere il proprio scopo primario e la propria integrità alla luce di un attacco informatico.

Il sondaggio è stato condotto a livello globale e riporta le opinioni raccolte da più di 3600 professionisti della sicurezza e dell’IT di tutto il mondo, ha evidenziato come il 77% degli intervistati ha affermato di non avere un piano di risposta agli incidenti di cybersecurity applicato in maniera consistente in tutta l’azienda.

Investire nella sicurezza porta ricchezza

Mentre gli studi mostrano che le compagnie in grado di rispondere in modo rapido ed efficace, contenendo un cyber attacco in 30 giorni, risparmiano in media **oltre 1 milione di dollari** sul costo totale di un data breach, la mancanza di piani di risposta a incidenti di cybersecurity è rimasta costante nell’arco dei quattro anni su cui si è protratto lo studio.

Delle aziende che hanno invece un piano in essere, più della metà (54%) non li testa regolarmente, trovandosi meno preparate a gestire efficacemente i complessi processi e la coordinazione necessari qualora vi sia un attacco.

“*Non pianificare è un piano per fallire rispetto alla necessità di rispondere a un incidente di cybersecurity. I piani di risposta agli incidenti devono essere testati*

regolarmente e necessitano il pieno supporto del board per investire nelle persone, nei processi e nelle tecnologie necessarie al mantenimento di tale programma," afferma **Ted Julian**, VP del Product Management e Co-Founder di IBM Resilient. "*Quando una pianificazione adeguata è affiancata da investimenti nell'automazione, vediamo aziende in grado di risparmiare milioni di dollari durante unattacco*".

L'importanza del GDPR

La prolungata difficoltà che i team di cybersecurity stanno affrontando nell'implementazione di piani di risposta a incidenti di cybersecurity ha impattato la conformità delle imprese alla **General Data Protection Regulation (GDPR**). Quasi metà degli intervistati (46%) afferma che la propria azienda deve ancora arrivare a una totale ottemperanza del GDPR, persino a un anno dall'anniversario dell'entrata in vigore della legge.

La privacy sempre più prioritaria

Le aziende stanno finalmente riconoscendo che la collaborazione tra privacy e sicurezza informatica migliora la resilienza digitale, con il 62%, che ritengono essenziale l'allineamento dei rispettivi team. La maggior parte degli intervistati crede che il ruolo della privacy stia diventato sempre più importante, specialmente con l'emergere di nuove leggi come il GDPR o il California Consumer Privacy Act, e stanno dando priorità alla protezione dei dati nelle decisioni d'acquisto per l'IT.

Quando richiesto quale fosse il maggior fattore nella giustificazione delle spese per la sicurezza informatica, il 56% delle risposte si concentrava su perdita o furto di informazioni.

Questo risulta particolarmente vero, con i consumatori che

richiedono alle aziende di essere maggiormente proattive nella protezione dei propri dati. Secondo una recente ricerca di IBM, il 78% degli intervistati dice che l'abilità di una organizzazione nel proteggere i dati è estremamente importante, con solo il 20% che ha piena fiducia nelle aziende con cui interagisce riguardo il mantenimento della privacy dei propri dati.

In aggiunta, la maggior parte dei partecipanti ha riportato la presenza di un privacy leader in azienda, con il 73% che dice di avere un **Chief Privacy Officer,** provando ulteriormente come la privacy sia diventata una importante priorità per le aziende.

L'automazione è un'area emergente

Per la prima volta, lo studio di quest'anno ha misurato l'impatto dell'automazione sulla resilienza informatica. Nel contesto della ricerca, con automazione si intendono quelle tecnologie di sicurezza che permettono di aumentare o sostituire l'intervento umano nell'identificazione e contenimento di cyber exploit o breach. Queste tecnologie si basano su intelligenza artificiale, machine learning, analytics e orchestrazione.

Quando è stato chiesto se le proprie aziende facessero uso dell'automazione, solo il 23% ha risposto indicando un uso significativo, mentre il 77% ha detto che ne fa un uso moderato, insignificante o nessuno. Le aziende con uso estensivo dell'automazione stimano la propria abilità a prevenire (69% vs 53%), rilevare (76% vs 53%), rispondere (68% vs 53%) e contenere (74% vs 49%) più alta del campione totale di rispondenti.

Lo scarso utilizzo di sistemi automatizzati è un'opportunità mancata per rinforzare la resilienza informatica: infatti, secondo lo Studio sul costo di un Data Breach del 2018, le aziende che implementano l'automazione nei meccanismi di

sicurezza risparmiano 1,55 milioni di dollari sul costo totale di un data breach, contrariamente a quanto accade a quelle che non ne fanno uso e che totalizzano un costo molto maggiore per lo stesso tipo di evento.

Lo skills gap impatta ancora la resilienza informatica

Lo skill gap nella cybersecurity sta ulteriormente indebolendo la resilienza informatica, con aziende a corto di personale e impossibilitate a gestire appropriatamente risorse e necessità. I partecipanti al sondaggio hanno riferito che non dispongono del numero di persone necessarie al corretto mantenimento e test dei propri piani di risposta agli incidenti e che stanno fronteggiando tra le 10 e 20 posizioni scoperte nei propri team di sicurezza. Solo il 30% dei partecipanti ha riportato che il personale per la sicurezza informatica è sufficiente per ottenere un alto livello di resilienza informatica. Inoltre, il 75% degli intervistati ha valutato la propria difficoltà nelle assunzioni e nel mantenimento del personale competente per la sicurezza informatica tra moderatamente alta a alta.

In aggiunta al gap di competenze, quasi la metà dei partecipanti (48%) ha ammesso che le proprie aziende ricorrono a troppi strumenti e soluzioni per la sicurezza, causando una maggiore complessità e riducendo la visione d'insieme sui sistemi di sicurezza.

Per scaricare lo Studio "The 2019 Study on the Cyber Resilient Organization" clicca qui.

https://www.key4biz.it/data-breach-quasi-la-meta-delle-aziende-non-si-e-adeguata-al-gdpr-ecco-perche-vittime-di-attacchi/254066/

5G, Gabrielli: “Su protezione infrastrutture critiche non siamo al giurassico, ma non molto lontano”

“Sul tema della protezione delle infrastrutture critiche non siamo al giurassico, ma non molto lontano: si tratta di una questione fondamentale per la vita del Paese che purtroppo non sempre è stata vissuta come prioritaria”. L’allarme è stato lanciato dal capo della Polizia, **Franco Gabrielli**, intervenendo al convegno su “*Sicurezza nazionale e cooperazione internazionale*” organizzato, ieri, nell’ambito del Salone della Giustizia.

Nella Pa a tutti i livelli c’è analfabetismo su sicurezza delle infrastrutture critiche

“Nel mondo della pubblica amministrazione a tutti i livelli c’è ancora analfabetismo sotto il profilo della sicurezza delle infrastrutture critiche – ha spiegato il capo della Polizia – *e già solo farne un elenco potrebbe rappresentare un problema. Su questi temi servono visione, condivisione, forte partnership tra pubblico e privato: e la difesa dell’interesse nazionale non può essere considerata autarchia, chiusura al mondo o negazione di vecchie e nuove relazioni”.*

Partnership pubblico-privato per fronteggiare gli attacchi informatici e proteggere le infrastrutture critiche

La partnership tra pubblico e privato per fronteggiare gli attacchi informatici e proteggere le infrastrutture critiche è la strategia indicata anche dal ministero della Difesa: *"Lo Stato è un attore fondamentale per la sicurezza, anche in quella cibernetica, ma devono partecipare anche gli utenti e le grandi realtà, quelle che gestiscono le reti e producono i software: sono private ma hanno un grande impatto sulla collettività e devono partecipare per tutelare il bene comune",* ha detto il ministro **Elisabetta Trenta** intervenuta al **Cnr** di Pisa nel corso di **Itasec19**. Stesso concetto ripetuto dal sottosegretario alla Difesa presso l'Ambasciata italiana a Washington: *"Il Governo non può proteggere il dominio cibernetico da solo, abbiamo bisogno di rafforzare le partnership pubblico-privato. Dobbiamo lavorare con i principali stakeholder",* ha dichiarato **Angelo Tofalo** nel suo recente intervento negli Stati Uniti.

"Con il 5G no approccio settoriale"

Il **5G** non è solo la tecnologia successiva al **4G**, è un ecosistema di trasformazione abilitante per tante altre tecnologie: a partire dall'IoT fino all'Intelligenza artificiale. Tutto sarà, a regime, connesso con innumerevoli vantaggi e nuovi servizi in una pluralità di settori, ma con la tecnologia di quinta generazione le minacce cibernetiche *"sono destinate a crescere esponenzialmente",* ha fatto notare il Garante Privacy, **Antonello Soro**, nell'audizione al **Copasir**.

Per questo motivo Franco Gabrielli ha lanciato l'appello alle aziende pubbliche e private, che rappresentano un'eccellenza nella cybersecurity, a fare squadra: *"Pensiamo al 5G, si dovrà necessariamente capire che le cose saranno profondante modificate. La velocità e la molteplicità delle interconnessioni finiranno inevitabilmente con il cambiare molte cose: saremo sempre più chiamati a navigare in un mare dove i punti di riferimento non sempre saranno cosi definiti. Invece l'approccio è sempre molto settoriale, riferito al momento",* ha osservato il capo della Polizia.

Infine, Gabrielli ha ricordato come *"già dal 2005 l'amministrazione della Polizia abbia riservato alle nuove frontiere del web, ai suoi rischi e ai suoi vantaggi un'attenzione crescente"*, che ha portato tra l'altro alla creazione di una struttura all'avanguardia come il **Cnapic** (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche). "*Sui temi della sicurezza* – ha concluso – *ci deve essere sempre maggiore condivisione tra i cittadini e istituzioni ma la consapevolezza dei rischi non deve essere vissuta, come spesso accade, in un'ottica di paura o di preoccupazione, ma di fiducia nelle opportunità offerte da una tecnologia sempre più spinta e sempre più capace di modellare le nostre vite. La consapevolezza è una precondizione per avviare a soluzione i problemi: bisogna evitare che di fronte alle straordinarie opportunità offerte dalla rete prevalga una mentalità eccessivamente difensiva".*

Cosa fa il Cnapic?

- Il C.N.A.I.P.I.C. è incaricato in via esclusiva della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura

critica e di rilevanza nazionale. Il valore aggiunto che il Centro rappresenta, nel panorama della protezione delle Infrastrutture Critiche deriva:

- Dalla realizzazione di una Sala operativa, disponibile 24 ore su 24 e 7 giorni su 7, in qualità di Punto di contatto univoco dedicato sia alle I.C., sia ad ogni altro attore, anche a livello internazionale, impegnato nella protezione delle I.C.;
- Dai collegamenti telematici esclusivi, dedicati e protetti, tra il C.N.A.I.P.I.C. e le I.C., per il condiviso, reciproco e costante trasferimento dei dati e delle informazioni utili all'esercizio delle funzioni di valutazione, prevenzione e repressione delle minacce e dei crimini informatici.
- Si avvale di tecnologie di elevato livello e di personale altamente qualificato, specializzato nel contrasto del cybercrime, che ha maturato concreta esperienza anche nei settori del c.d. cyberterrorismo e dello spionaggio industriale.

https://www.key4biz.it/5g-gabrielli-su-protezione-infrastrutture-critiche-non-siamo-al-giurassico-ma-non-molto-lontano/254084/