Bitcoin e criptovalute, nel 2021 sempre più utilizzate per chiedere riscatti. Il trend

La recente risalita dei Bitcoin è una notizia che fa felici anche gli hacker. La regina delle criptovalute sarà tra le protagoniste nel traffico economico del cybercrimine nel 2021. Lo rende noto Kaspersky, individuando i principali trend che dovrà affrontare il panorama finanziario nel prossimo anno.

Criptovalute: bitcoin e monero al top nel 2021

Oltre i bitcoin, secondo i ricercatori di sicurezza, nel 2021 aumenteranno altri metodi di scambio di denaro digitale, con la crescita di quelli che promettono ancora maggior privacy. Le estorsioni ai danni degli utenti punteranno proprio a questo: ricatti e pagamenti ancora tramite Bitcoin ma con il consolidamento di piattaforme, come **Monero**, che consentono una maggiore tutela dell'anonimato, con conseguente difficoltà nel rintracciare il passaggio tra i portafogli.

Il furto stesso di **Bitcoin** diventerà ancora più presente quando molte nazioni rischieranno la povertà a causa della pandemia. Con il crollo delle economie e il calo delle valute locali, un numero maggiore di persone potrebbe interessarsi al mondo della criminalità informatica, con un conseguente aumento dei casi. Grazie al successo delle loro operazioni, i responsabili degli attacchi ransomware alzeranno le somme di denaro richieste alle vittime, con la promessa di non

pubblicare le informazioni rubate.

Bitrail: identificato in Italia il responsabile della ‘buco’ di 120 milioni di euro

Lo scorso 21 dicembre la Polizia Postale ha identificato l’autore del “più grande attacco cyberfinanziario in Italia, uno dei più grandi mai realizzati nel mondo nel settore delle criptovalute”: si tratta di un fiorentino di 34 anni responsabile di un “buco” pari a 120 milioni di euro sulla piattaforma informatica hackerata Bitgrail. Oltre 230 mila risparmiatori truffati.

L’uomo è accusato di frode informatica, auto-riciclaggio e bancarotta fraudolenta. La polizia postale italiana ha posto così *“una pietra miliare a livello mondiale nel settore delle indagini sulle criptovalute, con un’indagine unica nel suo genere ad alto impatto tecnologico”.*

“Per la prima volta in Italia e in Europa – ha sottolineato la polizia postale – *si sono documentate condotte fraudolente e distrattive in danno di investitori, poste in essere integralmente su piattaforme informatiche e l’impiego di monete virtuali”.*

https://www.key4biz.it/bitcoin-e-criptovalute-nel-2021-sempre-piu-utilizzate-per-chiedere-riscatti-il-trend/336760/

Cybercrime, deepfake e

fattore umano le principali minacce per le aziende

Il 2021 sarà per la sicurezza informatica un anno pieno di insidie. La pandemia ha determinato una drastica accelerazione delle iniziative digitali in tutti i settori di mercato in quanto le aziende hanno dovuto adottare rapidamente tecnologie a supporto della produttività e della continuità del business.

Sia che si trattasse di portare nuovi strumenti di collaborazione o di spostare infrastrutture e applicazioni critiche nel cloud, tutto è diventato più distribuito, aumentando notevolmente, di conseguenza, le opportunità per i potenziali aggressori.

Che impatto avrà la convergenza di queste forze ed eventi sulla sicurezza informatica nei prossimi 12 mesi? Eccone due particolarmente importanti: deepfake e dipendenti.

I deepfake diventano una minaccia anche per le aziende

Qualcosa può essere troppo enfatizzato e rappresentare comunque una minaccia emergente? Questo è il caso dei deepfake – un termine che è simulatamene abusato e un esempio di come gli attaccanti continueranno a personalizzare i loro attacchi.

In sintesi, i deepfake sono video o immagini, sintetici o manipolati, in cui una persona viene sostituita con la somiglianza di qualcun altro. Da un punto di vista culturale, il concetto di deepfake ha dominato i notiziari come una potenziale minaccia che potrebbe influenzare l’opinione

pubblica, danneggiare la reputazione e altro ancora. Spesso questi attacchi fanno notizia, ma finiscono per essere relativamente poco efficaci.

Tuttavia, man mano che la tendenza della catena di attacchi personalizzati continua, vedremo l'emergere di deepfake negli attacchi alle imprese – non per seminare necessariamente confusione o caos di massa, ma più per amplificare gli attacchi di ingegneria sociale.

Video e registrazioni di dirigenti sono spesso già disponibili per attività di marketing, social media e altro ancora. Gli attaccanti potrebbero inserire deepfake in tentativi di phishing (che si allontaneranno dalla posta elettronica per sfruttare altre piattaforme come le applicazioni di chat e collaborazione) per rendere le comunicazioni manipolate ancora più autentiche. Soprattutto al giorno d'oggi, dove sempre più organizzazioni si affidano al video come mezzo di comunicazione tra dirigenti e dipendenti, gli aggressori possono approfittare di questo livello di fiducia instillato.

Sono comuni, ad esempio, le e-mail di phishing che chiedono le password – ma cosa succederebbe se a quell'e-mail seguisse un messaggio urgente del CEO su WhatsApp? Gli attaccanti potrebbero anche utilizzare video manipolati di dirigenti sui social per invogliare clienti, dipendenti, partner e altro ancora a cliccare su link dannosi – creando nuove vie di attacco più ampie per gli attori dannosi.

I dipendenti

La pandemia ha creato un'enorme tensione sui dipendenti e sulle loro famiglie. L'incertezza economica e il passaggio al lavoro e alla scuola a distanza ha messo molti in un territorio inesplorato. Queste nuove sfide potrebbero probabilmente spingere un numero maggiore di dipendenti a prendere decisioni sbagliate quando si tratta di sicurezza informatica e creare una nuova ondata di insider

malintenzionati.

Come abbiamo già osservato nel 2020, gli attaccanti offrono sempre più spesso ai dipendenti con accesso privilegiato incentivi finanziari allettanti per condividere o "accidentalmente" far trapelare le proprie credenziali. Inoltre, l'accesso privilegiato sul dark web è più popolare che mai, e alcune ricerche indicano che gli aggressori sono disposti a pagare per ottenere l'accesso privilegiato alle reti aziendali, alle VPN e alle workstation.

La potenziale ricompensa finanziaria, combinata con l'aumento dell'ansia economica, porterà alla nascita di nuove minacce che le organizzazioni faticheranno a fronteggiare.

https://www.key4biz.it/cybercrime-deepfake-e-fattore-umano-le-principali-minacce-per-le-aziende/336238/

Cybersecurity, i principali trend per il 2021

Con la diffusione della pandemia di Coronavirus si è visto un incremento dell'attività dei criminali informatici in tutto il mondo. In modo particolare FBI, Europol e società di intelligence hanno visto un particolare aumento della diffusione di attacchi ransomware, programmi malevoli che possono *"infettare"* un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".

Ma cosa succederà l'anno prossimo e come sarà necessario modificare le strategie aziendali man mano che il panorama delle minacce continuerà a evolvere? I ricercatori di sicurezza di **Proofpoint**, cercano di rispondere analizzando i principali trend previsti per il 2021.

Ransomware

Il ransomware rimane la principale fonte di preoccupazione per i CISO. Come consolidata macchina da soldi per i cybercriminali, era solo una questione di tempo prima che i suoi principali creatori arrivassero a sviluppare nuovi metodi di estorsione, in particolare con la minaccia di diffondere le informazioni rubate. Nel 2021, in seguito alla rapida accelerazione dell'adozione del cloud guidata dalla pandemia COVID-19, ci aspettiamo che anche gli attacchi ransomware si evolvano verso il cloud. Molte aziende ora ospitano porzioni importanti dei loro dati sensibili in repository esterni basati nel cloud, e questi archivi sono spesso meno visibili a chi si occupa di sicurezza – spesso anche non così protetti o sottoposti a backup in modo da essere a prova di cifratura criminale. Nel 2021, i professionisti della sicurezza possono aspettarsi di vedere un numero sempre maggiore di ransomware indirizzati verso lo storage cloud per massimizzare l'impatto e aumentare la leva per incrementare i profitti.

Malware

La stragrande maggioranza dei cyberattacchi inizia via e-mail e praticamente il 100% del malware si basa su un'azione dell'utente per la compromissione iniziale. I cybercriminali hanno ormai ben chiaro che cercare di sfondare in altri modi (ad esempio usando gateway VPN senza patch) è possibile, ma molto più difficile grazie al grande lavoro che i professionisti della sicurezza hanno svolto nel corso degli anni e alla scarsità di vulnerabilità utili nei sistemi aperti

verso Internet. Di conseguenza, gli hacker oggi indirizzano i loro attacchi verso gli utenti più vulnerabili, convincendoli a compiere una qualche azione che comprometta i loro sistemi. Se basta un clic per abilitare le macro, perché lanciarsi nel complicato obiettivo di trovare una vulnerabilità in un sistema operativo o browser moderno?

Ci aspettiamo anche che non ci si sposterà dal "malware fileless" per le attività post-compromissione. Dal punto di vista di un cybercriminale, quale modo migliore per evitare il rilevamento di malware se non utilizzando qualcosa che non sia malware? Ci aspettiamo che gli hacker continuino a sfruttare i LOLBins e i LOLScripts ("Living off the land Binaries/Scripts") per compromettere i sistemi e rubare/danneggiare i dati. È fondamentale che le aziende lavorino per individuare e prevenire l'uso pericoloso di questi LOLBins lavorando per fermare la compromissione iniziale e limitando l'uso di strumenti come PowerShell ovunque sia possibile.

Attacchi BEC

Sono già un problema di massa, ma gli attacchi di business email compromise (BEC) accresceranno il loro peso. Con un costo per le organizzazioni stimato in miliardi di dollari ogni anno, la frode BEC è responsabile della maggior parte delle richieste di risarcimento in tema di cyber-assicurazione e ha una barriera all'ingresso molto bassa, quindi rimarrà una forte attrazione per i cybercriminali. Di conseguenza, gli hacker lavoreranno per aumentare ulteriormente potenziale di guadagno e tasso di successo, compiendo il passo ulteriore di compromettere l'account di un utente per poi fingere di essere legittimi. L'FBI ha già attribuito al BEC la maggior parte delle perdite dovute al cybercrime e, man mano che i responsabili BEC ampliano il loro set di strumenti per compromettere gli account cloud e i fornitori e i venditori delle organizzazioni, fermarli continuerà a essere una sfida

impegnativa.

L’automazione e sicurezza

La carenza di talenti nel campo della cybersecurity è da anni una preoccupazione, con i CISO che lottano per mantenere nel tempo team completi e qualificati. L’unico modo per far sopravvivere le funzioni di sicurezza è automatizzare componenti del loro ruolo – dall’amministrazione degli account (nuovi ingressi, trasferimenti, abbandoni) all’amministrazione del firewall, fino alla creazione di metriche, al triage e agli avvisi del SOC, alle indagini DLP e altro ancora. Fino a oggi, l’automazione è stata in genere affrontata acquistando strumenti o funzionalità aggiuntive dai fornitori. Ci aspettiamo che questa situazione cambierà nel 2021, dato che l’automazione diventerà più che altro una funzione standard “in the box” per la maggior parte degli strumenti di sicurezza enterprise – cosa che molti CISO attendono ormai da tempo.

Gruppi di cybercriminali sempre più forti

I tre canali preferenziali utilizzati dai cybercriminali per il loro profitto sono BEC, EAC (email account compromise) e ransomware. Molti hacker specializzati in BEC ed EAC, tuttavia, non tendono a fungere da intermediari per i team specializzati nel ransomware, anche se dispongono dell’accesso necessario. Analogamente, gli attori di minacce focalizzati sul ransomware non tendono a utilizzare attacchi BEC ed EAC. Ci aspettiamo che questa situazione cambierà nel corso del 2021, quando i vari cybercriminali collaboreranno sempre più per creare attacchi più efficaci e raccogliere maggiori profitti. Ad esempio, potremmo vedere imprese colpite da attacchi EAC, con un accesso viene poi “venduto” a un altro gruppo per inviare ransomware; in alternativa, il gruppo EAC potrà elevare le proprie competenze iniziando a sfruttare

strumenti di ransomware disponibili in commercio. Ci attendiamo anche attacchi BEC ed EAC più avanzati.

Il prossimo anno continuerà certamente a rappresentare una sfida per i responsabili della sicurezza; tuttavia, la possibilità di fare leva su una strategia incentrata sulle persone, che protegge gli utenti attraverso i canali di comunicazione di cui hanno bisogno per lavorare, contribuirà a garantire l'efficacia delle loro contromisure.

Mancano i talenti

La pandemia ha portato a un taglio delle risorse per molte organizzazioni, compresa la spesa per la sicurezza. Speriamo di vedere nel 2021 un ritorno alla "normalità" e questo si rifletterà probabilmente nei budget per la sicurezza che torneranno ai livelli previsti. Il personale responsabile, tuttavia, non è un problema di breve termine. Infatti, i CISO continueranno a lottare per reclutare risorse per i loro team in crescita. L'offerta di posizioni remote e flessibili aiuterà organizzazioni di tutte le dimensioni, ma il problema dell'aumento degli stipendi continuerà. Di conseguenza, molte aziende più piccole e regionali si troveranno a non potersi permettere i talenti di cui hanno effettivamente bisogno, nonostante possano accedere a un bacino ancoro più diversificato costituito da lavoratori completamente remoti.

https://www.key4biz.it/cybersecurity-i-principali-trend-per-il-2021/336234/

Attacco hacker SolarWinds, Italia coinvolta? Riunito il nucleo di sicurezza cibernetica

"L'Italia ha attivato dalle prime fasi della scoperta dell'attacco hacker della piattaforma ***SolarWinds Orion*** *che ha coinvolto i sistemi informatici di enti governativi statunitensi, il* ***Nucleo per la Sicurezza Cibernetica*** *per monitorare un potenziale impatto sulla sicurezza nazionale*".

E' questo l'annuncio dato dall'organismo collegiale italiano a cui è affidato il compito di gestire gli incidenti informatici, guidato dal vicedirettore generale del Dipartimento delle informazioni per la sicurezza (Dis), **Roberto Baldoni**.

Il Nucleo, si legge in una nota del DIS, si è riunito per valutare ogni possibile impatto della campagna di attacchi informatici condotti attraverso la compromissione della piattaforma **SolarWinds Orion** anche sulle reti e sui sistemi nazionali.

L'attacco a SolarWinds: cosa è successo

Lo scorso 13 dicembre i media statunitensi hanno diffuso la notizia del "*più grave attacco informatico da cinque anni a questa parte agli Stati Uniti" che ha coinvolto l'amministrazione Usa.* I cyber attacchi, legati si pensa ai servizi segreti russi con il gruppo APT29 "*Cozy Bear*", hanno

colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale tra cui l'Agenzia per la sicurezza nucleare degli Stati Uniti.

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione. Ma la falla più grave è stata individuata dagli investigatori americaninegli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all'intelligence USA e ai militari.

La backdoor su SolarWinds

Il DIS ricorda che "*il sofisticato attacco introduce una backdoor all'interno della piattaforma SolarWinds attraverso un aggiornamento che permette all'hacker, una volta selezionate le vittime di interesse, di eseguire comandi manuali all'interno dei sistemi della vittima. Ponendo quindi le basi anche per il rilascio di ulteriore codice malevolo volto potenzialmente a spiare o a manomettere ulteriormente i sistemi dell'ente attaccato o dei servizi da esso erogati".*

SolarWinds vanta oltre 300mila clienti, fra cui aziende del calibro di M**icrosoft, Gartner, Mastercard, Mc Donald's, Ing Direct e Volvo**, vendor di sicurezza come **Symantec** e **FireEye**, operatori di telecomunicazione come **Telecom Italia**, **Us Telecom** e **Korea Telecom**.

Sono, inoltre, state avviate tutte le attività di supporto e contatto con i soggetti nazionali preposti a gestire le funzioni ed i servizi essenziali dello Stato (inclusi nel Perimetro di sicurezza nazionale cibernetica), gli operatori di servizi essenziali (previsti dalla Direttiva Europea NIS – Network information System) e gli enti della Pubblica

Amministrazione.

Per il Nucleo di Sicurezza Cibernetica la gravità dell'evento cibernetico e dei suoi effetti resta elevato, per questo il nucleo "*resta in continuo contatto con **"CyCLONe"***, le neo-costituita rete di collegamento europeo, che si propone di agevolare la cooperazione tra le autorità nazionali di cybersecurity in caso di incidenti informatici destabilizzanti.

Il CSIRT

Il Nucleo raccomanda in ogni caso a tutte le organizzazioni che utilizzano la citata piattaforma Orion di **esaminare la problematica con la massima e puntuale attenzione**, avvalendosi a tal fine anche dell'apposita sezione creata sul sito web del CSIRT italiano contenente consigli, aggiornamenti e possibili misure di mitigazione dell'incidente.

https://www.key4biz.it/attacco-hacker-solarwinds-italia-coinvolta-riunito-il-nucleo-di-sicurezza-cibernetica/336708/

Estensioni browser infette da malware, a rischio la sicurezza di milioni di utenti

Il team di ricercatori del *Threat Intelligence* di **Avast** ha

identificato di recente, nascosto in almeno 28 estensioni realizzate da terze parti per i browser **Google Chrome e Microsoft Edge**, un malware con grande capacità di elusione in grado di reindirizzare il traffico di rete verso annunci o siti di phishing e rubare informazioni riservate alle ignare vittime.

Le estensioni e i plug-in dei browser

Per i browser di ultima generazione esiste la possibilità di aggiungere dei componenti che ne consentono la relativa personalizzazione. Si tratta di programmi integrativi che possono essere distinti in plug-in ed add-on. A differenza dei plug-in che sono componenti software che permettono di usufruire di contenuti speciali all'interno delle pagine web visualizzate come filmati, animazioni e presentazioni che il browser non è in grado di gestire, le estensioni sono componenti software che permettono di ampliare le funzionalità, aggiungendo o modificando le caratteristiche dei browser in uso. Si possono trovare estensioni per una miriade di scopi come, ad esempio, aumentare l'accessibilità del browser, gestire download o velocizzare la navigazione e tradurre pagine web.

Gli add-on incriminati

Sebbene sia i plug-in che gli add-on, spesso gratuiti e quasi sempre sviluppati da terze parti, possono essere potenzialmente alterati, senza un adeguato controllo e supervisione, per veicolare software malevolo o propinare servizi illeciti, sono gli add-on per i browser Chrome e Edge le estensioni contaminate oggetto di questa analisi.

Sulla base dei dati raccolti dagli analisti e del numero di download registrati sugli store di Microsoft e di Google

Chrome WEB sarebbero circa tre milioni gli utenti nel mondo ad essere potenzialmente interessati al problema, considerando che queste estensioni malevole sarebbero, per lo più, servizi per note piattaforme social network:

Direct Message for Instagram™, DM for Instagram, Invisible mode for Instagram Direct Message, Downloader for Instagram, Instagram Download Video & Image, App Phone for Instagram, Stories for Instagram, Universal Video Downloader, Video Downloader for FaceBook™, Vimeo™ Video Downloader, Volume Controller, Zoomer for Instagram and FaceBook, VK UnBlock.Works fast, Odnoklassniki UnBlock. Works quickly, Upload photo to Instagram™, Spotify Music Downloader, Upload photo to Instagram™, Pretty Kitty. The Cat Pet, Video Downloader for YouTube, SoundCloud Music Downloader, The New York Times News, Instagram App with Direct Message DM.

Malware e browser: l'attività delle estensioni malevoli

I ricercatori che hanno iniziato a monitorare questa minaccia nel novembre 2020 ritengono che in realtà la campagna possa essere attiva già da diversi anni, grazie all'alta capacità di elusione posseduta dal malware. Dall'analisi dei campioni si è potuto infatti riscontrare che il malware ben nascosto nelle estensioni, resta dormiente per qualche giorno dopo l'installazione e sarebbe anche in grado di rilevare comportamenti di personale esperto nelle attività dell'utente colpito, mantenendo in tal caso la propria inattività.

Il codice dannoso rilevato nelle estensioni basate su javascript consente anche di scaricare ulteriori malware, registrare ed inviare informazioni sui click eseguiti ad un server di comando remoto, effettuare reindirizzamenti URL, geolocalizzare e esfiltrare informazioni sui dispositivi, sistemi operativi e browser usati, consentendo agli attori della minaccia di capitalizzare ogni attività illecita

eseguita.

Come difendersi dai malware

Gli analisti circa l'origine di queste estensioni hanno avanzato diverse ipotesi. Potrebbero essere state create con il malware integrato oppure potrebbero essere state infettate successivamente tramite un aggiornamento nocivo o una iniezione malevola da parte di terzi.

Avast, in ogni caso, ha contattato in modo responsabile i team degli store interessati segnalando l'elenco delle estensioni infette. Anche se Microsoft e Google dopo aver confermato il problema hanno prontamente provveduto a rimuovere gli add-on incriminati, nell'attesa che vengano eventualmente sostituiti resta comunque ancora valida la raccomandazione di disinstallare le estensioni in oggetto, se non ancora fatto, e eseguire quanto prima una bonifica antivirus.

https://www.key4biz.it/estensioni-browser-infette-da-malware-a-rischio-la-sicurezza-di-milioni-di-utenti/336400/

Bitgrail, arrestato l'autore della più grande cybertruffa avvenuta in Italia

Aveva rubato 120 milioni di euro dalla piattaforma informatica "**Bitgrail**", truffando così oltre 230 mila risparmiatori in quello che è stato definitivo il più grande attacco cyber-

finanziario in Italia, uno dei più grandi mai realizzati nel mondo nel settore delle cryptovalute.

La Polizia Postale ha identificato il responsabile: un fiorentino di 34 anni amministratore unico di una società italiana che gestisce una piattaforma di scambio di cryptovalute (exchange), ritenuto responsabile della frode informatica di 120 milioni di euro, di bancarotta fraudolenta e di auto riciclaggio.

La polizia postale italiana pone una pietra miliare a livello mondiale nel settore delle indagini sulle cryptovalute, con un'indagine unica nel suo genere ad alto impatto tecnologico.

Bitgrail: la truffa dei Nano Coin

L'indagine è stata avviata nel febbraio del 2018 dopo la denuncia da parte dell'uomo incriminato del furto di un'ingente somma della cryptovaluta denominata «**NANO**» XRP per un controvalore di circa 120.000.000,00 di euro, realizzato sfruttando un bug del protocollo Nano ed effettuando illecite transazioni, tutte relative a gennaio 2018.

L'indagine ha preso il via nel febbraio del 2018, dopo la denuncia presentata dall'amministratore unico della piattaforma di **exchange**, per il furto di un'ingente somma in criptovaluta "NANO" XRP per un controvalore di circa 120 milioni di euro, realizzato sfruttando un bug del protocollo Nano e compiendo transazioni illecite, tutte relative a gennaio 2018. L'uomo era già noto agli investigatori ai quali forniva Bitcoin per pagare i 'riscatti' delle vittime di criptolocker. Gli inquirenti hanno cominciato a sospettare di lui fin dalle prime battute delle indagini, nonostante collaborasse per non lasciare intendere di essere coinvolto nella vicenda.

La Polizia Postale ed FBI

Le indagini, andate avanti per mesi anche con il supporto dell'FBI, con intercettazioni e complesse attività di analisi informatiche dei database della piattaforma di exchange, hanno portato alla luce le responsabilità dell'uomo e dimostrato che le sottrazioni di criptovaluta sono avvenute in più riprese, a partire da giugno 2017, e che l'uomo consapevolmente non le ha impedite omettendo di implementare la sicurezza della piattaforma con uno dei metodi disponibili resi noti dal Team Nano Developers (Società americana creatrice della criptovaluta), così procurando agli hackers, non ancora individuati, un profitto di circa 11.500.000 XRB, equivalenti a circa 12 milioni di euro, danneggiando più di 230.000 persone in tutto il mondo (peraltro con l'aggravante di aver commesso i fatti con abuso della qualità di operatore del sistema).

https://www.key4biz.it/bitgrail-arrestato-lautore-della-piu-grande-cybertruffa-avvenuta-in-italia/336092/

Nucleare USA sotto cyber attacco, caccia ai mandanti. Biden: "I responsabili pagheranno"

Continuano gli **attacchi informatici** all'amministrazione americana e ad alcune delle sue più rilevanti agenzie

governative, tra cui l'**Agenzia per la sicurezza nucleare degli Stati Uniti**.

La cyber offensiva non si ferma

Joe Biden, fresco di elezioni a 46° Presidente degli Stati Uniti d'America, ha subito annunciato in un comunicato che "*responsabili e mandanti pagheranno un prezzo sostanziale*", secondo quanto riportato dal quotidiano La Repubblica.

Preoccupato, il Presidente ha commentato, in una nota ufficiale, che quanto accaduto: "*sembra assumere sempre più i connotati di un serio tentativo di violazione della sicurezza informatica nazionale su vasta scala, che potenzialmente poteva colpire migliaia di target strategici, comprese società private o legate alla Pubblica Amministrazione ed enti governativi federali*".

Shaylyn Hynes, portavoce del Dipartimento dell'Energia (DoE) degli Stati Uniti, ha garantito che l'attacco non è andato a buon fine, nel senso che gli autori non sono riusciti ad entrare nel sistema per manometterlo o rubare dati sensibili.

Preoccupazione per l'arsenale nucleare

L'attacco però c'è stato, eccome. Il **Dipartimento dell'Energia** e la **National nuclear security Administration** (NnsA), incaricata di gestire l'arsenale nucleare nazionale, si legge su *politico.com*, hanno registrato "*attività informatiche sospette*" nelle reti della **Federal energy regulatory commission** (Ferc), all'interno dei laboratori nazionali Sandia e Los Alamos nel New Mexico e Washington, nell'*Office of Secure Transportation* dell'NnsA e al *Richland Field Office* del DoE.

Tanto per capirci, il laboratorio di Los Alamos è quello dove

è stato portato avanti il “***progetto Manhattan***”, per lo sviluppo del programma atomico americano partito nel 1942. È da questi laboratori che uscirono “*Little Boy*” e “*Fat Man*”, le bombe atomiche che poi furono sganciate rispettivamente su Hiroshima e Nagasaki nel 1945.

Le indagini e i sospetti su Mosca

Su quanto accaduto stanno indagando sia l’**FBI**, sia la **Cisa** (*Cybersecurity and Infrastructure Security Agency*), sia l’Agenzia per la sicurezza nazionale (**Nsa**) e dai primi risultati sembra che i danni principali li abbia subiti la Ferc, la Commissione federale per la regolamentazione dell’energia.

Si suppone che gli hacker abbiano ottenuto l’accesso alle reti delle agenzie federali sfruttando delle **vulnerabilità dei software SolarWinds**, fornitrice di soluzioni IT per centinaia di clienti governativi e del settore privato.

Fin da subito gli inquirenti hanno sospettato il **coinvolgimento di Mosca** in questa vasta cyber offensiva informatica, perché il *modus operandi* sembra molto simile a quello considerato tipico dell’intelligence russa.

Ciò che spaventa di più gli americani (e non solo) è che ad esser preso di mira è stato il cuore nevralgico della sicurezza nazionale, in particolare alcune agenzie governative che più di altre gestiscono direttamente alcune funzioni relative all’arsenale nucleare.

> *Nucleare USA sotto cyber attacco, caccia ai mandanti. Biden: “I responsabili pagheranno”*

Attacco hacker al Governo Usa, le falle di SolarWinds colpiscono 275mila clienti

Emergono tanti retroscena nell'attacco hacker dello scorso 12 dicembre che hai coinvolto l'amministrazione USA nel "*più grave attacco informatico da cinque anni a questa parte agli Stati Uniti*" secondo i media statunitensi.

I cyber attacchi hanno colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale. Dietro a tutto questo, secondo quanto riportato dal **New York Times** e dai media americani c'e la Russia con il gruppo **APT29** "***Cozy Bear***".

Breccia nei sistemi Microsoft e SolarWinds

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione.

Altra falla individuata dagli investigatori americani è negli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all'intelligence USA e ai militari.

SolarWinds vanta oltre 300mila clienti, fra cui aziende del calibro di M**icrosoft, Gartner, Mastercard, Mc Donald's, Ing Direct e Volvo**, vendor di sicurezza come **Symantec** e **FireEye**, operatori di telecomunicazione come **Telecom Italia**, **Us Telecom** e **Korea Telecom**. Cuore dell'offerta di SolarWinds è la piattaforma **Orion**, comprensiva di strumenti di gestione, configurazione e analisi delle reti, dei server e delle applicazioni.

Secondo quanto riportata dalla Reuters, l'azienda ha dichiarato che gli upgrade in questione possano esser stati manomessi in effetti tra marzo e giugno 2020 in occasione di un grande attacco informatico, ben pianificato e mirato a degli specifici target.

Il presidente di Microsoft **Brad Smith** ha dichiarato ieri sera che le informazioni su un coinvolgimento del software di Redmond sono del tutto false: *"Vogliamo rassicurare i nostri clienti che non abbiamo identificato alcuna vulnerabilità nei prodotti o servizi cloud Microsoft nel corso delle indagini"*, aggiungendo successivamente come *"tutti i dati sono al sicuro".*

La portata dell'azione non è ancora chiara. SolarWinds ritiene che siano stati colpiti tra i 180mila e i 275mila clienti, tra cui tutte le grandi agenzie governative e centinaia di importanti aziende private.

È possibile che siano stati coinvolti anche clienti stranieri di SolarWinds, ma ci vorranno mesi, se non anni, per avere un'idea complessiva di quali siano gli effetti dell'attacco.

https://www.key4biz.it/attacco-hacker-al-governo-usa-le-falle-di-solarwinds-colpiscono-275mila-clienti/335919/

Allarme cybercrime nella Ue ‘Siamo un obiettivo primario’

L’Unione Europea è stata identificata come un **“target primario”** dai cyber criminali globali e per questo deve rinforzare le sue capacità difensive in base al nuovo scenario, secondo la Commissione Ue. A dirlo apertamente è stato ieri il vicepresidente della Commissione Ue **Margaritis Schinas**, in occasione del lancio del nuovo pacchetto di misure Nis 2 che aggiorna la direttiva Nis.

“Ci sono diverse entità, statali e non, che molto semplicemente vogliono che l’Europa fallisca”, ha detto il greco. *“E ci sono molti concorrenti strategici in aree chiave delle nostre politiche e delle nostre industry che utilizzano queste strade per esplorare le nostre vulnerabilità e riuscire a ottenere un vantaggio competitivo. Non c’è dubbio che siamo un obiettivo primario “,* ha aggiunto Schinas.

Un esempio per tutti è il recente cyberattacco del 10 dicembre scorso all’Agenzia Europea del Farmaco di Amsterdam, con l’accesso a informazioni sensibili relative al vaccino per il Covid-19.

“E ci sono molti concorrenti strategici in aree chiave delle nostre politiche e dei nostri settori che utilizzano queste strade per esplorare le nostre vulnerabilità e riuscire a ottenere un vantaggio competitivo. Non c’è dubbio che siamo un obiettivo primario “, ha aggiunto Schinas.

L’alto rappresentante dell’UE **Josep Borrell**, il vicepresidente della Commissione **Margaritis Schinas** e il commissario **Thierry Breton** hanno presentato la strategia ieri in una conferenza stampa a Bruxelles, promettendo che rafforzerebbe la

“*resilienza collettiva contro le minacce informatiche*” in tutto il blocco.

Tra le iniziative vi è l’uso di centri operativi per la sicurezza abilitati all’intelligenza artificiale istituiti in tutta l’UE per creare un *“Cyber Shield”* che rilevi i segnali di attacco e possa avviare un’azione preventiva tempestiva.

Un altro è la creazione di una Joint Cyber Unit per garantire una migliore protezione dagli attacchi informatici dannosi e transfrontalieri.

Cos’altro c’è nella strategia?

• Nuove soluzioni europee per rafforzare la sicurezza Internet globale
• Un regolamento per promuovere un Internet of Secure Things
• Una migliore cassetta degli attrezzi diplomatica per prevenire, scoraggiare e rispondere agli attacchi
• Cooperazione rafforzata per la difesa informatica
• Maggiore dialogo sulla sicurezza informatica con i paesi al di fuori dell’UE, insieme a organizzazioni internazionali come la NATO
• La creazione di un’agenda dell’UE per lo sviluppo di capacità informatiche esterne e di un comitato interistituzionale dell’UE per lo sviluppo di capacità informatiche

La strategia da 2 miliardi di euro sarà finanziata dal programma Europa digitale dell’UE e da Orizzonte Europa, con l’aggiunta di investimenti da parte degli Stati membri e dell’industria.
Inoltre, gli esperti prevedono che il numero di dispositivi connessi in tutto il mondo salirà a 25 miliardi entro il 2025. Si prevede che un quarto di questi dispositivi sarà in Europa.

Dichiarazioni di alcuni membri del collegio

Margrethe **Vestager**, Vicepresidente esecutiva per Un'Europa pronta per l'era digitale, ha dichiarato: *"L'Europa è determinata a portare avanti una trasformazione digitale della nostra società ed economia, che dobbiamo quindi sostenere con livelli di investimento senza precedenti. La riuscita della trasformazione digitale, che sta accelerando, si basa sulla fiducia dei cittadini e delle imprese nella sicurezza dei prodotti e dei servizi connessi che utilizzano."*

L'Alto rappresentante Josep **Borrell** ha dichiarato: *"La sicurezza e la stabilità a livello internazionale dipendono più che mai da un ciberspazio globale, aperto, stabile e sicuro in cui siano rispettati lo Stato di diritto, i diritti umani, le libertà e la democrazia. Con la strategia di oggi l'UE fa un passo avanti nella protezione dei propri governi, dei cittadini e delle imprese dalle minacce informatiche, esercitando la sua leadership nel ciberspazio, di modo che tutti possano trarre vantaggio dall'uso di Internet e delle tecnologie."*

Margaritis **Schinas**, Vicepresidente per la Promozione dello stile di vita europeo, ha affermato: *"La cibersicurezza è un elemento centrale dell'Unione della sicurezza. Non esistono più distinzioni tra minacce online e offline e la dimensione digitale è ormai indissolubilmente connessa alla dimensione reale. L'insieme di misure varate oggi dimostra che l'UE è pronta a usare tutte le risorse e le competenze a sua disposizione per prepararsi e far fronte alle minacce fisiche e informatiche con lo stesso livello di determinazione."*

Thierry **Breton**, Commissario per il Mercato interno, ha dichiarato a sua volta: *"Le minacce informatiche evolvono rapidamente e sono sempre più complesse e adattabili. Per garantire la protezione dei nostri cittadini e delle nostre*

infrastrutture, dobbiamo giocare d'anticipo: uno scudo europeo per la cibersicurezza resiliente e autonomo consentirà di sfruttare le nostre competenze e conoscenze per reagire più rapidamente, limitare i danni potenziali ed essere più resilienti. Investire nella cibersicurezza significa investire nella nostra autonomia strategica e in un ambiente online sano per il futuro."

Ylva **Johansson**, Commissaria per gli Affari interni, ha dichiarato: *"I nostri ospedali, i nostri sistemi di trattamento delle acque reflue o le nostre infrastrutture di trasporto sono forti solo quanto gli anelli più deboli della catena: vi è il rischio che le perturbazioni che si verificano in una parte dell'Unione incidano sulla fornitura di servizi essenziali altrove. Per garantire il buon funzionamento del mercato interno e i mezzi di sussistenza di coloro che vivono in Europa, le nostre infrastrutture essenziali devono essere resilienti di fronte a rischi quali catastrofi naturali, attentati terroristici, incidenti e pandemie come quella che stiamo vivendo oggi. È proprio questo l'intento della mia proposta sulle infrastrutture critiche."*

La nota ufficiale della Commissione UE

Oggi la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza presentano una nuova strategia dell'UE per la cibersicurezza. In quanto componente essenziale della strategia digitale dell'UE Plasmare il futuro digitale dell'Europa, del piano per la ripresa dell'Europa e della strategia dell'UE per l'Unione della sicurezza, la strategia rafforzerà la resilienza collettiva dell'Europa contro le minacce informatiche e contribuirà a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. A prescindere da quali siano i

dispositivi connessi, le reti elettriche, i servizi bancari o i trasporti aerei che i cittadini europei utilizzano o le amministrazioni pubbliche o le strutture ospedaliere che frequentano, essi devono potervi accedere con la sicurezza di essere protetti dalle minacce informatiche.

La nuova strategia per la cibersicurezza consente inoltre all'UE di rafforzare la leadership su norme e standard internazionali nel ciberspazio e di intensificare la collaborazione con i partner in tutto il mondo al fine di promuovere un ciberspazio globale, aperto, stabile e sicuro, fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori della democrazia.

La Commissione sta inoltre presentando proposte per affrontare la questione della resilienza sia informatica che fisica dei soggetti critici e delle reti essenziali: una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") e una nuova direttiva sulla resilienza dei soggetti critici. Questi documenti coprono un'ampia gamma di settori e mirano ad affrontare in maniera coerente e complementare i rischi online e offline attuali e futuri, dagli attacchi informatici alla criminalità o alle catastrofi naturali.

Fiducia e sicurezza al centro del decennio digitale dell'UE

La nuova strategia per la cibersicurezza mira a salvaguardare un'Internet globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza ma anche per proteggere i valori europei e i diritti fondamentali di tutti. Sulla base dei risultati conseguiti negli ultimi mesi e anni, contiene proposte concrete di iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE:

1. **resilienza, sovranità tecnologica e leadership**

In questa linea d'azione la Commissione propone di riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") al fine di aumentare il livello di ciberresilienza dei settori pubblici e privati essenziali: strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali, nonché altre infrastrutture e servizi essenziali che devono rimanere impermeabili in un contesto di minacce sempre più repentine e complesse.

La Commissione propone inoltre di avviare una rete di centri operativi per la sicurezza in tutta l'UE, alimentati dall'intelligenza artificiale (IA), che costituirà per l'UE una vera e propria barriera di cibersicurezza in grado di rilevare tempestivamente i segnali di un attacco informatico e consentire un'azione proattiva prima che si verifichino danni. Ulteriori misure comprenderanno un sostegno dedicato alle piccole e medie imprese (PMI) nel quadro dei poli dell'innovazione digitale e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i migliori talenti in materia di cibersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza.

2. **Sviluppo della capacità operativa di prevenzione, deterrenza e risposta**

Nell'ambito di un processo progressivo e inclusivo portato avanti con gli Stati membri, la Commissione sta preparando, una nuova unità congiunta per il ciberspazio allo scopo di rafforzare la collaborazione tra gli organismi dell'UE e le autorità degli Stati membri responsabili della prevenzione, della deterrenza e della risposta agli attacchi informatici,

comprese le comunità civili, diplomatiche, di contrasto e di difesa informatica. L'alto rappresentante ha presentato proposte per rafforzare il pacchetto di strumenti della diplomazia informatica dell'UE al fine di prevenire, dissuadere e rispondere in modo efficace alle attività informatiche dolose, in particolare quelle che interessano le nostre infrastrutture, le catene di fornitura, le istituzioni e i processi democratici essenziali. L'UE mira inoltre a rafforzare ulteriormente la collaborazione in materia di ciberdifesa e a sviluppare capacità di ciberdifesa all'avanguardia, basandosi sul lavoro svolto dall'Agenzia europea per la difesa e incoraggiando gli Stati membri a sfruttare appieno la cooperazione strutturata permanente e il Fondo europeo per la difesa.

3. **Promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione**

L'UE intensificherà la collaborazione con i partner internazionali per rafforzare l'ordine mondiale basato su regole, promuovere la sicurezza e la stabilità nel ciberspazio e proteggere i diritti umani e le libertà fondamentali online. Promuoverà norme e standard internazionali che riflettano questi valori fondamentali dell'UE cooperando con i suoi partner internazionali nell'ambito delle Nazioni Unite e in altri contesti pertinenti. L'UE rafforzerà ulteriormente il suo pacchetto di strumenti della diplomazia informatica e intensificherà gli sforzi per la creazione di capacità informatiche nei paesi terzi sviluppando un'apposita agenda esterna dell'UE. Saranno intensificati i dialoghi in materia di cibersicurezza con i paesi terzi e le organizzazioni regionali e internazionali, nonché con la comunità multipartecipativa. L'UE istituirà inoltre una rete per la diplomazia informatica in tutto il mondo per promuovere la propria visione del ciberspazio.

L'UE si è impegnata a sostenere la nuova strategia per la cibersicurezza nei prossimi sette anni con investimenti nella

transizione digitale dell'UE a livelli finora mai raggiunti, attraverso il prossimo bilancio a lungo termine dell'UE, in particolare tramite il programma Europa digitale, Orizzonte Europa e il piano per la ripresa dell'Europa. Gli Stati membri sono pertanto incoraggiati a utilizzare appieno il dispositivo per la ripresa e la resilienza dell'UE per rafforzare la cibersicurezza e a fare investimenti a pari livello di quelli dell'UE. L'obiettivo è raggiungere fino a 4,5 miliardi di € di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, in particolare nell'ambito del Centro di competenza sulla cibersicurezza e della rete dei centri di coordinamento e garantire che una parte importante di questi investimenti siano effettivamente attribuiti alle PMI.

La Commissione mira inoltre a rafforzare le capacità industriali e tecnologiche dell'UE in materia di cibersicurezza, anche tramite progetti finanziati congiuntamente dall'UE e dai bilanci nazionali. L'UE ha l'opportunità unica di mettere in comune le proprie risorse per rafforzare la sua autonomia strategica e promuovere la sua leadership nel campo della cibersicurezza lungo tutta la catena di fornitura digitale (compresi dati e cloud, tecnologie per processori di prossima generazione, connettività ultrasicura e reti 6G), in linea con i suoi valori e le sue priorità.

Ue: Resilienza informatica e fisica delle reti, dei sistemi informativi e dei soggetti critici

È necessario aggiornare le misure esistenti a livello dell'UE volte a proteggere i servizi e le infrastrutture essenziali dai rischi sia informatici che fisici. I rischi per la cibersicurezza continuano a evolvere con la crescente digitalizzazione e interconnessione. Anche i rischi fisici sono diventati più complessi dall'adozione delle norme dell'UE

sulle infrastrutture essenziali del 2008, che attualmente riguardano solo i settori dell'energia e dei trasporti. L'obiettivo delle revisioni è aggiornare le norme seguendo la logica della strategia dell'UE per l'Unione della sicurezza, superando la falsa dicotomia tra online e offline e mettendo da parte l'approccio a compartimenti stagni.

Per rispondere alle crescenti minacce dovute alla digitalizzazione e all'interconnessione, **la direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2")** proposta riguarderà le entità di medie e grandi dimensioni di diversi settori in base alla loro importanza per l'economia e la società. La direttiva NIS 2 renderà più rigidi i requisiti di sicurezza imposti alle imprese, affronterà la sicurezza delle catene di fornitura e delle relazioni con i fornitori, semplificherà gli obblighi di notifica, introdurrà misure di vigilanza più rigorose per le autorità nazionali e obblighi di esecuzione più severi e avrà l'obiettivo di armonizzare i regimi sanzionatori in tutti gli Stati membri. La direttiva NIS 2 proposta contribuirà ad aumentare la condivisione delle informazioni e la cooperazione in materia di gestione delle crisi informatiche a livello nazionale e dell'UE.

La **direttiva sulla resilienza dei soggetti critici** proposta estende sia l'ambito di applicazione, sia la profondità della direttiva sulle infrastrutture critiche europee del 2008. Sono ora contemplati dieci settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Nell'ambito della direttiva proposta ciascuno Stato membro adotterebbe una strategia nazionale per garantire la resilienza dei soggetti critici ed effettuerebbe valutazioni periodiche dei rischi. Tali valutazioni contribuirebbero a individuare un sottoinsieme più ristretto di soggetti critici cui incomberebbero obblighi volti a rafforzarne la resilienza di fronte ai rischi non informatici,

comprese le valutazioni dei rischi a livello di soggetto, l'adozione di misure tecniche e organizzative e la notifica degli incidenti. A sua volta la Commissione fornirebbe sostegno complementare agli Stati membri e ai soggetti critici, per esempio sviluppando una visione d'insieme a livello dell'UE dei rischi transfrontalieri e intersettoriali e delle migliori pratiche, metodologie e attività di formazione e di esercizio transfrontaliere per testare la resilienza dei soggetti critici.

Garantire la sicurezza delle reti di prossima generazione: 5G e oltre

Nell'ambito della nuova strategia per la cibersicurezza e con il sostegno della Commissione e dell'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, gli Stati membri sono incoraggiati a portare a termine l'attuazione del pacchetto di strumenti dell'UE per le reti 5G, che definisce un approccio globale e basato sui rischi oggettivi per la sicurezza delle reti 5G e di prossima generazione.

Secondo una relazione pubblicata oggi sull'impatto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G e sui progressi compiuti nell'attuazione del pacchetto di strumenti comune dell'UE comprendente misure di attenuazione, rispetto alla relazione sui progressi compiuti, pubblicata nel luglio 2020, la maggior parte degli Stati membri è già a buon punto nell'attuazione delle misure raccomandate. Ora dovrebbero mirare a completarne l'attuazione entro il secondo trimestre del 2021 e a garantire che i rischi individuati siano adeguatamente mitigati, in modo coordinato, in particolare nell'ottica di ridurre al minimo l'esposizione ed evitare la dipendenza dai fornitori ad alto rischio. La Commissione oggi delinea inoltre gli obiettivi e le azioni chiave volte a portare avanti tale sforzo coordinato a livello dell'UE.

Prossime tappe

La Commissione europea e l’alto rappresentante sono determinati ad attuare la nuova strategia per la cibersicurezza nei prossimi mesi. Entrambi riferiranno periodicamente sui progressi compiuti e informeranno e coinvolgeranno a pieno titolo in tutte le azioni pertinenti il Parlamento europeo, il Consiglio dell’Unione europea e i portatori di interessi.

Spetta ora al Parlamento europeo e al Consiglio esaminare e adottare la proposta di direttiva NIS 2 e la direttiva sulla resilienza dei soggetti critici. Una volta che le proposte saranno concordate e successivamente adottate, gli Stati membri dovranno recepirle entro 18 mesi dall’entrata in vigore.

La Commissione riesaminerà periodicamente la direttiva NIS 2 e la direttiva sulla resilienza dei soggetti critici e presenterà relazioni in merito al loro funzionamento.

https://www.key4biz.it/allarme-cybercrime-nella-ue-siamo-un-obiettivo-primario/335741/

Intelligenza artificiale e sicurezza, quali nuove minacce informatiche? Il report ENISA

Dopo la pubblicazione del report delle nuove minacce informatiche nelle reti quinta generazione, l'agenzia dell'**Unione europea per la sicurezza informatica** ha pubblicato il rapporto sul panorama delle minacce cyber anche nel settore dell'intelligenza artificiale, svelando le principali sfide alla sicurezza informatica che l'ecosistema dell'IA deve affrontare.

Nel report "**AI Threat Landscape" l'ENISA** sottolinea l'importanza della sicurezza informatica e della protezione dei dati in ogni parte dell'ecosistema AI per creare una tecnologia affidabile per gli utenti.

Lo studio dell'agenzia per la sicurezza adotta un approccio metodologico per mappare i principali attori e minacce nell'IA. La relazione fa seguito alle priorità definite nel Libro bianco sull'IA 2020 della Commissione europea.

Intelligenza artificiale e cybersecurity

Il nuovo lavoro dell'agenzia mira a fungere da base per le iniziative per proteggere l'IA: sia in termini di politiche, poiché inquadra il problema e fornisce indicazioni sulle minacce alla sicurezza informatica, sia in termini di controlli tecnici, in quanto evidenzia minacce specifiche per quale azione può essere necessaria.

Il rapporto è diretto ai responsabili delle politiche quando sviluppano linee guida future sulle implementazioni sicure dell'IA, agli esperti tecnici per supportare valutazioni del rischio personalizzate e agli organismi di standardizzazione per supportare i futuri standard di sicurezza dell'IA.

Il panorama delle minacce dell'IA dell'ENISA identifica le

sfide e le opportunità per implementare sistemi e servizi di IA sicuri in tutta l’Unione. Il rapporto sottolinea la necessità di misure di sicurezza più mirate e proporzionate per mitigare le minacce individuate, nonché la necessità di un’analisi approfondita dell’uso dell’IA in settori come la salute, l’automotive e la finanza.

Per approfondire

https://www.key4biz.it/intelligenza-artificiale-e-sicurezza-quali-nuove-minacce-informatiche-il-report-enisa/335531/