Come gestire un attacco informatico e quali errori non fare. Il truck di IBM

Simulare un cyber attack, è un modo per capire come le aziende potrebbero reagire ad un eventuale attacco informatico imparando a gestire lo stress e a difendersi da un possibile data breach.

Tutto questo è opera di **IBM** che ha investito 200 milioni di dollari nella costruzione del'**X-Force Command Cyber Tactical Operations Center** (C-TOC), una sala operativa cyber su ruote, approdata al **Politecnico di Milano,** in piazza Leonardo da Vinci (dove rimarrà fino al 20 settembre).

X-Force Command C-TOC

[embedded content]
L' X-Force C-TOC è un **Cybersecurity Operation Center** basato sul modello dei centri operativi tattici utilizzati dalle postazioni di comando militari. La struttura mobile contiene un centro di sorveglianza, un data center e strutture per conferenze in grado di ospitare oltre venti operatori tra analisti e personale.

L'autoarticolato, equipaggiato con alimentazione autosufficiente e comunicazioni satellitari e cellulari, offre una rete sterile e resiliente per indagini sugli incidenti informatici e relativa risposta.

"*Grazie all'X-Force andiamo a creare una simulazione immersiva e integrale per far testare alle aziende la risposta ad un attacco informatico",* ha spiegato **Francesco Teodonno**, IBM

Security Leader per l'Italia. *"Gli attacchi al giorno d'oggi sono diventati molto più sofisticati, non parliamo di malware ma di veri e propri sistemi di attacco. Quindi per affrontare una sfida di questo tipo bisogna essere preparati a saper prendere l'attacco".*

La simulazione

Durante la simulazione cerchiamo di prendere in considerazione più punti di vista. Non solo l'aspetto tecnico, ma anche la gestione degli aspetti di leadership, di gestione del rischio, di gestione della comunicazione, di policy e la relazione che c'è con i media", ha spiegato durante la simulazione **Pompeo D'Urso**, C-TOC Technical Leader di IBM Security. *"E' quello che facciamo nella nostra tipologia di sessione, orientata quindi alla leadership e alla Business Relationship Responsive, nella quale l'azienda deve vedere il livello di preparazione nel caso in cui devono interagire anche con enti esterni.*

La sala operativa dell'X-Force durante la simulazione
"E' in virtù di tutta una serie di possibili attacchi – continua Pompeo *– come ad esempio problemi con i bancomat, problemi con la divulgazione online dei dati degli utenti e di quanti questi abbiamo un impatto sulla brand reputation, che ne può derivare un danno economico. Quindi bisogna considerare più punti di vista e allenarsi il più possibile per essere pronti ad affrontare nel momento in cui si è esposti ad un cyber attack".*

> *#CToc #CyberSecurity #IBM a #Milano in collaborazione con @polimi: #presstour e simulazione di un #CyberAttack: come gestire al meglio un attacco informatico. pic.twitter.com/vV4OlCAx9D*
>
> *— IBM Italia (@IBMItalia) September 12, 2019*

Formazione e mancanza di cyberskills

La funzione del camion C-TOC non è solo quella di aiutare le aziende nella loro formazione sulla sicurezza informatica, ma anche di fornire uno scopo educativo per aiutare a colmare il crescente divario delle **cyberskills**.

Portando il camion C-TOC nelle scuole e nelle università, IBM si augura di incoraggiare sempre più studenti a prendere in considerazione una carriera nel settore della sicurezza informatica.

L'X-Force Command C-TOC di IBM in piazza Leonardo Da Vinci a Milano
Nei prossimi giorni saranno ospiti del truck anche gli studenti del Politecnico che potranno provare le simulazioni **il 19 settembre**. Partito dagli Usa nel 2018 e dopo aver toccato le principali città europee, il truck andrà alla volta di Madrid per l'ultima tappa del suo tour europeo.

https://www.key4biz.it/come-gestire-un-attacco-informatico-e-quali-errori-non-fare-il-truck-di-ibm/270613/

Non ci sono più gli hacker di una volta

Nel variegato mondo delle minacce di sicurezza informatica uno dei pericoli più insidiosi è sicuramente il **Remote Access Trojan (RAT)**.

Si tratta di un programma malware che lavora includendo una back door per il controllo amministrativo del computer bersaglio.

Una delle inside principali è proprio l'abilità del **RAT** di essere scaricato in modo invisibile con un programma richiesto dall'utente – che si tratti di un'applicazione, un gioco o un semplice PDF – o inviato come allegato a un'e-mail.

Una volta che il sistema host è compromesso, l'intruso può usarlo per distribuire RAT ad altri computer vulnerabili e creare una botnet.

Adwind: il più pericoloso

Esistono, come per tutti i malware, vari tipi di RAT, ma non c'è dubbio che il più "completo" sia **Adwind**, grazie alla sua capacità di sottrarre informazioni dai sistemi bersaglio, di crittografare file e di impossessarsi delle credenziali **VPN**.

Come se non bastasse, nelle sue ultime release, è stata aggiunta l'abilità di fare keylogging, screenshot, registrare video dalla webcam del pc bersaglio e audio dal microfono.

Scoperto per la prima volta nel 2012 – al tempo era noto come Frutas – Adwind mantenendo la sua struttura è anche chiamato **AlienSpy, Unrecom, Sockrat, JSocket** e **JRAT**. Nel suo primo picco di attività (2013-2016) è stato indicato come il colpevole di quasi 160 campagne di attacco nei confronti di oltre 70mila target.

Tra queste spicca quella portata avanti da AlienSpy sul finire del 2015 che ha preso di mira tutti i maggiori player nel settore della finanza e delle TelCo statunitensi oltre ad alcuni enti governativi attraverso delle campagne di phishing

mirate. All’interno delle e-mail incriminate il malware era ben nascosto nei panni di fatture, note spesa o addirittura ordine da parte di fornitori.

La facilità con cui era riuscito a diffondersi era anche in parte dovuta all’abilità del malware di funzionare su tutte le principali piattaforme disponibili sul mercato: da Windows a Mac, passando per Linux e Android.

Bersagli diversificati

Se inizialmente Adwind sembrava avere come bersaglio unicamente i settori citati poco prima, di recente, secondo uno studio pubblicato da un’università americana, il malware è cominciato ad apparire come il principale indiziato in attacchi che hanno coinvolto oltre 1.500 organizzazioni di oltre 100 Paesi; organizzazioni che andavano dal settore dell’industria pesante fino ai piccoli studi legali. Un pattern che non sembra seguire particolari “agende” come spesso accade quando alle spalle di queste campagne ci sono gruppi hacker sponsorizzati. Nel 2017 è comparso dopo una serie di incidenti che hanno coinvolto le principali aziende del settore aerospaziale europeo, preambolato da una attenta strategia di social engineering. Nel 2018 ha sfruttato una vulnerabilità di Autodesk A360 per ottenere il controllo numerosi sistemi. Nel 2019 è stato trovato in oltre 2 milioni di email di phishing.

Il Cyber crimine diventa SaaS

Uno dei motivi per questa apparente randomizzazione degli attacchi è dovuta al fatto che Adwind, nelle sue versioni **JSocket**, è da qualche tempo distribuito nel dark web, in una sorta di perverso e-commerce del Cyber crimine.

I prezzi variano dai 30 dollari per il pacchetto contenente il Malware pronto ad essere lanciato (solo per un mese) fino ai

200 per una licenza illimitata, una sorta di crimine as a service; il tutto – ovviamente – corredato di supporto tecnico e assistenza via mail.

Sfortunatamente il fenomeno non è limitato ai soli RAT: il mercato del Dark web è diventato un vero e proprio retail che opera su piattaforme, non troppo differenti da un qualsiasi e-shop, 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 accennato, che comprendono FAQ, chat di supporto e dettagliate pagine di aiuto.

Oltre ai già i citati RAT si possono trovare Decrittatori di Password, campagne di Phishing pre-confezionate, keyloggers e pacchetti completi "end to end" che comprendono tutti gli elementi necessari a compiere frodi bancarie. Naturalmente in questo mondo regnano le cripto valute, per loro natura difficili da tracciare.

Gli esempi qui elencati sono solo la punta dell'iceberg di un mondo che, nonostante i migliori tentativi delle autorità preposte, sembra essere solo in crescita.

Oggi, esistono decine di piattaforme che vendono software come i malware e per ogni sito che viene abbattuto un altro eventualmente prende il suo posto.

È stato stimato che nel 2017 negli Stati Uniti d'America le frodi commesse online hanno causato circa 17 miliardi di dollari di perdite ad aziende e privati, mentre in Europa l'Italia si piazza in seconda posizione per numero di crimini subiti.

È sicuramente utopistico augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono aiutare a scongiurare questi attacchi.

Una delle misure più semplici parte dall'igiene delle password: una password 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.

Un altro 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.

Sono regole semplici da seguire, ma che possono migliorare drasticamente la resilience dei propri sistemi e dispositivi.

Sparisce la barriera d'ingresso

Ma facendo un passo indietro, la preoccupazione più grande è inerente alla facilità di accesso per attori malintenzionati agli strumenti necessari per compiere crimini on-line.

La scena del Criminal hacking fino a pochi anni fa era stata dominata da un substrato di persone in possesso di un certo livello di *skill*.

La recente ondata di pacchetti e soluzioni *ready made* rischia di inondare il web di aspiranti Criminal hacker che ora non hanno necessariamente le competenze e le conoscenze necessarie per portare avanti campagne di phishing o di malware da soli, ma che grazie ai servizi del Dark Web si trovano le soluzioni già preconfezionate e pronte ad essere utilizzate.

La democratizzazione del Cyber crime, quindi, sembra essere alle porte.

https://www.key4biz.it/non-ci-sono-piu-gli-hacker-di-una-volta/269783/

Google scopre vulnerabilità sugli iPhone, rubati dati personali degli utenti

Bastava visitare siti malevoli attraverso un iPhone per diventare bersaglio di cybercriminali che potevano prendere il controllo del telefono e attingere a dati personali degli utenti, posizione, foto. In pratica monitorarli. Lo riporta oggi il Guardian dove a scoprire, a febbraio scorso, le falle di sicurezza di Apple è stato un gruppo di ricercatori di **Google Project Zero**, il team che si occupa di attacchi informatici 'zero days' cioè quelli di cui non sono a conoscenza neanche gli sviluppatori o le aziende informatiche che hanno creato i software. **Cupertino**, dopo la segnalazione dei ricercatori ha corretto le vulnerabilità.

"*La semplice visita al sito compromesso era sufficiente affinché il server attaccasse il dispositivo e, in caso di successo, installasse un impianto di monitoraggio*", ha spiegato **Ian Beer** in un post pubblicato sul blog di Project Zero. In pratica, gli hacker potevano avere accesso all'iPhone, installando applicazioni dannose e anche monitorando l'attività dell'utente a sua insaputa. Per i ricercatori di Google, le vulnerabilità del sistema operativo sarebbero state sfruttate sia per rubare foto e messaggi, che per rintracciare la posizione in tempo reale di dispositivi e utenti. Gli esperti di Google hanno segnalato la scoperta a Cupertino lo scorso 1 febbraio. I vertici americani hanno subito rilasciato le correzioni per evitare problemi legati

alla sicurezza, lanciando il 7 febbraio l'aggiornamento iOS 12.1.4, proprio per correggere i problemi riscontrati nelle versioni precedenti.

Le vulnerabilità erano presenti in quasi tutte le versioni di iOS 10 e fino all'ultima versione di iOS 12, il sistema operativo per dispositivi mobili di Cupertino. "*Questo* – aggiunge Ian Beer – *indica che un gruppo stava compiendo uno sforzo prolungato per hackerare gli utenti di iPhone su un periodo di almeno due anni". Secondo i ricercatori, inoltre, alla base delle vulnerabilità ci sono "codici che sembra non abbiano mai funzionato"* oppure *"abbiano avuto pochi test o revisioni prima di essere resi disponibili agli utenti*".

https://www.key4biz.it/google-scopre-vulnerabilita-sugli-iphone-rubati-dati-personali-degli-utenti/269160/

Cybercrime, aumentano gli attacchi phishing in Italia. Come difendersi

In Italia e nel mondo continuano ad aumentare gli attacchi del cybercrime di tipo phishing. Secondo gli esperti di cybersecurity il fenomeno è in crescita a causa di due elementi: da una parte la disponibilità di liste infinite di email, in vendita per pochi soldi sul dark web o sui forum degli hacker. Dall'altra la costante disattenzione degli utenti quando ricevono un messaggio o navigano su Internet.

Il phishing è una truffa veicolata tramite Internet, in cui si cerca di ingannare la vittima al fine di recuperare informazioni sensibili come username, password o dati bancari. Generalmente, il criminale informatico invia false comunicazioni al soggetto-vittima, fingendosi un Ente o un'azienda ben conosciuta o con cui è possibile che si stiano avendo conversazioni e relazioni, usando scuse plausibili per ottenere i dati personali della vittima.

6 consigli su come difendersi

1. **mantenere il proprio browser sempre aggiornato.** Installando le ultime versioni e inserendo dei filtri anti-spam, o degli appositi plug-in
2. **controllare il dominio da cui proviene la comunicazione.** Una società o un ente scriveranno sempre dal proprio dominio, bisogna controllare che corrisponda a quello ufficiale. Questa verifica non dà la massima garanzia di autenticità ma rappresenta un primo controllo da poter effettuare;
3. **fare attenzione a cliccare sui link nelle e-mail.** Come buona norma si consiglia di non cliccare mai sui link contenuti nella comunicazione ma digitare direttamente nel browser l'indirizzo del sito ufficiale del mittente della comunicazione e verificare sul sito il contenuto descritto nella comunicazione dell'e-mail;
4. **utilizzare più indirizzi e-mail.** Quando ci si iscrive a servizi, o siti web, di dubbia affidabilità, è preferibile utilizzare e-mail secondarie, in modo da non rischiare di contaminare la propria casella e-mail principale;
5. **contattare il servizio clienti.** Se arriva una e-mail ambigua e non si capisce con certezza se sia una frode o meno, è meglio contattare il servizio clienti dell'azienda a cui la mail fa riferimento.
6. **segnalare un sito di phishing** aiutando altri utenti a non cadere nella truffa.

Cybercrime, aumentano gli attacchi phishing in Italia. Come difendersi

---

Intel, nuova vulnerabilità sui processori: interessa le Cpu dal 2012 in poi. Rilasciata da Windows ‘patch’

Dopo Spectre e Meltdown, le due falle di sicurezza di cui il mondo è venuto a conoscenza nel gennaio 2018, i processori prodotti da **Intel** hanno un’altra vulnerabilità che permetterebbe a un criminale informatico di impossessarsi di informazioni rilevanti. A scoprire la nuova falla, simile alle due precedenti e chiamata **SwapGs**, è stata la società di sicurezza informatica **Bitdefender**. **Windows** ha già rilasciato una patch di sicurezza per evitare lo sfruttamento della vulnerabilità, mentre i computer **Mac** e **Linux** non sarebbero interessati dal problema.

La falla riguarda tutte le Cpu prodotte da Intel a partire dal 2012, processori *“che sfruttano la tecnica di esecuzione speculativa, consentendo agli hacker di accedere a password, token, conversazioni private, file crittografati e altri dati sensibili degli utenti, sia di tipo privato che professionale”,* spiega Bitdefender in una nota. La vulnerabilità, si legge, apre a un *“attacco laterale che fornisce all’aggressore un metodo per accedere a tutte le informazioni contenute nella memoria del kernel del sistema operativo”.* L’attacco sfrutta l’esecuzione speculativa, una

funzionalità che cerca di velocizzare la Cpu “educandola” a prevedere le istruzioni successive.

“I criminali a conoscenza di questi attacchi avrebbero il potere di individuare le informazioni più vitali e meglio protette sia di aziende che di privati in tutto il mondo, e la relativa facoltà di rubare, ricattare, sabotare e spiare”, ha affermato **Gavin Hill**, vicepresidente di Bitdefender.

La vulnerabilità è simile e collegata a Spectre e Meltdown, ma le misure di sicurezza messe in campo per neutralizzare quelle due falle sono inefficaci contro la nuova minaccia. Microsoft, come detto, ha rilasciato una patch, e Bitdefender ha messo a disposizione una soluzione per mitigare l’attacco sui sistemi Windows senza patch.

https://www.key4biz.it/intel-nuova-vulnerabilita-sui-processori-interessa-le-cpu-dal-2012-in-poi-rilasciata-da-windows-patch/268314/

Capital One, UniCredit smentisce il data leak: ‘Nessuna violazione’

Dopo aver condotto un’indagine interna, **UniCredit** ha rivelato che non sussisterebbe alcuna prova del suo coinvolgimento nella violazione dei dati di **Capital One**. Lo ha dichiarato l’Istituto bancario in una nota interna indirizza ai dipendenti.

L’azienda ha infatti affermato di non aver trovato prove di violazione, sottolineando come i dati dei propri clienti non siano stati salvati sui server **Amazon** hackerati.

La violazione a Capital One

Il 30 luglio **Capital One**, holding bancaria con Sede in Virginia, ha dichiarato di aver subìto una data leak che ha coinvolto circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada.

Secondo la banca americana i criminali informatici sono riusciti a sfruttare una “*vulnerabilità di configurazione*” nella strutture informatiche dell’azienda rubando dati sensibili quali: nomi, indirizzi, numeri di telefono ed estratti conto.

L’azienda ha però precisato che gli hacker non sono arrivati ad avere accesso ai numeri di conto corrente collegati ai numeri di carte di credito.

UniCredit

UniCredit ieri ha dichiarato di aver avviato un’indagine sulla vicenda dopo che il nome della banca è stato citato in un blog come un possibile obiettivo della presunta hacker, **Paige A. Thompson,** una ex dipendente di Amazon.

Secondo Capital One, Thompson “*ha utilizzato le credenziali del firewall dell’applicazione Web per raggiungere il database del clienti della banca e di altre organizzazioni finanziarie*“.

Non solo UniCredit, ma anche la **Ford** ha avviato indagini per accertare se i propri dati siano stati hackerati durante

l’hackeraggio alla holding bancaria, ma la casa automobilistica americana al momento non ha ancora rilasciato dichiarazioni ufficiali.

https://www.key4biz.it/capital-one-unicredit-smentisce-il-data-leak-nessuna-violazione/267809/

Capital One, anche UniCredit coinvolta? Cosa sappiamo sul data breach

Sono stati hackerati dati personali di milioni di persone di **Capital One,** banca americana con Sede in **Virginia**. L’azienda, attraverso un comunicato diffuso il 30 luglio, ha dichiarato che l’incidente ha colpito circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada.

Nomi, indirizzi, numeri di telefono, storia bancaria, estratti conto, entità di prestiti ed altro sono tra i dati sottratti, ha reso noto l’azienda, precisando che gli hacker non sono arrivati però ad avere accesso ai numeri di conto corrente collegati ai numeri di carte di credito.

Secondo la banca, l’hackeraggio è stato rilevato il 19 luglio, precisando che l’hacker, apparentemente già arrestata, è riuscita a “*sfruttare*” una “vulnerabilità di configurazione” nella strutture informatiche dell’azienda. Il presidente di Capital One, **Richard Fairbank**, si è scusato dicendosi “*grato che la responsabile sia stata catturata*“, ma “*profondamente dispiaciuto per quanto è accaduto*“.

Cosa è successo

Il 29 luglio, agenti dell'FBI hanno arrestato **Paige A. Thompson** con il sospetto di aver scaricato circa **30 GB di dati** relativi alle richieste di credito di Capital One da un server.

Tali dati includevano circa 140.000 numeri di previdenza sociale e circa 80.000 numeri di conti bancari su consumatori statunitensi e circa 1 milione di numeri di previdenza sociale (SIN) per clienti di carte di credito canadesi.

"*È importante sottolineare che nessun numero di conto della carta di credito o credenziali di accesso è stato compromesso e oltre il 99% dei numeri di previdenza sociale non è stato compromesso*", ha dichiarato Capital One in una nota pubblicata sul suo sito.

"*La più ampia categoria di informazioni a cui si è avuto accesso sono state le informazioni sui consumatori e le piccole imprese dal momento in cui hanno richiesto uno dei nostri prodotti con carta di credito dal 2005 all'inizio del 2019*", continua la nota. "*Queste informazioni includevano informazioni personali che Capital One raccoglie regolarmente nel momento in cui riceve le richieste di carte di credito, inclusi nomi, indirizzi, codici postali, numeri di telefono, indirizzi e-mail e date di nascita*."

Il profilo della ex dipendente di Amazon

Il responsabile del databreach a Capital One è stato un ex dipendente della società di web hosting **Amazon**.

Presumibilmente il dipendente "*infedele ha utilizzato le*

credenziali del firewall dell'applicazione Web per ottenere l'escalation dei privilegi e raggiungere il database del clienti della banca e di altre organizzazioni finanziarie".

Capital One ha dichiarato di aspettarsi costi per sanare l'incidente compresi tra 100 e 150 milioni. La compagnia ha una polizza assicurativa a rischio cibernetico con una franchigia di 10 milioni e una copertura di 400 milioni di dollari.

Unicredit: "Stiamo effettuando gli approfondimenti necessari"

La banca italiana **UniCredit** e la casa automobilistica americana **Ford** hanno avviato indagini per accertare se i loro dati siano stati hackerati dalla violazione della sicurezza dei dati di Capital One,

Secondo quanto riporta quotidiano statunitense "**Wall Street Journal**", la banca italiana sta esaminando se una directory che si trova su un server cloud è stata raggiunta senza autorizzazione.

UniCredit, la più grande banca italiana, ha dichiarato in una nota di aver contattato le autorità competenti e di effettuare tutti gli approfondimenti necessari.

"*Il 30 luglio UniCredit è venuto a conoscenza del fatto che il suo nome è stato menzionato in relazione all'emissione di Capital One*", ha dichiarato il portavoce in una nota. "*La sicurezza dei dati e la privacy sono le priorità chiave da sempre. UniCredit ha contattato le autorità interessate e sta effettuando tutti gli approfondimenti necessar*i".

https://www.key4biz.it/capital-one-anche-unicredit-coinvolta-cosa-sappiamo-sul-data-breach/267627/

Alessandro Morelli (Lega): ‘Un pacchetto di proposte di legge su digitale e Tlc per la sovranità digitale’

“L’Italia deve mettere la quinta sulle tematiche digitali!”, così **Alessandro Morelli**, presidente della commissione Tlc alla Camera, ha annunciato il pacchetto di proposte di legge della **Lega** sulle nuove frontiere del digitale e delle telecomunicazioni che domani presenterà a Montecitorio insieme ai deputati **Massimiliano Capitanio**, membro della Commissione Telecomunicazioni alla Camera, e **Igor Iezzi,** componente della Commissione Affari Costituzionali.

Le proposte di legge saranno illustrate nel dettaglio alle ore 14:30 presso la sala stampa della Camera dei Deputati.

Morelli: “Tra le nostre proposte includiamo un aggiornamento della Carta Costituzionale, norme per migliorare la sicurezza in Rete e aprire dibattito sul cloud nazionale e la gestione delle reti 5G’

“Sono provvedimenti variegati, che però hanno un unico denominatore comune: fare un grande passo avanti a livello normativo nella direzione che sta prendendo tutto il mondo, per quanto riguarda il digitale”, ha dichiarato Morelli*. “Non si tratta solo di colmare un vuoto normativo, il legislatore ha il compito di stare al passo con i tempi e persino*

anticiparli, trovare ora una soluzione ai problemi che sorgeranno in Italia in tempi brevi”, ha aggiunto il presidente della Commissione Tlc e responsabile Editoria della Lega.

“Il senso di una proposta di legge è aprire un dibattito nel Paese, ecco perché è importante parlarne adesso. Tra le nostre proposte”, ha annunciato il deputato della Lega*, “includiamo un aggiornamento della Carta Costituzionale, che è stata scritta in un’epoca in cui i computer non esistevano, ma anche norme per migliorare la sicurezza in Rete”. “Ancora”,* ha continuato Morelli, *“si apre il dibattito sul cloud nazionale”,* in cui il presidente della Commissione Tlc vorrebbe custodire i dati della Pa, come già annunciato, *“e sulla gestione dell’infrastruttura fisica per la diffusione nelle grandi città della rete 5G. Le istituzioni devono parlare oggi per agire da subito, perché domani sarà già troppo tardi”*, ha concluso Morelli.

Le proposte di legge che saranno presentate domani, apriranno un dibattito sul tema della sovranità digitale, diritto rivendicato anche dalla Germania, che è già all’opera per realizzare la piattaforma cloud nazionale.

“La Germania ha diritto alla sovranità tecnologica. I data center dei cloud non dovrebbero essere installati solo negli Stati Uniti o in Cina, ma anche in Germania, in modo che le aziende europee, che desiderano un’archiviazione sicura e affidabile dei dati, abbiano questa opzione“, ha detto il ministro dell’Economia tedesco **Peter Altmaier**.

https://www.key4biz.it/alessandro-morelli-lega-un-pacchetto-di-proposte-di-legge-su-digitale-e-tlc-per-la-sovranita-digitale/266426/

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

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

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

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

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

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

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

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

Swascan e le vulnerabilità di Huawei

Finanza Agevolata è la rubrica a cura di **Sercam Advisory** dedicata agli aggiornamenti sui bandi pubblici (europei, nazionali, regionali) aperti o in prossima apertura. Per consultare tutti gli articoli clicca qui.

Lo scorso 8 luglio gli esperti **Swascan** avevano identificato una serie di criticità sull'infrastruttura e sulle web app **Huawei**.

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

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

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

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

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

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

Quando a maggio abbiamo contattato Huawei, l'attenzione che ha dimostrato verso le nostre scoperte, unitamente agli scambi di e-mail, le valutazioni, le attività di remediation e i tempi

di risoluzione sono stati tra i più seri, professionali e trasparenti che abbiamo potuto sperimentare in prima persona.

La filosofia alla base dei *Responsible Vulnerability Discosure* è quella di portare maggiore attenzione sull'importanza di una collaborazione reale, vera, efficace ed efficiente tra i software vendor e le aziende di CyberSecurity.

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

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

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

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

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

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