Agenzia per la cybersicurezza, l’importanza del fattore umano e della formazione

Come ho avuto modo di evidenziare durante la mia audizione davanti alle Commissioni competenti della Camera, la valorizzazione del fattore umano è un elemento imprescindibile per la costituenda **Agenzia per la Cybersicurezza Nazionale**. Nella stessa sede il Sottosegretario Gabrielli ha, per altro, evidenziato che una delle principali difficoltà riscontrate per la partenza del **CVCN** (Centro di valutazione e Certificazione Nazionale) è stata proprio la difficoltà di reperire sul mercato figure professionali con adeguati profili e con le giuste competenze nonché disposti a lavorare per la pubblica amministrazione.

La limitata capacità di formare

figure professionali e la limitata attrattività del settore pubblico

Questo episodio, unitamente alle decine di richieste per profili con competenze cyber che ricevo regolarmente dal mondo imprenditoriale, evidenzia due aspetti: il primo è la limitata capacità di formare figure professionali con queste competenze da parte del mondo universitario e, dall'altro, la limitata attrattività del settore pubblico per figure professionali che possono scegliere fra una pletora di invitanti percorsi e carriere sia in Italia che all'estero.

Per ovviare a questo secondo problema, il D.L. di istituzione della Agenzia di Cybersicurezza prevede uno status per i propri lavorati estremamente competitivo al fine di favorire quella attrattività che, invece, manca nel resto della Pubblica Amministrazione, aspetto questo sicuramente pregevole.

La *cyber-hygiene* minimale

È necessario, però, agire anche sulla offerta andando a promuovere, incentivare, sollecitare il mondo universitario, e più in generale quello della formazione, perché siano formati sia specialisti nel settore della cyber-security sia venga innalzato il livello minimo di competenze specifiche al fine di poter garantire una *cyber-hygiene* minimale. Non dobbiamo dimenticarci, infatti, che ancora oggi quasi il 90% degli attacchi cyber è reso possibili da comportamenti non adeguati da parte degli operatori. Nessuna efficace strategia di cyber-security può quindi prescindere da un innalzamento della "cultura della sicurezza", per usare una locuzione presente nel D.L., sebbene i compiti assegnati all'Agenzia su questo aspetto, come elencati alla lettera v) del comma 1 dell'art .7, appaiono limitati ed andrebbero estesi per coprire oltre

che l’altissima formazione (dottorato di ricerca) anche la **formazione universitaria e professionale**.

L’information sharing è la modalità con la quale le azioni di reazione di un soggetto si tramutano in azioni di prevenzione per un altro

Il cyber space è un dominio estremante pervasivo dove è difficile tracciare perimetri netti e dove le vulnerabilità di un singolo possono riverberarsi sull’intera collettività a causa della presenza di complessi fenomeni di dipendenza ed interdipendenza. Questo impone che le strategie di cyber-security si fondino su un proficuo e costruttivo scambio di informazioni fra i diversi attori coinvolti in quanto soprattutto in questo settore si può affermare, riprendendo la frase usata da un docente del mio Master, che l’information sharing è la modalità con la quale le azioni di reazione di un soggetto si tramutano in azioni di prevenzione per un altro. Da qui la necessità di avere una struttura, come quella delineata dal D.L., formata da competenze di primo piano in grado di dialogare con gli operatori pubblici e privati. Affinché, però, tale dialogo sia efficace e fattibile occorre far crescere le competenze e valorizzare le figure professionali che in ambito privato sovrintendono la gestione degli aspetti di sicurezza. In questi ultimi anni le associazioni di categoria del settore, in primo luogo AIPSA, hanno lavorato molto per evidenziare la necessità che le aziende si dotino di persone con specifiche competenze e professionalità in grado di avere una visione olistica della sicurezza in tutte le sue sfaccettature e come tali porsi quali autorevoli interlocutori nei confronti delle controparti pubbliche. Questo aspetto non appare però ancora adeguatamente coperto da prescrizione legislative con la sola eccezione della figura del Security Liaison Officer presente nella

“vecchia” direttiva sulla sicurezza delle infrastrutture critiche.

La proposta: nella PA percorsi di carriera “riservati” a coloro in possesso di tali competenze

Se nel settore privato qualcosa si sta muovendo, in quello pubblico, come si accennava, la situazione è molto più preoccupante…

Continua a leggere l’articolo su Cybersecurity Italia, su cui l’articolo è stato originariamente pubblicato.

https://www.key4biz.it/agenzia-per-la-cybersicurezza-limportanza-del-fattore-umano-e-della-formazione/367113/

Crackonosh, the malware that attacks gamers

This cryptocurrency mining malware was found in pirated versions of video games such as Grand Theft Auto V.

June 29, 2021 2 min read

This article was translated from our Spanish edition using AI technologies. Errors may exist due to this process.

If you are a gamer , you should be careful of the “pirate” versions of your favorite video games. The cybersecurity company Avast published an investigation carried out by its Threat Laboratory on the discovery of a new malware called

Crackonosh that hides in “cracked” games.

It is a malicious crypto mining program that takes its name from Czech folklore meaning “mountain spirit” and has been circulating since at least June 2018.

According to the investigation, this malware has already generated its authors more than two million dollars in the Monero cryptocurrency, coming from more than 222 thousand infected systems around the world. Avast even warns that in Mexico Crackonosh has already infected 2,200 systems.

The majority of users infected with Crackonosh are from Brazil, the United States, India, the Philippines and Poland, with an average of between 12 and 19 thousand infected systems per country.

Countries affected by Crackonosh / Image: Avast

Crackonosh spreads by getting into “cracked” versions of popular online games. Cracked versions are pirated copies of games that people download to avoid paying for the original versions.

Malware has been found in cracked versions of these games:

- *NBA 2K19*
- *Grand theft auto v*
- *Far cry 5*
- *The Sims 4 Seasons*
- *Euro Truck Simulator 2*
- *The sims 4*
- *Jurassic World Evolution*
- *Fallout 4 GOTY*
- *Call of Cthulhu*
- *Pro Evolution Soccer 2018*

- *We Happy Few*

When Crackonosh is installed, it looks for a way to protect itself, so it replaces critical files on the Windows system and uninstalls some security programs such as Adaware, Bitdefender, Escan, F-secure, Kaspersky, Mcafee (scanner), Norton and Panda.

“Crackonosh is very profitable for attackers and warns of the risks of downloading cracked software. As long as people continue to download cracked software, these types of attacks will continue to be profitable for their authors,” says Daniel Beneš, malware researcher at Avast.

https://www.entrepreneur.com/article/376107

Affrontare le sfide della sicurezza informatica nelle infrastrutture critiche. Il webinar il 7 luglio in diretta

Le utility stanno subendo una massiccia trasformazione e digitalizzazione delle infrastrutture per migliorare l’efficienza e ridurre i costi operativi, ma così diventano anche significativamente più esposti e vulnerabili agli attacchi informatici esterni e interni.

Nel webinar verranno trattati i seguenti temi:

1. Le sfide della sicurezza informatica nelle utility

2. Quali sono le maggiori criticità per la sicurezza informatica delle utility?

3. Quali sono gli approcci alla sicurezza?

4. Il nuovo livello di sicurezza e l’approccio zero trust

5. Le soluzioni di **Atlantica Cyber Security** e **NanoLock Security**

6. Q&A

[embedded content]

Gli speaker

- **Luigi Maracino**, direttore generale di Atlantica Cyber Security, la società di cybersecurity di Atlantica Digital. Ha ricoperto negli anni posizioni apicali nell’ambito della gestione aziendale, lanciando start up di successo. È specializzato nella gestione delle vendite e del marketing focalizzato sulla Cybersecurity.

- **Yanir Laubshtein,** VP Cyber Solutions – **Nanolock Security**. Vanta oltre 20 anni di esperienza lavorativa nel settore della sicurezza informatica in vari ruoli sia per il governo sia per il settore privato, incluso il suo più recente al Cybersecurity & Privacy Impact Center di PwC.
  Yanir ha guidato due progetti strategici del governo in Israele¸ gestendo le operazioni di sicurezza informatica per conto del Ministero dell'Energia e della Water & Sewage Authority e successivamente progettando e gestendo lo sviluppo del C-SOC nazionale israeliano per le infrastrutture critiche.

GUARDA SU YOUTUBE

- Su canale YouTube di **CyberSecurity Italia**, cliccando qui è già possibile impostare il “promemoria” ed avviare la condivisione.

[embedded content]
https://www.key4biz.it/affrontare-le-sfide-della-sicurezza-informatica-nelle-infrastrutture-critiche-il-webinar-il-7-luglio-ore-11-in-diretta/366097/

Joint Cyber Unit (JCU), come cambia e si rafforza la cybersecurity europea. Le 3 novità

Oggi la Commissione europea ha annunciato il piano per la costituzione di una **Joint Cyber Unit (JCU),** che sarà costituita nel 2022 e sarà pienamente operativa nel giugno 2023. Si tratta di un ulteriore passo di una più ampia e completa strategia europea per la cybersecurity, attuata non solo dalle istituzioni UE ma anche dall’apposita agenzia europea per la cybersecurity (ENISA), che alla JCU offrirà supporto. La **Joint Cyber Unit** sarà piattaforma fisica e virtuale di cooperazione, finanziata dalla Commissione.

La Joint Cyber Unit pienamente

operativa nel 2023

L’azione europea sulla cybersecurity è stata tardiva (la strategia complessiva è del 2020 e l’ha adottata l’attuale Commissione, la proposta di una JCU risale al 2019); è tempo di recuperare. Lo fanno gli Stati membri, e l’Italia è un *benchmark*, con le norme in evoluzione sul perimetro di sicurezza cibernetica e la costituenda Agenzia nazionale. Lo fa la Commissione, con una raccomandazione, atto solo formalmente non vincolante gli Stati membri, che individua forme specifiche di coordinamento. Le quali non seguono i percorsi classici della legislazione europea, direttive (all’epoca) o regolamenti (oggi): i tempi legislativi (18-24 mesi) sono necessari per garantire il contemperamento degli interessi dell’Unione, degli Stati e dei popoli (rappresentati da Commissione, Consiglio UE e Parlamento UE, rispettivamente) ma sono poco compatibili con le necessità operative di intervento rapido. E quindi: ‘circolo regolatorio’. Dai mercati nascono le *best practices* che le autorità trasformano in *benchmark* che diventano regole. Da qui nasce l’esigenza dell’agenzia nazionale per la cybersecurity, e si giustifica il coordinamento europeo. Per il quale esistono già le norme e le competenze; esecutive appunto.

Non si tratta di inventare ma di replicare, in parte, modelli esistenti che si sono rivelati efficaci: il sistema di allarme

rapido realizzato con l'agenzia europea per la sicurezza alimentare costituita a seguito di un'altra pandemia ('mucca pazza') ha evitato molte altre crisi, anche più pericolose. Modello che potrebbe replicarsi anche per la sanità (i poteri, la Commissione li ha). E ancora: esiste un esercito europeo, *in nuce*, e un coordinamento europeo di quelli nazionali. Esiste e si è sviluppata sul piano legislativo ma anche giurisprudenziale una competenza unionale e un coordinamento nelle materie della giustizia e degli affari interni. Insomma, competenze dell'Unione che vengono esercitate con 'convinzione progressiva', e che portano a una 'regolazione a cooperazione rafforzata', forma esecutiva di quella prevista dai Trattati europei che ha consentito il superamento del metodo intergovernativo.

Il piano europeo per la cybersecurity: le tre novità

Rispetto al passato, di cui costituisce evoluzione, il piano europeo per la cybersecurity presenta però novità importanti, precipitato delle recenti evoluzioni, regolatorie e dei mercati. Tre esempi, tra tutti. Il primo: la piattaforma di coordinamento delle risposte e di condivisione delle risorse è aperta a polizia anticrimine, agenzie informatiche, strutture diplomatiche, servizi militari, società di sicurezza informatica. E impone, di fatto, un coordinamento analogo anche agli Stati membri: non solo dunque tra strutture pubbliche ma anche private. Regolazione pubblica e privata come vasi comunicanti, dove la prima interviene quando la seconda non è adeguata: sussidiarietà regolatoria, applicata.

Il secondo esempio concerne il sistema di allarme rapido, che non consente solo – come nelle esperienze passate – un intervento di Stati e autorità per limitare il perimetro (del contagio, o dell'attacco) ed evitarne la propagazione, ma prevede un aiuto concreto, immediato e specifico da parte

degli Stati (e delle autorità) non destinatarie degli attacchi a sostegno di chi deve combatterli. Quasi un sistema di 'legittima difesa collettiva' in reazione all'uso della forza (art. 51, Carta delle nazioni Unite). Il cambio di paradigma è evidente, come chiare sono le conseguenze. Entità e dislocazione delle difese sono essenziali sia per reagire nell'immediato agli attacchi, sia per prevenirli, con rapporti regolari sulle minacce, piani di emergenza, accordi di condivisione delle informazioni tra le autorità, e tra queste e le società private di sicurezza informatica.

E veniamo così al terzo esempio della novità dell'intervento: … (***Continua a leggere l'articolo completo su Cybersecurity Italia, dove è stato pubblicato originariamente).***

https://www.key4biz.it/joint-cyber-unit-jcu-come-cambia-e-si-rafforza-la-cybersecurity-europea-le-3-novita/365658/

---

5 Reasons You Shouldn't Trust Your Cyber Defense to Your IT Vendor or Service Provider

Many small and medium-sized businesses utilize IT vendors and service providers to help them with their technology needs. But a business's cyber defense should not be left solely in the hands of these types of firms.

June 23, 2021 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Let me preface this article by saying that I mean no disrespect to IT vendors or managed-service providers (MSPs). For many organizations, these firms are a huge help, economically feasible and do help businesses figure out technical solutions to their problems. In addition to your traditional IT services, many IT vendors or service providers provide basic security services as part of their normal engagement with customers. Many may even offer a separate, more comprehensive security offering for an increased cost.

But if you do use one of these services for your business, consider getting another set of eyes to examine your cyber defenses. Below are five reasons not to fully trust your cyber defenses to an IT vendor or MSP.

1. Tools are a double-edged sword

Behind every good cybersecurity defense is a toolset to make it happen: antivirus, data protection, email defense, backups and more. Often, IT vendors and MSPs tend to use the same tools across many clients because it's what they know and are used to. Unfortunately, if the tools they regularly use aren't that great, then as a client of theirs, you suffer the consequences. This is especially true if you are purchasing licenses for these security tools directly from the IT vendor or MSP. If they stand to make money by selling you a product, then they aren't really putting your best interests first in selecting the best possible tool. Tools are also a double-edged sword because on one hand they are supposed to help your business, but on the other, solely relying on them for your defense would be a huge mistake. There is much more to a good cyber defense than simply installing some tools and hoping for the best.

Related: 4 Major Cybersecurity Risks of Working From Home

2. Security can become an afterthought

I might be generalizing a bit with this one, however, in my opinion, IT vendors and MSPs tend to be focused mostly on technology stability, performance, ease of use and cost savings. Even though there is a place for all those things, security becomes an afterthought or something to be "bolted on" later. In the current digital environment, security should be at the center of technology with all of the above items built around it. Since general IT vendors and MSPs are not security consultants or dedicated security professionals, their mindset will never be equal to that of somebody who focuses solely on cyber defense.

3. They generally have a security "recipe"

The ultimate goal of any cybersecurity effort is to lower the risk of becoming a victim of a cyber attack. No amount of effort will ever reduce the risk to zero, but managing the risk and mitigating it where we can is definitely doable. In my experience, IT vendors and MSPs do not approach cyber defense from a risk perspective. They generally have a security "recipe" to provide you by way of the tools they deploy, as mentioned above. Install these tools and you're now done with "doing security." It doesn't really work that way, unfortunately. Each business is different and often requires a custom effort to adequately address cyber risk. Worth mentioning in this category is the importance of reducing your risk to ransomware and destructive malware. Not all preventative tools and measures are created equally when dealing with these threats, so don't cut corners and simply go with what your IT vendor has offered you.

Related: The One Cybersecurity Risk You're Probably Not Even

Thinking About

4. Many lack the necessary experience

The truth is that attackers have gotten more sophisticated over the years, especially in areas such as phishing and business-email compromise. Nigerian prince scam emails that are easy to spot are not the only nefarious emails your business may encounter. Many IT vendors and MSPs simply lack the experience and expertise to adequately shore up a business's cyber defenses. It's not that they aren't good at what they do, or that they are lacking in other technology-delivery areas; it's just that security is often not their focus or prime objective.

5. Everyone has bias

This is the old saying, "Don't put all your eggs in one basket." Of course, MSPs and vendors will tell you their security solutions are the best. Maybe they use "military-grade encryption" or "artificial intelligence," or pepper their marketing material with "best in class" or other snazzy buzzwords. Okay, if that is the case, then it should pass a third-party review with flying colors. Everyone has bias (including me, of course), but gathering an independent second or third opinion is a prudent move given what is on the line if your cyber defenses fail.

Related: 13 Cognitive Biases That Really Screw Things Up For You

There is definitely a place for MSPs and IT vendors in your overall technology strategy, especially if you don't have a robust internal team to take care of tech problems for you. With or without an internal team, it's always a wise decision to seek third-party counsel for a reality check and an

independent peek at your cyber defenses.

loading…

https://www.entrepreneur.com/article/373581

Akamai cosa fai. Internet è di nuovo down a causa di un Content Delivery Network

Prima Fastly, ora Akamai. Internet è di nuovo in down nell'arco di 8 giorni a causa di un problema tecnico di **Akamai Technologies Inc.**, multinazionale americana che fornisce una piattaforma di Content Delivery Network (CDN). A causa del guasto di Akamai sono andati in tilt i siti Internet delle principali compagnie aeree americane come **American Airlines**, **Southwest Airlines, United Airlines e Delta Air Lines.**

Secondo quanto riporta la CNN, i disagi riscontrati sul web dalle principali compagnie aree americane hanno avuto conseguenze pratiche. La Southwest ha cancellato in due giorni quasi 300 voli e ne ha ritardati più di 500 dopo essere stata costretta a interrompere temporaneamente le operazioni a causa dei problemi tecnici del sito.

Problema Akamai: fuori uso i siti e le app delle principali banche in Australia

Il sito di monitoraggio Downdetector ha segnalato anche siti in tilt di alcune banche australiane come **Commonwealth Bank of Australia** (CBAUF), **Westpac Bank (**WBK) e **Australia and New Zealand Banking Group** (ANEWF) (ANZ). Anche il sito web della Borsa di Hong Kong è stato brevemente offline.

Fonte: Downdetector
Virgin Australia, la seconda compagnia aerea del Paese e coinvolta anch'essa ha dichiarato:*"Virgin Australia è stata una delle tante organizzazioni a subire un'interruzione del sistema di distribuzione dei contenuti di Akamai, stiamo lavorando con loro per garantire che vengano prese le misure necessarie per evitare che si ripetano queste interruzioni"*, ha affermato la compagnia aerea in una nota.

> *Firms now say the problem was with tech provider Akamai https://t.co/SYnZahQIA8*
>
> *— Andrew Beatty (@AndrewBeatty) June 17, 2021*

Contattato per i dettagli sull'origine di questo incidente un portavoce di Akamai ha dichiarato l'azienda è *"Consapevole del problema e stiamo lavorando attivamente per ripristinare i servizi il prima possibile"*. Le fonti indicano che l'interruzione è dovuta a un malfunzionamento del servizio **Prolexic** di **Akamai**, una piattaforma utilizzata dalle aziende per proteggersi dagli attacchi DDoS. Le cause del problema non sono state avanzate nè di qualche un'attacco informatico che avrebbe potuto prendere di mira la rete e l'infrastruttura di sicurezza del provider CDN.

La rete CDN: una rete di dipendenze incredibilmente complessa

Le reti di distribuzione dei contenuti (CDN) sono una parte fondamentale dell'infrastruttura Internet. Queste aziende **(Akamai, CDNetworks, Cloudflare, Amazon CloudFront, Fastly…**) gestiscono reti globali di server cache per migliorare le prestazioni e la disponibilità dei servizi web. Quando sono interessati, è quindi l'accesso a siti Web e servizi Web di tutto il mondo a essere minacciato.

La scorsa settimana proprio Akamai, tramite le dichiarazioni di **Andy Champagne, SVP and chief technology officer of Akamai Labs**, aveva commentato così l'interruzione di Fastly: *"L'infrastruttura Internet è una rete di dipendenze incredibilmente complessa e l'affidabilità non è un caso. Ci vuole una combinazione di tecnologia e persone che lavorano con estrema precisione per assicurarsi che funzioni come una macchina ben oliata*".

Il caso…

https://www.key4biz.it/akamai-cosa-fai-internet-e-di-nuovo-down-a-causa-di-un-content-delivery-network/364928/

Ransomware, potrebbero costare alle aziende 265 miliardi di dollari entro il 2030

Ransomware la minaccia informatica più grande del decennio

Durante il 2020 gli **attacchi di tipo ransomware sono aumentati del +485%,** secondo il "*2020 Consumer Threat Landscape Report*", e la pandemia di Covid-19 non ha fatto altro che peggiorare lo scenario generale della sicurezza informatica, sia delle imprese, sia degli enti pubblici, sia dei singoli utenti di rete.

Anche la cifra del pagamento medio del riscatto ha continuato a salire, con un incremento del +43% tra l'ultimo trimestre del 2020 e il primo del 2021, raggiungendo i 200.000 dollari.

Una potenza di fuoco crescente, questa dei cybercriminali, che nei prossimi dieci anni potrebbe generare **un costo complessivo per le organizzazioni di tutto il mondo pari a 265 miliardi di dollari**. Entro il 2030, si arriverà ad una media di **un nuovo attacco ransomware ogni due secondi**, con un aumento del valore del riscatto in dollari del +30% l'anno.

Il **trend dei costi** legati ai danni e al pagamento del riscatto, dovuti al ransomware, potrebbe registrare una progressione notevole dai **20 miliardi di dollari attesi per la fine del 2021** agli oltre **42 miliardi stimati per il 2024**.

Il lavoro dell'FBI

L'Internet Crime Complaint Center (IC3) dell'**FBI** ha raccolto 2.474 denunce legate a questo tipo di attacchi informatici nel 2020, per un volume di pagamenti di riscatti pari a 30 milioni di dollari circa (sono esclusi altri costi legati agli attacchi e soprattutto non conteggiano i pagamenti dei riscatti non denunciati da parte delle aziende, che potrebbero rappresentare la parte maggiore del bottino per i criminali online).

Secondo stime Mimecast, invece, il 60% delle imprese ha subito un attacco ransomware durante l'ultimo anno, per un media di sei giorni di blocco delle attività. Le categorie più prese di mira sono quelle del manifatturiero, del retail online, l'industria dei servizi, ma anche il sistema sanitario e le imprese del settore energetico.

Esempio concreto di quanto siano pesanti le conseguenze di queste operazioni cybercrime di livello globale sono gli attacchi alle infrastrutture dell'utility **Colonial Pipeline** e della multinazionale **JBS**, oppure al **sistema sanitario nazionale irlandese**, l'Nhs.

L'FBI chiede sempre alle vittime di non pagare i riscatti, perché poi non è certo che si riceva indietro le chiavi per

decrittare i file sequestrati. Suggerimento seguito dall’80% delle organizzazioni, secondo un sondaggio eseguito da Threatpost, anche perché nella stragrande maggioranza dei casi al primo segue sempre un secondo attacco.

Chi paga potrebbe essere catalogato come “preda facile”, tant’è che circa l’80% di chi ha subito un primo attacco ha poi dovuto sostenerne anche un secondo e nel 50% dei casi è sempre lo stesso gruppo di cyber criminali.

Come il ransomware danneggia un’impresa

Secondo stime Cybereason, nel 65% dei casi di attacchi ransomware si registrano perdite di dati ed economiche, mentre nel 25% dei casi si arriva addirittura alla chiusura dell’azienda. Nel 53% dei casi, inoltre, si è registrato un danno al brand e alla reputazione online, nel 32% infine l’organizzazione ha dovuto affrontare una fuga di personale specializzato e di competenze elevate a livello manageriale.

https://www.key4biz.it/ransomware-potrebbero-costare-alle-aziende-265-miliardi-di-dollari-entro-il-2030/364849/

La cybersecurity all’improvviso in cima alle agende del Governo e della

Nato. Le 5 novità

Quella appena trascorsa è stata la settimana con 5 novità che determineranno il settore della cybersecurity a livello nazionale ed internazionale per i prossimi anni.

Ecco quali sono:

- **Paesi Nato, alleati anche contro attacchi cibernetici**
- **È stata istituita l’Agenzia per la Cybersicurezza Nazionale (ACN)**
- **Il Governo italiano ha aggiornato l’elenco dei soggetti del perimetro di sicurezza cibernetica nazionale**
- **In Gazzetta ufficiale è stato pubblicato il secondo DPCM del Perimetro di sicurezza nazionale cibernetica per disciplinare l’obbligo di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici ed introduce le misure per garantire elevati livelli di sicurezza.**
- **Infine, è cambiato anche il vertice del COPASIR, Aldolfo Urso (FdI) è il nuovo presidente e Federica Dieni (M5S) vicepresidente.**

Nato, l’articolo 5 invocabile in caso di attacchi informatici e mutuo soccorso tra i Paesi alleati

Se non ci fossero stati l’hack del **Colonial Pipeline**, il cui attacco a maggio aveva portato al blocco della più grande rete di oleodotti degli Usa, e il cyberattacco alla **JBS**, causando la riduzione del 22% dell’industria della carne USA in pochi giorni, il presidente degli Stati Uniti non avrebbe posto la cybersecurity tra i temi principali della sua agenda, ricordiamo che Joe Biden aveva ‘dimenticato’ la sicurezza cibernetica nel suo piano di 2mila miliardi di dollari.

Dopo questi gravi episodi, Biden ha sia chiesto al Dipartimento di Giustizia Usa di elevare le indagini sugli attacchi ransomware a una priorità simile a quella del terrorismo e poi ha proposto ed ottenuto di estendere l’articolo 5 del Trattato Nato anche in caso di attacchi cibernetici. Quest’ultima novità è contenuta nel comunicato congiunto dei capi di Stato e di Governo a conclusione del recente summit a Bruxelles in cui il Patto Atlantico è stato rinsaldato e aggiornato alle nuove sfide tecnologiche e all’attuale scenario geopolitico, con Cina e Russia “sorvegliati speciali”.

“Riteniamo che gli attacchi informatici verso, dallo o all’interno dello spazio rappresentino una chiara sfida alla sicurezza dell’Alleanza, il cui impatto potrebbe minacciare la prosperità, la sicurezza e la stabilità nazionali ed euro-atlantiche e potrebbe essere dannoso per le società moderne quanto un attacco convenzionale. Tali attacchi potrebbero portare all’invocazione dell’articolo 5. Una decisione su quando tali attacchi porterebbero all’invocazione dell’articolo 5 sarebbe presa dal Consiglio Nord Atlantico caso per caso”, è scritto al punto 33 del comunicato.

L’Agenzia per la cybersicurezza nazionale

La sua creazione è stata annunciata l’8 aprile scorso da **Franco Gabrielli**, Sottosegretario alla Presidenza del Consiglio con delega agli 007, in questa intervista esclusiva di Cybersecurity Italia. Il 14 giugno è stato pubblicato in Gazzetta ufficiale il decreto legge che istituisce l’Agenzia per la cybersicurezza nazionale, voluta da Gabrielli, e definisce l’architettura nazionale di cybersicurezza.

Alzato il livello di resilienza cibernetica degli attori maggiormente sensibili ai fini della sicurezza nazionale

Ieri, il Governo ha alzato il livello di resilienza cibernetica degli attori maggiormente sensibili ai fini della sicurezza nazionale

Il Presidente del Consiglio, Mario Draghi, a seguito della proposta formulata dal Comitato interministeriale per la sicurezza della Repubblica, ha firmato l’aggiornamento dell’elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. È stato, così, previsto un allargamento dell’ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che, complessivamente, esercitano, attraverso reti, sistemi informativi e servizi informatici, 223 funzioni essenziali dello Stato, ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche. Allo stesso tempo, si è provveduto ad un affinamento di alcune funzioni e servizi essenziali dello Stato già ricompresi nel perimetro.

Nei prossimi giorni, il Dipartimento delle informazioni per la

sicurezza provvederà a darne comunicazione agli interessati che, entro sei mesi, saranno tenuti a comunicare le reti, i sistemi informativi ed i servizi informatici che impiegano rispettivamente per l'erogazione delle funzioni e dei servizi essenziali dello Stato inclusi nel perimetro.

Perimetro di sicurezza cibernetica nazionale, in vigore l'obbligo di notifica per le aziende pubbliche e private che ne fanno parte (elenco top secret)

In Gazzetta ufficiale è stato pubblicato il secondo DPCM del Perimetro di sicurezza nazionale cibernetica per disciplinare l'obbligo di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici ed introduce le misure per garantire elevati livelli di sicurezza. Entrerà in vigore il 26 giugno prossimo.

Così, il perimetro di sicurezza nazionale cibernetica inizierà ad essere "operativo" nei confronti dei soggetti inseriti il 22 dicembre scorso. Questi ultimi saranno, quindi, tenuti ad applicare le previste misure di sicurezza e a notificare allo CSIRT italiano gli eventuali incidenti che si dovessero verificare. La lista delle misure di sicurezza e la tassonomia degli incidenti per cui il soggetto è tenuto a notificare sono state pubblicate venerdì scorso, 11 Giugno 2021, in Gazzetta Ufficiale. Per permettere una adeguata organizzazione ai soggetti inclusi nel perimetro per ottemperare alle procedure di notifica di incidenti, queste ultime procederanno in via sperimentale fino al 31 Dicembre 2021.

Da gennaio 2022 le notifiche saranno obbligatorie e inviare entro un'ora o 6 ore da quando il soggetto all'interno del perimetro di sicurezza nazionale cibernetica abbia preso

realmente atto dell’incidente, secondo le categorie indicate dal medesimo DPCM.

Infine, il COPASIR ha un nuovo vertice e svolge un ruolo sempre più centrale anche in merito all’Agenzia per la cybersicurezza nazionale. Aldolfo Urso (FdI) è il nuovo presidente e Federica Dieni (M5S) vicepresidente.

https://www.key4biz.it/la-cybersecurity-allimprovviso-in-cima-alle-agende-del-governo-e-della-nato-le-5-novita/364728/

Energia: sempre più esposte le utility globali ai cyber attacchi, cresce il rischio ransomware

Exploit e nuove minacce informatiche per le aziende

Il termine *exploit* sta ad indicare in via generale un modello di attacco informatico che prende di mira una vulnerabilità specifica di un software, nel tentativo di generare problemi di varia natura al sistema sotto attacco, dalla distribuzione di malware fino al controllo/accesso da remoto del programma in questione, dell’hardware e del dispositivo elettronico.

Secondo un nuovo Rapporto di WhiteHat Security, si è osservato durante gli ultimi mesi che la quantità di tempo in cui le reti energetiche sono esposte ad un exploit sta aumentando

progressivamente. **La “*Windows of Exposure*” o WoE è secondo i ricercatori passata dal 55% di due mesi fa al 67% di maggio 2021.**

L’exploit inoltre rende molto più facile anche l’attacco di **ransomware**, perché maggiore è il numero di vulnerabilità software/hardware maggiore è la possibilità che il numero di attacchi e la loro durata crescano nel tempo.

Le utility nel mirino dei cyber criminali

Di queste minacce abbiamo diversi esempi: Colonial Pipeline, che nelle scorse settimane è rimasta vittima di un pesante attacco ransomware, oppure Eletrobras, la più grande compagnia elettrica dell’America Latina, insieme al fornitore elettrico Companhia Paranaense de Energia (Copel), che hanno subito un altro attacco ransomware a febbraio di quest’anno, con la decisione di sospendere temporaneamente le attività.

La proliferazione di tecnologie di rete, dell’Internet delle cose e dei dispositivi OT, *Operation Technology* o tecnologia operativa (l’uso di hardware e software per monitorare e controllare processi fisici, dispositivi e infrastrutture), ha reso le società energetiche e le utility molto più esposte ai cyber attacchi che in passato.

Basti pensare che nel caso della **Bonneville Power Administration**, agenzia federale che gestisce la rete elettrica di otto Stati americani (Washington, Idaho, Montana, Wyoming, Utah, Nevada e California), a fine 2020 circa i due terzi delle oltre 100 vulnerabilità informatiche individuate dal team per la cybersecurity del Dipartimento dell'Energia degli Stati Uniti nello Stato dell'Oregon ancora erano da sistemare.

Le vulnerabilità

Secondo il Rapporto Clusit 2021, il settore dell'energia e delle utility è uno dei più bersagliati: **nella prima parte del 2020 gli attacchi a centrali elettriche, idriche e gasdotti sono aumentati del +85%** rispetto allo stesso periodo del 2019.

Il 56% delle imprese del settore energetico, inoltre, deve migliorare la protezione dei dati, mentre nel 44% dei casi la gestione degli asset digitali avviene ancora manualmente, secondo stime Minsait. Tutte aree di intervento su cui si deve e si può fare molto di più per alzare il livello di cybersecurity nelle società del settore energy.

https://www.key4biz.it/energia-sempre-piu-esposte-le-utility-globali-ai-cyber-attacchi-cresce-il-rischio-ransomware/364709/

OliCyber, Tiesse gold sponsor delle olimpiadi nazionali di cybersicurezza

Si concluderà domani con la finale nazionale la prima edizione di **OliCyber**, il primo programma di addestramento e competizioni in cybersecurity interamente dedicato agli studenti degli istituti superiori di secondo grado.

L'iniziativa, organizzata dal Laboratorio Nazionale di Cybersecurity del **Cini** (Consorzio Interuniversitario nazionale per l'informatica) ha coinvolto 185 istituti superiori di II grado, permettendo l'avvicinamento al campo della sicurezza informatica di ben 1107 aspiranti hacker etici. Attraverso attività formative mirate e un percorso unico di affiancamento con i maggiori esperti del Paese, i partecipanti hanno potuto perfezionare le loro competenze in un ambito sempre più centrale nella nostra quotidianità e nel mercato del lavoro.

Le premiazioni si terranno lunedì 14 giugno alle 14:30, alla presenza delle autorità, della direzione del Laboratorio Nazionale di Cybersecurity e degli sponsor, Autostrade per l'Italia come platinum e **Tiesse** come gold, che hanno sostenuto e reso possibile l'iniziativa. La cerimonia sarà trasmessa in streaming su YouTube.

Il programma si è avvalso dell'esperienza maturata in anni di fortunate edizioni di CyberChallenge.IT, la scuola per gli hacker etici del futuro, e ha visto i giovani allievi impegnati in circa cinquanta ore di formazione avanzata, lungo un periodo di 8 settimane. Tra gli altri, gli argomenti principali al centro delle lezioni hanno riguardato crittografia, reverse engineering, sicurezza della rete e sicurezza delle infrastrutture, coprendo gli ambiti più rilevanti nel complesso settore della cybersicurezza.

Ciascuna competenza acquisita durante il periodo delle lezioni tornerà utile durante la gara finale, sabato prossimo, che metterà alla prova gli studenti che si potranno sfidare in

speciali arene virtuali, e sarà volta a individuare i campioni olimpici italiani della sicurezza informatica. Per arrivare a questo risultato, il Laboratorio ha coinvolto più di 40 istruttori, da 10 dei migliori team Capture-The-Flag italiani, tra gli ex-partecipanti a CyberChallenge.IT e tra i membri della Nazionale Italiana di Cyberdefender – il TeamItaly -, i quali hanno organizzato 130 esercitazioni, oltre a tenere i corsi per i discenti.

"L'obiettivo di questo percorso sarà di creare maggiore coinvolgimento tra i giovani talenti di CyberChallenge.IT, dove i partecipanti hanno tra i 16 e i 23 anni, e quelli ancora più giovani in OliCyber", ha commentato il coordinatore del progetto, **Gaspare Ferraro:** *"Desideriamo che studentesse e studenti abbiano l'opportunità di capire cosa c'è dietro la sicurezza informatica, un mondo che muove infrastrutture cruciali e servizi per l'intero Paese, così che capiscano quanto possono realizzare con la sola forza della determinazione"*.

https://www.key4biz.it/olicyber-tiesse-gold-sponsor-delle-olimpiadi-nazionali-di-cybersicurezza/364195/