Decreto-legge cybersecurity. In Aula il testo che estende il Golden Power al 5G

Nell'Aula di Montecitorio inizia la discussione sul decreto-legge che crea, finalmente, un vero perimetro di sicurezza cibernetica, dotandosi di strumenti normativi che consentono al nostro paese di intervenire in maniera più tempestiva in caso di minacce e pericoli per la sicurezza nazionale provenienti dal cyberspazio.

Infatti, le commissioni Affari costituzionali e Trasporti della Camera hanno concluso l'esame del Decreto-legge cybersecurity affidando ai relatori **Emanuele Fiano** (**Pd**) e **Emanuele Scagliusi** (**M5S**) il mandato a riferire favorevolmente all'Aula. Il decreto-legge dovrà poi passare in Senato e deve essere approvato entro il 20 novembre.

Luigi Iovino (M5S): 'Ora Italia più preparata alle minacce cibernetiche"

"Il parere favorevole della commissione, è un passo importante, che avvicina il nostro Paese ad una nuova mentalità, più preparata e reattiva nei confronti delle minacce cibernetiche". Così il relatore del disegno di legge di conversione del decreto sul Perimetro di sicurezza nazionale cibernetica, **Luigi Iovino** (M5S), dopo il parere positivo al testo, da parte della commissione Difesa di Montecitorio.

"Queste misure, ha continuato Iovino*, "si avvarranno di una stretta sinergia fra Difesa e università, per attrarre giovani promesse del settore cibenenetico e per acquisire studi,*

conoscenze, esperienze e know how, coinvolgendo poli di eccellenza, di ricerca e di produzione nel campo della tecnologia".

Decreto-legge cybersecurity, cosa prevede

Il provvedimento dispone la definizione di un 'Perimetro di sicurezza nazionale cibernetica' rinviando a un Decreto del presidente del Consiglio dei ministri l'individuazione dei soggetti pubblici e privati le cui reti e sistemi informativi e informatici sono necessari per l'esercizio di una funzione essenziale dello Stato. Con un emendamento del Governo sono state inoltre 'recuperate' le norme sul rafforzamento della 'Golden power', con particolare riferimento ai contratti **5G**, varate nel luglio scorso con il decreto Brexit e successivamente decaduto.

Decreto cybersecurity esteso al 5G

Così il decreto-legge cybersecurity estende l'esercizio dei poteri speciali del Governo ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

In particolare, il testo prevede l'obbligo per gli operatori nazionali di notificare al Governo alla stipula di contratti o accordi con soggetti extra europei aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione.

Per questo motivo, lo scorso 5 settembre, il Consiglio dei Ministri, su proposta del Ministero dello sviluppo economico, ha esercitato i poteri speciali in relazione all'acquisto di beni e servizi da parte degli operatori **Linkem**, **Vodafone**, **Tim**, **Wind Tre** e **Fastweb**.

Il decreto prevede, inoltre, che il presidente del Consiglio abbia il potere in caso di crisi cibernetica, su indicazione del **Comitato interministeriale per la sicurezza della Repubblica (CISR)** di intervenire rimuovendo la fonte della minaccia e quindi di reagire ad una minaccia difendendosi ma anche attaccando.

La nuova normativa impone anche l'obbligo di comunicare sempre un attacco informatico, l'obbligo di controllare il procurement di forniture che rientrino nel perimetro di sicurezza cibernetica. Sono previste, infine, sanzioni che possono variare da 200mila euro a 1,8 milioni di euro.

Per saperne di più: 5G

> *Decreto-legge cybersecurity. In Aula il testo che estende il Golden Power al 5G*

Pagamenti elettronici, qual è il livello di sicurezza attuale?

In questi giorni di fervide trattative per il varo della legge finanziaria, i pagamenti elettronici sono sotto i riflettori degli organi di informazione e all'attenzione della classe politica e dei cittadini come mai avvenuto in precedenza.

E’ opportuno ricordare scenari di minacce informatiche che possono inficiare il valore assicurato dall’impiego del servizio di pagamento elettronico, come il caso relativo alle carte *contactless* (senza contatto) e *mobile wallet* (portafoglio mobile)

Nuove vulnerabilità offrono agli hacker la possibilità di aggirare i limiti di pagamento sulle carte contactless **Visa** indipendentemente dal terminale della carta, secondo una ricerca di **Positive Technologies** (Visa card vulnerability can bypass contactless limits.)

In un comunicato stampa del 29 luglio, Positive Technologies ha affermato che i ricercatori hanno testato più volte i difetti con cinque principali banche del Regno Unito e con carte e terminali al di fuori del Regno Unito. Hanno scoperto che i limiti potevano essere aggirati il □□100% delle volte e potevano consentire a un attaccante di rubare dai conti.

Scenario di attacco

L’attacco funziona manipolando due campi di dati che vengono scambiati tra la carta e il terminale durante un pagamento contactless. Soprattutto nel Regno Unito, se il pagamento necessita di un’ulteriore verifica del titolare della carta (che è richiesta per pagamenti superiori a 30 sterline nel Regno Unito), le carte risponderanno “Non posso farlo”, il che impedisce di effettuare pagamenti oltre questo limite. *In secondo luogo, il terminale utilizza impostazioni specifiche del paese, che richiedono che la carta o il portafoglio mobile forniscano un ulteriore verifica del titolare della carta, ad esempio inserendo il PIN della carta o l’autenticazione tramite impronta digitale sul telefono*“, si legge nel comunicato stampa.

I controlli sono stati aggirati utilizzando un dispositivo che fungeva da proxy per intercettare la comunicazione tra il terminale di pagamento e la carta, un attacco noto come man in the middle (MITM). Questi attacchi MITM possono anche essere eseguiti utilizzando i portafogli mobili, consentendo a un truffatore di caricare fino a £ 30 senza sbloccare il telefono.

La sicurezza dei pagamenti elettronici

Secondo il comunicato "*Il dispositivo dice alla carta che la verifica non è necessaria, anche se l'importo è superiore a £ 30. Il dispositivo quindi comunica al terminale che la verifica è già stata effettuata con altri mezzi. Questo attacco è possibile perché Visa non richiede che gli emittenti e gli acquirenti dispongano di controlli che blocchino i pagamenti senza presentare la verifica minima*".

"L'industria dei pagamenti ritiene che i pagamenti contactless siano protetti dalle garanzie che hanno messo in atto, ma il fatto è che le frodi sono in aumento. Sebbene si tratti di un tipo di frode relativamente nuovo e al momento potrebbe non essere la priorità numero uno per le banche, se i limiti di verifica senza contatto possono essere facilmente aggirati, ciò significa che potremmo vedere perdite più dannose per le banche e i loro clienti.", secondo il comunicato.

Salvaguardia e raccomandazioni

I ricercatori Positive Technologies suggeriscono che gli utenti di carte contacless devono essere vigili nel monitorare i loro estratti conto bancari per rilevare tempestivamente le frodi e, se disponibili con la propria banca, implementare ulteriori misure di sicurezza come limiti di verifica dei pagamenti e notifiche via SMS.

https://www.key4biz.it/pagamenti-elettronici-qual-e-il-livello-di-sicurezza-attuale/276177/

Should all connected cars have a physical network kill switch?

Aurich Lawson / Getty

reader comments

114 with 79 posters participating, including story author

Share this story

Connected cars should come with a kill switch. That’s the take-home message—and the title—of a report by the group Consumer Watchdog. Software increasingly defines the vehicles we drive, and software can be exploited by nefarious people for nefarious means. The problem is compounded by the fact that automakers rely on software written by third parties, including open source software that is riddled with security holes, it says.

Therefore, to prevent “a 9/11-like cyber-attack on our cars,” the report calls for physical “kill switches” to be built into new cars to allow them to be completely disconnected from the Internet. If carmakers don’t agree to the report’s recommendations by year’s end, then “legislators and regulators should mandate these protections,” it says.

Yes, there’s a modem in your new car

You may have noticed that it’s becoming increasingly difficult to buy a new vehicle that doesn’t feature an embedded modem in it. The benefits of a connected car are various, we’re told. It enables onboard telematics that the car maker can use both to improve future products and to allow features like predictive maintenance alerts. And an Internet connection to the infotainment system opens up streaming media services alongside more traditional platforms like FM or satellite radio. In Europe, an onboard modem that can call emergency services in the event of a serious crash has been mandatory since last year.

Depending on the car, you can do a lot more. I’m pretty sure every battery-electric vehicle has a smartphone app that lets you control charging and climate settings. And many more cars (with all kinds of powertrains) have apps that let you monitor and even geofence a car. Some new cars have APIs that are accessible to services like Alexa, and an industry-wide fascination with AI is driving digital assistants and of course autonomy itself. All of this is enabled by wireless connection to the outside world, and it involves some pretty deep hooks into the innards of a car—stuff like the brakes, for instance.

Unfortunately, much of the basic internal network that connects the different bits of a car—called a CANbus—was set in stone in the mid-1990s. And much like the cyberpunk fiction of the period, no one really grasped that everything was about to go wireless. As we’ve learned ever since, if you connect a system to the Internet and you don’t make it secure, someone can come along and hack it.

Consumer Watchdog’s report explains this in great depth. It quotes Linus Torvalds on why Linux should never be trusted

with a nuclear power station and explains some potential methods of attacking a connected car. It details car hacks of the past such as the infamous Miller and Valasek Jeep hack, and it reprints excerpts from investor communications from companies like Tesla and GM that acknowledge the risks a hacking incident could cause to the company share price.

But the report is curiously ill-informed on some matters and positively misguided in others. And the picture it paints of the industry—as secretive and sleepwalking into danger—doesn't really reflect the state of the industry as it is today.

"When we talk about the car, I think what's interesting is that the OEMs and tier one suppliers have taken security very seriously," said John Wall, SVP at Blackberry and head of its QNX activities. "If I look back three or four CESes past, there was a lot of emphasis on autonomous drive. Then the Jeep hack happened. It changed the industry overnight. The next year at CES, everybody was coming to us and asking us, "OK, we know you have an ASIL-D certified product. We know you know how to do Functional Safety. What's your security story?" Companies went out and bought security companies. I mean, some of the reaction was knee-jerk," he told Ars. "But the point was, people were taking it seriously. I don't know that they exactly knew. I mean, the reality is, if you look at the Jeep hack, this wasn't a sophisticated hack. This was 'the doors were left wide open,'" Wall said.

Modern cars have modern security on them

As Wall noted, the Jeep hack was possible because the point of entry—its infotainment system—was developed before anyone thought it would one day be connected to the Internet. "The only way you could break into that head unit was physically. At that point, who cares? I mean, if you're inside the vehicle, you can do whatever you want, but then they added a

module to it. And suddenly, you had a connected unsecured device. So the first step was for a lot of the OEMs to look at their current crop of devices and say, 'OK, what are the steps we need to take to at least close the open doors?'"

"Putting in passwords, encryption, Secure Boot—all these different things have followed. But now what we're actually seeing in the industry is the architecture of the vehicle itself is changing. And we're seeing things like gateways get put into place, separating non-safety buses from safety buses. So there's a lot of effort going into re-architecting the vehicle from how the buses are actually connected through to issuing certificates for modules that need to authenticate; the level of sophistication is getting much higher," Wall told Ars.

All of that sounds sensible, but not to Consumer Watchdog. The report gives modern connected device security scant mention beyond a throwaway paragraph on gateways, which it says are "responsible for ensuring only authorized communication can reach the safety-critical systems. While this would seem to solve the problem, it really only adds more complexity. A successful attack must pass through the gateway unit, requiring a more sophisticated attack. However, the additional hardware and software in the gateway unit also create more opportunities for hackers to find vulnerabilities."

If you have to flip a kill switch in your own car, it's too late

As an observer of the industry over the past few years, I have to agree with Wall's assessment—the Jeep hack certainly woke everyone up. When we launched our car section in 2014, it was extremely difficult to get any OEM to talk about the topic of cybersecurity. These days, car companies like GM will even let journalists like me meet their Red Teams, who spend their days finding creative ways to compromise new systems before the

cars are unleashed on the public. There's an Auto-ISAC, where the industry meets to share threat intelligence. And there has been a proliferation of cybersecurity companies pitching their services to the auto industry, with more than a few acqui-hires.

And even as the automotive threat surface expands, we've yet to see much evidence of malicious actors targeting cars. Why bother going after a car for a bitcoin or two when you could ransomware some hospitals, 23 Texas local agencies, Georgia's court system, Baltimore City government, or a Chinese shipping company? In fact, the only automotive ransomware event we've covered in the past few years was a WCry infection at one of Honda's Japanese factories.

If criminals want to ransom cars, they'll do it by going after someone who can afford to pay them, and that means the OEMs, not end users. And in turn, any kill switches need to be (and indeed are) at that level. Because by the time a driver realizes she needs to turn off the Internet connection to her compromised car, it's already too late. Sadly, most of the recommendations in the Consumer Watchdog report are similarly well-meaning but misguided; I'm not sure the authors would get any industry to agree that "CEOs… should sign personal statements and accept personal legal liability for the cybersecurity status" of whichever company they asked, other than perhaps an actual cybersecurity company. But if the aim was to get people talking about a topic that has very low public consciousness, it might have worked.

https://arstechnica.com/?p=1587835

Cybercrime, il 66% delle PMI subisce attacchi. Phishing l'arma più usata

Il sondaggio annuale **Ponemon sulle PMI** (*2019 Global State of Cybersecurity in Small and Medium-Sized Businesses)* è interessante in quanto cerca specificamente attacchi mirati.

Ci si aspetterebbe che il numero degli attacchi alle PMI cresca su tutta la gamma possibile man mano che gli strumenti di hacking automatizzati diventano più diffusi, invece gli attacchi registrati nel sondaggio sono sofisticati e coinvolgono azioni come il phishing mirato a e-mail di un dipendente o l'ottenimento di dati aziendali specifici.

Il sondaggio di quest'anno ha incluso 2.391 professionisti della sicurezza IT e decisori di aziende situate negli Stati Uniti, nel Regno Unito e in tutta Europa. Le aziende variano da 100 a 1.000 dipendenti e i dati sono stati raccolti in agosto e settembre.

I nuovi attacchi sembrano concentrarsi sulle PMI in regioni specifiche, con gli Stati Uniti che ottengono il peggior risultato. Il numero complessivo di attacchi globali alle PMI è rimasto abbastanza stabile, forse addirittura leggermente diminuito (passando dal 67% nel 2018 al 66% nel 2019). Ciò avviene dopo anni di crescita costante e significativa; dal 55% nello studio inaugurale nel 2016 al 61% nel 2017.

Il tipo di attacco globale più comune è il phishing, di cui il 57% delle PMI globali è stato vittima nello scorso anno. Anche i dispositivi rubati e compromessi (33%) e il furto di credenziali (30%) sono vie comuni di attacco.

La perdita di dati è il risultato più comune degli attacchi informatici alle PMI. Il 69% delle aziende negli Stati Uniti che hanno risposto ha perso informazione personale sensibile appartenente a dipendenti o a clienti. È un aumento del 50% da quando è stato condotto il primo sondaggio Ponemon nel 2016.

Le tecnologie

Le nuove tecnologie sembrano essere uno dei principali fattori alla base di questi attacchi. Gli sviluppi relativamente recenti come i dispositivi Internet of Things (IoT), la biometria e l'uso di dispositivi mobili personali per il lavoro sono stati rapidamente e ampiamente adattati dalle PMI. Ma le tecnologie e le pratiche di sicurezza tendono a rimanere indietro in queste aree.

Le aziende sembrano esserne consapevoli, ma sentono di non poter fare nulla al riguardo. Il 49% degli intervistati ritiene che l'uso di dispositivi mobili con applicazioni business-critical abbia indebolito la postura di sicurezza dell'organizzazione.

L'80% ritiene che i dispositivi IoT non garantiti possano portare a un incidente catastrofico sulla sicurezza, ma solo il 21% di queste aziende sta monitorando attivamente questi dispositivi. Il 75% degli intervistati ha implementato la biometria nel proprio profilo di sicurezza o intende farlo presto.

Benefici del GDPR

Grazie all'influenza del Regolamento generale sulla protezione dei dati (GDPR), varie regioni d'Europa hanno riferito di una maggiore fiducia nella loro postura di sicurezza e hanno dovuto gestire meno attacchi informatici nell'ultimo anno.

La regione **DACH** (Austria, Germania e Svizzera) ha

effettivamente la migliore postura di sicurezza dell'IoT, sebbene i numeri complessivi siano ancora relativamente bassi. DACH ha guidato tutte le altre parti del mondo con il 27% delle loro PMI che conduce formazione sulla sicurezza IoT per dipendenti e fornitori e il 25% monitora attivamente i dispositivi IoT utilizzati sul posto di lavoro per violazioni dei dati.

Tuttavia, queste aziende hanno anche espresso la minima preoccupazione per le password dei dipendenti, con solo il 58% che ha risposto che si trattava di un problema di sicurezza.

Benelux (Belgio, Lussemburgo e Paesi Bassi) ha registrato uno dei tassi più bassi di attacchi informatici contro le PMI. Questa regione aveva un'alta enfasi sulla sicurezza delle password complesse (68%) e ha guidato gli intervistati nell'implementazione della biometria (51%).

In Scandinavia il 64% delle PMI ha subito attacchi informatici e il 71% di queste ha riferito che malware o exploit sono riusciti a superare la propria sicurezza.

La Scandinavia è stata anche l'unica regione a concentrarsi principalmente sulla protezione della proprietà intellettuale, mentre altre regioni hanno dato la priorità alla protezione dei dati dei clienti.

Futuri scenari di sicurezza per PMI

Questi rapporti annuali chiariscono che se c'è un bersaglio vulnerabile là fuori, ci sarà un hacker interessato ad esso, non importa quanto piccolo possa sembrare. Sebbene le PMI non affrontino lo stesso profilo di rischio che devono affrontare le grandi organizzazioni aziendali (come attacchi provenienti da parte di gruppi di **APT** sponsorizzate da stati), tuttavia affrontano abbastanza attacchi informatici che un piano di prevenzione e risposta è vitale.

https://www.key4biz.it/cybercrime-il-66-delle-pmi-subisce-attacchi-phishing-larma-piu-usata/275600/

Jack Ma: ‘Alibaba subisce 300 milioni di attacchi informatici ogni giorno’

“***Alibaba*** *subisce circa 300 milioni di tentativi di attacchi informatici al giorno*“. A dirlo è **Jack Ma**, il fondatore ed ex Presidente del colosso cinese del commercio elettronico, ritirato da Alibaba il mese scorso 20 anni dopo la fondazione dell’azienda.

Ieri, a Singapore, ha ricevuto il **Malcolm S Forbes Lifetime Achievement Award** per i suoi “eccezionali” contributi all’imprenditoria. E’ il primo imprenditore del settore Internet a vincere il premio.

Ma, durante la premiazione, ha affermato di essere “orgoglioso” del fatto che, nonostante la sfilza di attacchi informatici, **Alipay** – la piattaforma dei pagamenti del gruppo che riporta quasi 1 miliardo di utenti ed elabora transazioni per un valore di 50 miliardi di dollari al giorno – gli hacker non sono riusciti ancora a rubare “un centesimo”.

AI: Alibaba Intelligence

A febbraio Alibaba ha dovuto affrontare un vasto tentativo di attacco informatico, che ha minacciato di compromettere i conti di 20 milioni di utenti sul suo sito di eCommerce di **Taobao**.

Ma ha citato le capacità tecnologiche avanzate dell'azienda, che ha soprannominato "**AI: Alibaba Intelligence**", per il suo continuo tasso di successo, osservando che le macchine sono superiori agli umani nell'usare la logica per contrastare i criminali informatici.

"*Insegniamo alla macchina tutti i modi in cui le persone (stanno) barando*", ha detto Ma. "*La macchina ricorda milioni di modi di barare, quindi quando iniziamo a barare, la (macchina) sa già che stai barando. In questo modo stiamo proteggendo tutta la tecnologia.* "

Per raggiungere questo grado di accuratezza, tuttavia, Ma ha osservato che la società deve raccogliere ampie parti dei dati dei clienti. Ha sostenuto che ciò ha permesso ad Alibaba di sviluppare tecnologie all'avanguardia di difesa per quanto riguarda la sicurezza informatica.

https://www.key4biz.it/jack-ma-alibaba-subisce-300-milioni-di-attacchi-informatici-ogni-giorno/275341/

Criptovalute, Gram slitta al 2020. Penali in arrivo per Telegram?

Il blocco imposto dalla **SEC** Usa a **GRAM**, la criptovaluta di **Telegram**, potrebbe far slittarne il debutto dai 6 ai 12 mesi.

Un ritardo che potrebbe far scattare delle penali – dato che il lancio era inizialmente previsto per il 24 ottobre – che

imporrebbero il rimborso ai finanziatori.

A bloccarla sul nascere è stata la **Sec** americana (*Securities and exchange commission*). Il motivo? Avrebbe cercato di violare alcune leggi federali.

La Sec ha ottenuto un ordine restrittivo temporaneo venerdì contro Telegram Group e la sua controllata al **Ton Issuer,** colpevoli di aver condotto una presunta offerta di token digitali non registrata negli Stati Uniti che finora ha raccolto oltre 1,7 miliardi di dollari.

Penali in arrivo per Telegram?

In un comunicato stampa, la SEC ha affermato di aver preso questa posizione per "i*mpedire a Telegram di inondare il mercato degli Stati Uniti con token digitali*" che ritiene siano *"venduti illegalmente*".

In base ai termini dell'investimento, Telegram è contrattualmente obbligato a fornire i token ai suoi investitori prima della fine di questo mese, o potrebbe affrontare la possibilità di restituire l'intero importo di 1,7 miliardi di dollari ai suoi oltre 100 investitori.

Come funzionerà Gram, la cripotvaluta di Telegram

Gram è la nuova criptovaluta di Telegram dell'ecosistema **TON**, Telegram Open Network. Il Telegram Open Network è la blockchain che regolerà la diffusione della criptovaluta di Telegram, i cosiddetti «Gram», e le transazioni nella piattaforma tra vari attori.

Si tratta, però, di molto più che una blockchain, o «struttura a blocchi»: come il documento redatto da **Nikolai Durov** specifica già nelle prime pagine, il TON è una «blockchain di blockchain», l'unica struttura che, grazie alle sue mastodontiche dimensioni, alla sua articolazione orizzontale e verticale assieme e all'implementazione di molte altre tecnologie proprietarie, può permettersi di mantenere la frequenza delle transazioni alla folle cifra di milioni di unità al secondo.

Una volta rilasciati i Gram, Telegram ha affermato che la criptovaluta sarà governata, appunto, da una rete decentralizzata di computer che non darà alla compagnia il controllo, che ricordiamo è una società senza scopo di lucro.

https://www.key4biz.it/criptovalute-gram-slitta-al-2020-penali-in-arrivo-per-telegram/275246/

Vaticano, il nuovo 'angelo custode' del Papa è un esperto cyber

Il nuovo capo dei gendarmi vaticani è un ingegnere di 45 anni che vanta una notevole esperienza nel settore della cybersecurity.

Si **Gianluca Gauzzi Broccoletti** e **Papa Francesco** lo ha scelto per la successione di **Domenico Giani**, il comandante dimessosi il 14 ottobre.

Giani si è dimesso dopo che era stato informalmente accusato di non aver trovato la persona che la settimana scorsa aveva

fatto trapelare alla stampa i nomi di cinque funzionari vaticani coinvolti in un'indagine interna su alcuni investimenti immobiliari.

Il profilo di Gianluca Gauzzi Broccoletti

Originario di Gubbio (PG), 45 anni, laureato in Ingegneria della Sicurezza e Protezione presso l'Università "La Sapienza" di Roma, Gauzzi Broccoletti è stato assunto presso il Corpo della Gendarmeria nel 1995.

Dal 1999 – riferisce in un comunicato la Sala Stampa della Santa Sede, è stato responsabile della progettazione e sviluppo dell'infrastruttura di tecnologia di networking e di sicurezza dello Stato della Città del Vaticano e di CyberSecurity. La schermatura dei conclavi del 2005 e 2013 che ha reso impermeabile a qualsiasi interferenza esterna le sedi del Vaticano è opera sua.

La carriera

Nel 2010 – si legge nel comunicato – è stato trasferito al Centro Operativo di Sicurezza, avanzando gradualmente nelle responsabilità e nei corrispondenti livelli fino a raggiungere la qualifica di Dirigente nel 2017 e di Vice Direttore e Vice Comandante nel 2018.

Ha accompagnato il Sommo Pontefice in numerosi Viaggi Apostolici e nelle Visite Pastorali in Italia e nel mondo. Inoltre ha espletato servizio di coordinamento in occasione dei soggiorni estivi di San Giovanni Paolo II e del Papa emerito Benedetto XVI ed ha svolto il servizio di Vice Comandante del Distaccamento di Castel Gandolfo durante la

permanenza estiva di Papa Benedetto XVI nelle Ville Pontificie.

Un uomo di fiducia

Nel corso degli anni ha instaurato un rapporto di fiducia con le varie Segreterie particolari del Santo Padre, le Superiori Autorità del Governatorato e della Segreteria di Stato, dove è stata richiesta competenza e professionalità per indagini a carattere riservato.

La scelta del papa quindi sarà indubbiamente ricaduta su Gauzzi per motivi di fiducia nei suoi riguardi, per la professionalità e competenza dimostrate durante il suo operato ma si potrebbe davvero rivelare una scelta non casuale se si pensa che si tratta di un esperto di sicurezza.

> *Vaticano, il nuovo 'angelo custode' del Papa è un esperto cyber*

Ransomware, le cyber assicurazioni alimentano il cybercrime?

Il trattamento dei rischi informatici si avvale di differenti opzioni fra le quali emerge la stipula di una cyber assicurazione.

Molti assicuratori inizialmente erano riluttanti a coprire i disastri informatici, in parte a causa della mancanza di dati

attuariali affidabili. Quando proteggono i clienti da rischi tradizionali quali incendi, inondazioni e incidenti automobilistici, stabiliscono una politica dei prezzi basata su informazioni autorevoli provenienti da fonti nazionali e industriali.

Come notato da **Lloyd** in un rapporto del 2017, "*non esistono fonti equivalenti per il cyber-rischio*" e i dati utilizzati per impostare i premi sono raccolti da Internet. È probabile che tali dati disponibili al pubblico sottostimino il potenziale impatto finanziario del rischio informatico per un assicuratore.

Secondo un rapporto della società di consulenza globale **PwC**, sia gli assicuratori e sia le aziende vittime sono riluttanti a rivelare violazioni a causa di preoccupazioni sulla perdita di vantaggio competitivo o danni alla reputazione.

Uno dei disastri informatici in cui può incorrere un'organizzazione e per il quale si stipulano cyber assicurazioni è il materializzarsi di un ransomware, come altresì evidenziato dall'annuale rapporto Internet *Organised Crime Threat Assessment (***IOCTA**) di **Europol**.

Perché pagare un ransom?

Nonostante i costanti avvertimenti delle autorità di contrasto al crimine, secondo cui le organizzazioni non dovrebbero mai pagare richieste di riscatto, esiste la ragionevole possibilità che l'intero sistema di cyber assicurazioni, ora disponibile per le organizzazioni sia grandi e sia piccole, non faccia altro che aggravare il problema. Una recente ricerca di **ProPublica** (*The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*) evidenzia tale fenomeno.

Ogni qual volta venisse erogato un pagamento tramite una assicurazione informatica, si alimenterebbe l'attività criminale e si incoraggerebbero più hacker ad attaccare le aziende e gli enti del settore pubblico per ottenere denaro portando i loro sistemi informatici offline. Di conseguenza, l'assicurazione informatica in questo scenario aumenterebbe e non diminuirebbe i rischi informatici.

Potrebbe sembrare contro intuitivo, ma le compagnie assicurative sarebbero effettivamente incentivate a pagare richieste di riscatto, anche se fossero decine e persino a centinaia di migliaia di euro. Il motivo è semplice: è più economico, più veloce e più semplice sborsare una grossa somma di denaro piuttosto che occuparsi di coprire tutti i costi d'interruzione delle attività e i ritardi del riavvio da zero di un'azienda.

In altre parole, se le compagnie assicurative non pagassero il riscatto, potrebbero essere necessarie settimane prima che un'organizzazione si rialzi e funzioni correttamente.

Nel frattempo, tali compagnie di cyber assicurazioni dovrebbero coprire il costo dei profitti persi durante i tempi d'inattività delle società, nonché i costi dell'assunzione di consulenti IT per ripristinare dalle risorse di backup le attività operative delle società. Quindi, avrebbe più senso sistemare le cose rapidamente e facilmente con un pagamento di riscatto e andare avanti con gli affari.

Qui le cose diventano molto perverse: gli hacker che eseguono attacchi ransomware potrebbero sfruttare questa mentalità, e in particolare prendendo di mira aziende o organizzazioni che dispongono di polizze informatiche per proteggere i sistemi operativi mission-critical. Con semplice calcolo, potrebbero capire le dimensioni della polizza assicurativa informatica, la probabilità che una società debba cedere alle richieste di riscatto e quanto dovrebbero chiedere come parte del riscatto.

L’importo ottimale da richiedere in una richiesta di riscatto sarebbe di 1 € in meno rispetto al costo che una società impiegherebbe per ripristinare i suoi sistemi informatici. Da una semplice analisi costi-benefici, è razionale ed economico pagare il minore dei due mali, specialmente quando è possibile ripristinare il funzionamento dei sistemi in 24 ore o meno (e non giorni, settimane o mesi che potrebbe richiedere il ripristino da un sistema di backup).

Quale futuro per Cyber Assicurazioni?

Tutto ciò, ovviamente, solleva interrogativi sul futuro del mercato delle cyber assicurazioni. Le compagnie assicurative s’impegnando nel raccogliere più premi mensili possibili dalle aziende che acquistano l’assicurazione cyber per proteggersi dall’impatto economico degli attacchi ransomware. Ciò incentiverebbe più hacker a produrre ransomware. L’intero sistema di cyber assicurazioni sarebbe a rischio di implodere su se stesso.

Pagare il riscatto in un attacco di ransomware è la soluzione facile a breve termine, ma a lungo termine renderebbe il problema molto grave. Ora che gli hacker sanno che le aziende stanno stipulando enormi cyber assicurazioni, sanno esattamente a chi rivolgersi.

Con attenta analisi, sanno chi probabilmente pagherà e quanto. In futuro, quindi, potrebbe essere necessario che organizzazioni come l’associazione nazionale delle compagnie assicurative, intervengano e stabiliscano alcune regole di base per l’industria delle assicurazioni.

Le organizzazioni non dovrebbero mai pagare la richiesta di riscatto e gli incentivi devono essere messi in atto per assicurarsi che il pagamento del riscatto non avvenga mai.

https://www.key4biz.it/ransomware-le-cyber-assicurazioni-alimentano-il-cybercrime/274507/

Europol, il cybercrime si evolve in fretta. Il ransomware rimane la principale minaccia informatica

Il crimine informatico continua a maturare spostando la sua attenzione su obiettivi più ampi e più redditizi, per raggiungere un unico obiettivo: i dati personali.

Sono questi i risultati che emergono dalla sesta edizione dell'*Internet Organised Crime Threat Assessment* (**IOCTA**) di **Europol**, l'agenzia anticrimine europea nata nel 1999, uno studio accurato che fornisce informazioni dettagliate sulle minacce emergenti e sugli sviluppi della sicurezza informatica.

Secondo il rapporto, le nuove minacce non derivano solo dalle nuove tecnologie, ma spesso provengono da vulnerabilità già presenti nelle tecnologie esistenti. Le forze dell'ordine – spiega il documento – devono pertanto non solo concentrarsi sul potenziale impatto dei futuri sviluppi tecnologici nel crimine informatico, come l'intelligenza artificiale, ma anche affrontare il crimine informatico in senso olistico, compresa la prevenzione, la consapevolezza e l'aumento della cyber educazione.

“*Alcune minacce di ieri rimangono rilevanti oggi e continueranno a sfidarci domani*“, ha dichiarato **Catherine De Bolle**, direttore esecutivo di Europol.

“L’impatto globale che ha acquisito la sicurezza informatica ha portato la minaccia del crimine informatico ad un altro livello”, spiega De Bolle. “*Serve sviluppare strumenti chiave per tenere sotto controllo i criminali informatici, considerando che altre aree criminali stanno diventando sempre più agevolate dal mondo informatico”.*

Il report evidenzia come quest’anno il ransomware rimane la principale minaccia alla criminalità informatica, seguito dagli attacchi **DDoS**, dal materiale di sfruttamento sessuale dei minori e dai mercati di blockchain, incluso il deepweb. La risposta coordinata agli attacchi informatici su vasta scala rimane una sfida chiave per un’efficace cooperazione internazionale, conclude il rapporto.

Clicca qui per scaricare il report completo IOCTA 2019

https://www.key4biz.it/europol-il-cybercrime-si-evolve-in-fretta-il-ransomware-rimane-la-principale-minaccia-informatica/274370/

Decreto Cybersecurity, Liuzzi: ‘Serve il doppio

delle assunzioni per il controllo delle reti’

Il Governo, con l’approvazione del decreto-legge cybersecurity, crea un vero perimetro di sicurezza cibernetica, dotandosi di strumenti normativi che consentono al nostro Paese di intervenire in maniera più tempestiva in caso di minacce e pericoli per la sicurezza delle reti, dei sistemi informativi e dei servizi informatici pubbliche e private provenienti dal cyberspazio, reti **5G** comprese. E presso il Ministero dello Sviluppo economico (**MiSe**) è stato istituito il Centro di valutazione e certificazione nazionale (**Cvcn**) con il compito di verificare le condizioni di sicurezza dei sistemi destinati alle infrastrutture strategiche. Per far fronte a questa complessa attività del Cvcn è stata prevista l’assunzione di 77 unità presso il Mise, ma quando sarà regime il numero del personale esperto sarà insufficiente. A lanciare l’appello è stata **Mirella Liuzzi**, sottosegretaria al Mise: “*Il numero di funzionari assegnati dalla legge al Cvcn, sebbene rappresenti un contingente numericamente importante in questa fase di start up, potrebbe risultare insufficiente quando il meccanismo di controllo entrerà a pieno regime*”, ha detto nel corso dell’audizione nelle commissioni Affari costituzionali e Trasporti della Camera sul decreto Cybersecurity. “*Pertanto*”, ha aggiunto la sottosegretaria, *“per il futuro ritengo auspicabile che si provveda all’aumento delle unità da destinare al Cvcn, considerando che sulla base di stime effettuate per far fronte alle richieste che arriveranno servirebbero addirittura il doppio delle unità autorizzate”.*

Regolamento per individuare i settori ad alta intensità tecnologica, a che punto sono?

Inoltre, Liuzzi ha fatto sapere che sono *"in stato avanzato di redazione"* le bozze del regolamento per individuare i settori ad alta intensità tecnologica, come previsto dal decreto-legge cybersecurity. La sottosegretaria al Mise ha assicurato anche che il ministero intende operare nell'ambito della sicurezza cibernetica *"con un approccio di salvaguardia degli interessi nazionali",* ma *"previa un'adeguata ponderazione degli interessi di natura commerciale degli operatori e delle imprese, che del resto quotidianamente si interfacciano con la nostra amministrazione".*

Con quale approccio il Mise assicurerà la salvaguardia dei nostri interessi nazionali?

"L'approccio che caratterizzerà l'azione del ministero sarà incentrato sull'assicurare la salvaguardia dei nostri interessi nazionali, in coordinamento con gli altri organismi competenti, previa adeguata ponderazione degli interessi commerciali degli operatori e delle imprese che quotidianamente si interfacciano con la nostra amministrazione", ha concluso Mirella Liuzzi, sottosegretaria allo Sviluppo economico.

Per saperne di più: 5G

> *Decreto Cybersecurity, Liuzzi: 'Serve il doppio delle assunzioni per il controllo delle reti'*