Cybertech 2018, gli esperti di sicurezza lanciano l'allarme. Nel 2017 perso 1 miliardo a causa del cybercrime

Più di 100 aziende, migliaia di partecipanti da oltre 40 Paesi nel mondo: sono questi i numeri della terza edizione di Cybertech Europe 2018, il più importante evento europeo dedicato al settore della cyber security organizzato in collaborazione con **Leonardo** e con l'innovation partner **Accenture**, che si è svolto a Roma il 26 e 27 settembre. La due giorni si è confermata occasione unica per riunire i leader di mercato e i maggiori esperti al mondo, che si sono confrontati sulla visione strategica del panorama presente e futuro e hanno così gettato le basi per affrontare le nuove sfide legate alla sicurezza informatica.

Parole chiave: resilienza e collaborazione. Nel corso dell'evento è emersa l'esigenza reale e concreta di adottare, aziende e istituzioni insieme, un approccio vigile nei confronti dei possibili scenari futuri e di potenziali rischi sconosciuti. Innovazione e strumenti tecnologici appropriati sono gli elementi imprescindibili per prevedere, identificare e affrontare le minacce.

"La rivoluzione parte dall'infrastruttura tecnologica, che è come l'ossigeno nell'aria: non si può farne a meno. È necessario creare un ambiente più resiliente ed essere più preparati; incoraggiare nuove idee, alimentare l'economia,

supportare le startup", ha dichiarato **Amir Rapaport**, Founder e Editor-in-Chief di Cybertech. "*Cybertech Europe rappresenta un palco strategico e prestigioso per far incontrare i guru della cyber security con i protagonisti di questo settore. Roma è il luogo ideale per mettere in contatto le istituzioni con il settore pubblico e privato, raggiungendo una visione comune e condivisa*".

Alessandro Profumo, Amministratore Delegato di Leonardo, ha introdotto la sessione plenaria focalizzandosi sull'approccio proattivo che è necessario adottare per affrontare le sfide di oggi. "*La protezione del dominio cibernetico è un aspetto fondamentale per garantire la resilienza delle infrastrutture critiche, la sicurezza della pubblica amministrazione, delle imprese e del singolo cittadino, la crescita economica di un Paese. Il cyber spazio e la cyber security hanno una rilevanza strategica per Leonardo, impegnata ad assicurare il massimo livello di affidabilità e resilienza mediante l'impiego delle proprie piattaforme e di competenze riconosciute a livello internazionale*".

Gus Hunt, Cyber Strategist Accenture Federal Services, ha parlato di come raggiungere la cyber resilienza. "*Nel combattere il cyber crime finora le organizzazioni hanno avuto un approccio puramente reattivo. Oggi l'87% degli attacchi informatici mirati ai nostri sistemi viene bloccato, eppure ogni anno le organizzazioni subiscono in media ancora 30 violazioni, con un costo medio annuo di quasi 12 milioni di dollari. Dobbiamo cambiare strategia e passare dalla cybersecurity alla cyber resilience, adottando un comportamento proattivo e progettando e costruendo tutti i sistemi in modo che le organizzazioni continuino ad operare malgrado gli attacchi*", ha spiegato.

Inoltre, **Eva Chen**, CEO di Trend Micro, ha spiegato cosa significa vivere in un mondo connesso: *"Siamo tutti connessi ma in qualità di vendor nell'ambito della cyber security, sono piuttosto preoccupata da una quantità così elevata di connessioni. Il 97% delle aziende ha avuto a che fare con malware; entro il 2020 vedremo ben 20 miliardi di oggetti connessi. Le minacce informatiche sono sempre più subdole, ogni mese compaiono 27 nuove famiglie di ransomware e ci aspettiamo che abbiano un impatto crescente su un numero sempre più alto di dispositivi. Inoltre, tali minacce, sono sempre più difficili da individuare per via del machine learning e dell'intelligenza artificiale*".

Eugene Kaspersky, CEO di Kaspersky Lab, ha condiviso la sua vision sul cybercrime e sulle nuove frontiere nella cyber security. È necessario un cambiamento di mentalità rispetto all'approccio tradizionale alla sicurezza informatica. *"Stiamo assistendo a un aumento delle organizzazioni criminali. Qualche numero sulle minacce informatiche: nel 2017 c'è stato un aumento esplosivo per i malware, arrivati a 117.000.000 e in 2 anni è stato sottratto 1 miliardo di dollari (Carbanak). Nell'era in cui il sistema industriale rappresenta uno degli scenari più pericolosi, il costo del cybercrime per l'economia globale all'anno equivale a quello di 4 stazioni spaziali. La mia speranza per il futuro è trasformare la sicurezza informatica in immunità*", ha così commentato.

Rodolfo Rotondo, Business Solutions Strategist, VMware Accelerate Advisory Services, ha illustrato come cloud, mobility e l'evoluzione delle architetture applicative trasformeranno l'approccio alla cyber security: *"La tecnologia da sola non è sufficiente per una protezione efficace delle*

minacce: seguire alcuni semplici principi di igiene cyber ed una educazione sulla consapevolezza del rischi sono elementi fondamentali per una strategia vincente di cyber security".

The post Cybertech 2018, gli esperti di sicurezza lanciano l'allarme. Nel 2017 perso 1 miliardo a causa del cybercrime appeared first on Key4biz.

https://www.key4biz.it/cybertech-2018-gli-esperti-di-sicurezza-lanciano-lallarme-nel-2017-perso-1-miliardo-a-causa-del-cybercrime/233097/

You're Probably Not Even Thinking About One of Social Media's Biggest Dangers

Here's how to protect yourself from identity theft on social media. https://www.entrepreneur.com/article/320172

Accenture, più collaborazione tra CISO e le altre business unit per migliorare la

sicurezza

Ieri **Gus Hunt**, già Chief Technology Officer per la **CIA** e oggi Cyber Strategist di **Accenture Federal Services,** dal palco del **Cybertech Europe 2018 –** la kermesse europea sulla cybersecurity e punto di incontro tra tutti i leader ed esperti provenienti da tutto il mondo – ha in più occasioni ribadito la necessità di quello che lui definisce un "Cyber Moonshot", una chiamata collettiva all'azione e alla massima cooperazione per risolvere le sfide della sicurezza informatica.

Oggi, una nuova ricerca di **Accenture** evidenzia come nel panorama attuale, con la proliferazione di dati sempre più sensibili, l'espansione della connettività e l'adozione di processi automatizzati, i dirigenti e i decision maker IT debbano adottare un approccio diverso alla cyber security per proteggere in modo efficace le aziende da futuri rischi informatici. Benché le aziende abbiano quasi tutte un Chief Information Security Officer (CISO) o un manager di alto livello come un Chief Information Officer (CIO), spesso al di fuori dei loro dipartimenti questi manager hanno un'influenza limitata sulla strategia della sicurezza informatica. Inoltre, quasi la metà dei CISO riconosce che le responsabilità di cui sono investiti per la sicurezza dell'organizzazione crescono più rapidamente della loro capacità di affrontare i problemi ad essa attinenti.

Nello studio "Securing the Future Enterprise Today – 2018," il 73% degli oltre 1.400 dirigenti di C-level intervistati si è detto concorde sul fatto che lo staff e le attività di cyber security vadano distribuiti su tutte le aree aziendali, eppure nel 74% delle aziende la sicurezza informatica è ancora

centralizzata. Ci sono pochi segnali che i dirigenti di alto livello prevedano di decentralizzare la responsabilità in ambito di security. Oggi solo il 25% dei dirigenti non CISO sostiene che i direttori delle business unit hanno anche responsabilità in materia di sicurezza informatica, e una percentuale altrettanto bassa pensa che dovrebbero averla anche in futuro.

Lo studio ha evidenziato una disparità tra quelle che secondo i dirigenti C-level sono le aree di preoccupazione emergenti e le strategie di sicurezza informatica utilizzate per la protezione. Le aziende, ad esempio, stanno facendo ancora poco per diffondere la cultura della cyber security tra i dipendenti e pochissimi CISO hanno l'autorità per influenzare le business unit delle loro organizzazioni.

- Solo metà degli intervistati dichiara che tutti i dipendenti ricevono formazione sulla sicurezza informatica al momento del loro ingresso nell'organizzazione e che vengono regolarmente sensibilizzati sulla questione nel corso della loro permanenza in azienda.
- Sorprendentemente, solo il 40% dei CISO dichiara che istituire o ampliare un programma di protezione dalle minacce interne è una priorità assoluta.
- Solo il 40% dei CISO dichiara di essersi sempre consultato con i direttori delle diverse aree aziendali per capire le esigenze di business prima di proporre un approccio alla sicurezza.

Lo studio di Accenture raccomanda cinque azioni da

intraprendere per garantire resilienza:

1. Fare dei propri leader aziendali dei leader di cyber resilience

La security deve essere tenuta in considerazione quando si definisce la strategia al fine di indirizzare le azioni necessarie a ridurre il rischio.

2. Sostenere il ruolo di business enabler dei leader della sicurezza informatica

Per implementare una resilienza informatica pervasiva sono necessari nuovi ruoli e nuove competenze all'interno dell'azienda.

3. Fare della forza lavoro una parte della soluzione

Le aziende devono prendere atto che i dipendenti sono tra i primi responsabili della cyber security e possono contribuire a aumentare i livelli di sicurezza.

4. Proteggere attivamente i clienti

Al fine di proteggere i dati dei propri clienti le aziende non devono soffermarsi al solo adempimento delle normative vigenti

5. Assicurare protezione all'intero ecosistema

Bisogna lavorare con i propri partner per proteggere tutta la catena del valore e l'ecosistema in cui l'azienda opera.

I principali rischi informatici: nuove tecnologie e condivisione dei dati

I manager di alto livello vedono nella **diffusione delle nuove tecnologie e dei nuovi strumenti un potenziale aumento del rischio informatico** per le loro aziende e percepiscono una crescita dei pericoli legati alla condivisione dei dati con terze parti.

- In cima alla lista c'è **l'Internet of Things**, a cui il **77%** degli intervistati imputa un aumento moderato o significativo del rischio informatico.
- Per il **74%** degli intervistati a elevare il rischio saranno **i servizi cloud**, eppure solo il 44% dichiara che la propria strategia di sicurezza informatica protegge anche l'ambiente cloud.
- **Più del 70%** degli intervistati si aspetta che la **condivisione dei dati con partner strategici e terze parti genererà un aumento del rischio**, ma solo il 39% afferma che i dati condivisi sono adeguatamente protetti dalla strategia di sicurezza informatica dell'azienda su questo fronte.

Per approfondire:

- Per scaricare il report completo "Securing the Future Enterprise Today – 2018" clicca qui.

The post Accenture, più collaborazione tra CISO e le altre business unit per migliorare la sicurezza appeared first on Key4biz.

https://www.key4biz.it/accenture-piu-collaborazione-tra-ciso-e

-le-altre-business-unit-per-migliorare-la-sicurezza/232960/

Carte di credito, la metà delle aziende non rispetta gli standard di sicurezza

Dopo aver documentato i miglioramenti nella compliance al Payment Card Industry Data Security Standard (PCI DSS) nei passati sei anni (2010-2016), il **Payment Security Report 2018 di Verizon (PSR**) adesso rivela un preoccupante trend al ribasso, secondo il quale le aziende non superano la valutazione della compliance a questi requisiti, e, aspetto forse ancor più grave, non riescono ad applicarla appieno.

I requisiti **Payment Card Industry Data Security Standard** (PCI DSS) aiutano le aziende che offrono servizi di pagamento tramite carta di credito a proteggere i loro sistemi di pagamento da violazioni e furti di dati dei possessori delle carte di credito.

E’ stato documentato (attraverso i dati del Data Breach Investigations Report di Verizon) che la compliance agli standard PCI DSS aiuta a proteggere i sistemi di pagamento sia dalle violazioni che dal furto dei dati degli intestatari delle carte di credito, ed è per questa ragione che il trend registrato risulta essere allarmante.

I dati raccolti dal team di Verizon PCI DSS Qualified Security Assessors (QSAs) nel 2017 hanno evidenziato che l’adeguamento ai requisiti PCI tra le aziende a livello mondiale è in calo; solo il 52.4% delle organizzazioni, infatti, ha mantenuto pieno rigore nell’adeguamento ai requisiti nel 2017, una percentuale inferiore se paragonata a quella del 2016, di 55.4%.

Sono state evidenziate le differenze di diverse aree regionali, e ciò che è emerso è che il 77.8% delle aziende appartenenti all’area Asia-Pacifico è propenso alla conformità di questi requisiti di sicurezza, a differenza delle aziende presenti in Europa (46.4%) e in America (39.7%). Le ragioni di tali differenze possono derivare da tempi differenti di applicazione delle strategie di compliance in base all’area

geografica di appartenenza, dall’approccio culturale nella valutazione di premi e riconoscimenti o dalla maturità dei sistemi IT.

Tra i diversi settori economici, i servizi IT restano i migliori per quanto concerne questo aspetto, con tre quarti delle organizzazioni (77.8%) che raggiungono il pieno stato di adeguamento. I settori del Retail (56.3%) e dei servizi finanziari (47.9%) sono molto più attenti rispetto alle organizzazioni del settore hospitality (38.5%), che hanno mostrato il livello di attuabilità della compliance più basso

Dato che diverse aziende spesso sfruttano gli sforzi di adeguamento ai requisiti PCI DSS per raggiungere gli standard di sicurezza imposti dalle normative sulla protezione dei dati, come il Regolamento Europeo per la protezione dei dati personali (GDPR), il gap esistente tra i vari settori economici che offrono quotidianamente pagamenti elettronici è certamente rilevante.

Di seguito, i nove fattori necessari per controllare efficacia e attuabilità, che sostengono i 12 requisiti chiave degli standard PCI DSS:

Fattore 1- Controllo dell’ambiente

L’attuabilità e l’efficacia dei 12 requisiti chiave dipendono da un **Controllo dell’ambiente** corretto.

Fattore 2 – Progettazione dei controlli

Un controllo appropriato dell'operatività, necessario per raggiungere gli obiettivi DSS di controllo della sicurezza, dipende da una puntuale Progettazione dei controlli.

Fattore 3 – Rischi associati ai controlli

Senza una cura continua (test di sicurezza, gestione dei rischi, etc.), l'efficacia dei controlli può scemare nel corso del tempo, e infine venire meno. Per mitigare un'eventuale mancata attivazione dei controlli, è imprescindibile una gestione integrata dei **rischi associati** a questi

Fattore 4 – Solidità dei controlli

I controlli vengono applicati ad ambienti dinamici e caratterizzati da minacce in costante evoluzione. Per questo, devono essere sufficientemente solidi per far fronte a cambiamenti inaspettati, per mantenere funzionalità e utilità verso gli obiettivi (standard di configurazione, controllo degli accessi, hardening dei sistemi, etc.).

Fattore 5 – Resilienza dei controlli

I controlli di sicurezza potrebbero non entrare in azione anche se vengono aggiunti molteplici step per massimizzarne la solidità, dunque la **resilienza** attraverso il rilevamento proattivo e il recupero tempestivo in caso di mancato funzionamento sono essenziali per l'efficacia e l'attuabilità.

Fattore 6 – Gestione del ciclo di vita dei controlli

Per raggiungere gli obiettivi sopra, è necessario monitorare i controlli e gestirli in modo attivo in tutte le fasi del loro **ciclo di vita**, a partire dalla loro creazione fino alla disattivazione.

Fattore 7 – Gestione delle performance dei controlli

Definire e comunicare **gli standard delle performance** per misurare i risultati reali dell'ambiente di controllo ne migliora l'efficacia, promuovendo risultati prevedibili sulla protezione dei dati e sulle attività di compliance, consentendo quindi di individuare tempestivamente un eventuale calo delle performance, e di invertire la tendenza.

Fattore 8 – Valutazione della maturità

Un ambiente di controllo non dovrebbe mai diventare stagnante – al contrario, dovrebbe migliorare costantemente. In quest'ottica, le aziende devono seguire una roadmap, definire un livello di riferimento per i procedimenti, e sviluppare risorse adeguate per monitorarne ottimizzazione e codificazione, come indicatori di quanto i processi di sviluppo siano completi e in grado di migliorarsi costantemente.

Fattore 9 – Autovalutazione

Per raggiungere tutti questi obiettivi è necessaria

un’autonomia interna alle aziende – disponibilità di risorse (professionisti, processi e tecnologia), competenze (processi di supporto), know how (skill, conoscenze ed esperienza) e impegno (determinazione nell’applicare in modo coerente gli standard) – in poche parole, capacità di autovalutazione.

Per scaricare il Payment Security Report 2018 di Verizon clicca qui.

The post Carte di credito, la metà delle aziende non rispetta gli standard di sicurezza appeared first on Key4biz.

https://www.key4biz.it/carte-di-credito-la-meta-delle-aziende-non-rispetta-gli-standard-di-sicurezza/232919/

CyberTech 2018, Gus Hunt (Accenture) ‘Contro il cybercrime serve uno sforzo comune’

Gus Hunt, già Chief Technology Officer per la **CIA** e oggi Cyber Strategist di **Accenture Federal Services,** ha in più occasioni ribadito la necessità di quello che lui definisce un “Cyber Moonshot”, una chiamata collettiva all’azione e alla massima cooperazione per risolvere le sfide della sicurezza informatica. Gus invita i governi, le imprese, il mondo accademico e tutte le parti interessate a lavorare insieme, superando il modello individualista del “ciascuno per sé”. Nel suo intervento a Cybertech Europe 2018, Gus Hunt ha parlato di

come per le organizzazioni sia imperativo abbandonare la logica della cybersecurity e adottare quella della cyber resilience.

“*Nel combattere il cyber crime finora le organizzazioni hanno avuto un approccio puramente reattivo. Oggi l’87% degli attacchi informatici mirati ai nostri sistemi viene bloccato, eppure ogni anno le organizzazioni subiscono in media ancora 30 violazioni, con un costo medio annuo di quasi 12 milioni di dollari. Il mondo è sempre più connesso e le nuove tecnologie, come l’IoT, stanno determinando una crescita esponenziale della superficie di attacco. Il nostro attuale approccio non ci porterà lontano: dobbiamo cambiare strategia e passare dalla cybersecurity alla cyber resilience, adottando un comportamento proattivo e progettando e costruendo tutti i sistemi in modo che le organizzazioni continuino ad operare malgrado gli attacchi. Bisogna diventare il cacciatore, non il cacciato*”, dichiara **Gus Hunt, Cyber Strategist di Accenture Federal Services**.

“*Non possiamo proteggere con successo le nostre infrastrutture critiche finché non affrontiamo la questione del divario tra le organizzazioni che hanno i mezzi finanziari, le risorse e le capacità per investire e proteggere i loro sistemi le piccole e medie aziende che interagiscono con le grandi, ma non hanno i mezzi per garantire la sicurezza ai livelli necessari. Il risultato è che gli attacchi alle infrastrutture critiche arrivano proprio da queste terze parti, che costituiscono un punto di vulnerabilità molto appetibile per il crimine informatico. Il modo più efficace di rafforzare la sicurezza e la resilienza delle nostre infrastrutture critiche è quindi quello di colmare questo divario*”.

The post CyberTech 2018, Gus Hunt (Accenture) ‘Contro il

cybercrime serve uno sforzo comune’ appeared first on Key4biz.

https://www.key4biz.it/cybertech-2018-gus-hunt-accenture-contro-il-cybercrime-serve-uno-sforzo-comune/232842/

La silente guerra degli hacker italiani

C’è una guerra in atto all’interno del panorama internet italiano, una guerra silenziosa di cui i quotidiani praticamente non parlano ma molto importante perché corre sul filo della responsabilità del trattamento dei dati personali. Forse il termine “guerra” potrà sembrare eccessivo ad alcuni di voi, ma permettetemi di snocciolare qualche dato che, sinceramente, dovrebbe far riflettere: a giugno di questo anno sono stati attaccati il sito del Consiglio della Regione Toscana: http://www.consiglio.regione.toscana.it e il sito riguardante il potenziamento delle linee della TAV http://www.e78grossetosiena.it. A luglio sono stati attaccati il Ministero della Salute e il sito che collegava le attività dell’Expo di Milano alle attività commerciali in Basilicata (http://www.daexpoallabasilicata.it). Ad agosto, mentre molti di noi erano sotto l’ombrellone, è stato attaccato il sito della UILM (Unione Italiana Lavoratori Metalmeccanici). Per continuare:

- 12 agosto: data breach con esposizione pubblica di credenziali utenti appartenenti al MEF;
- 7 settembre: data breach con esposizione pubblica di oltre 37.500 account di utenti INAS;
- 11 settembre: data breach con esposizione pubblica di username e password appartenenti al Ministero

dell’Ambiente e del Ministero del Tesoro;
- 16 settembre: data breach con esposizione pubblica di utenze appartenenti all’UNUCI (Unione Nazionale Ufficiali in Congedo d’Italia).

Ne sono previsti altri, entro il cinque novembre per l’esattezza, ma prima di proseguire credo sia giusto chiarire alcuni concetti chiave. Le azioni di cui parliamo si basano, grossomodo, su due tipologie di attacco: il *de facing* ossia la modifica dell’aspetto grafico di un sito in modo che possa apparire come vuole l’hacker, e il *data-breach* che prevede l’entrata in possesso di database da cui estrarre i dati. La tipologia di attacco sembra dimostrare che gli hacker hanno una fitta rete di “aiutanti”, pronti a garantire gli accessi ai dati o, quantomeno, in grado di semplificare le varie operazioni di sabotaggio. È un panorama preoccupante che lascia scoperti alcuni interrogativi ed il principale è *“come mai le protezioni non funzionano?*”.

La protezione non è solo un fattore tecnico, è altresì garantita dalle componenti umane di professionalità, competenza ed etica; questi ultimi spesso dimenticati, sottovalutati o letteralmente ignorati. Dai vari tweet di gruppi hacker come Anonymous Italia o LulzSecITA si scoprono principalmente due aspetti: il primo riguarda le password in uso agli utenti, spesso non in linea con i comuni criteri di sicurezza. Il secondo riguarda le banche dati, popolate da tabelle in cui le credenziali sono “in chiaro”, ossia in cui password dell’utente è leggibile a chiunque ne abbia accesso.

Esistono quindi due facce della stessa medaglia: da un lato c’è l’attaccante che viola la legge con un accesso abusivo al sistema informatico. Dall’altro c’è chi avrebbe dovuto gestire adeguatamente le informazioni e non lo ha fatto. A valle di un attacco c’è sempre un messaggio che lo reclama fornendo dati tecnici interessanti e ci si aspetterebbe provvedimenti legali in entrambe le direzioni, anche per chi non ha protetto adeguatamente tali informazioni. È il caso di Rogue0, l’hacker

che ha ripetutamente penetrato la piattaforma utilizzata dal Movimento 5 Stelle e di proprietà della Casaleggio Associati. L'hacker ha garantito che può accedere alla piattaforma ripetutamente e senza troppi problemi e a poco sono valse le raccomandazioni del Garante sulla Privacy: già dopo il primo attacco la piattaforma era stata data per sicura e invece sappiamo come è finita: il 6 settembre su Twitter appaiono i numeri di cellulare di esponenti del Movimento 5 Stelle e dati di tabelle provenienti dalla piattaforma. Come mai nessuno ha controllato che la falla fosse stata chiusa realmente e la piattaforma fosse davvero sicura e in grado di operare?

Diciamo la verità, in Italia abbiamo un brutto vizio: non controlla nessuno fino a quando non accade qualcosa di spiacevole e chi pensa che questi attacchi hacker abbiano finalità politica sbaglia anche se gli obiettivi sembrano suggerirlo. Questi gruppi hacker hanno lo scopo di detronizzare le istituzioni che vantano sicurezza e perfezione quando, in realtà, non sono in grado di fornirle. A valle dell'attacco all'INAS, il gruppo LulzSecITA ha scritto quanto segue: "**Ancora una volta, l'Istituzione Italiana si mostra incapace di #proteggere i #dati #sensibili dei propri cittadini, mettendo così in serio pericolo le loro vite, e se vogliamo parlare di numeri, sono ben 37.500**."

Alla base vi è la voglia di sbugiardare la sicurezza che molti soggetti istituzionali sembrano palesare e le tecniche adottate per riuscire in questo obiettivo, sono quelle che fanno più male perché mettono a nudo l'incapacità tecnica di difendersi oltre che la scarsa professionalità nella gestione dei dati. In un'intervista al sito Motherboard.it si leggono due risposte molto interessanti dell'hacker Rogue0:

Domanda di Motherboard.it: Hai anche accesso in scrittura al

database?

Risposta dell'hacker: L'accesso è sempre lo stesso quindi sì, in uno dei tweet ho scritto nome e tipo di user e i suoi privilegi, quindi è una cosa pubblica

Domanda di Motherboard.it: Cosa pensi dell'idea della democrazia diretta e del voto elettronico? La tua è anche una battaglia di principi o solo legata al comportamento del partito M5S?

Risposta dell'hacker: Ancora queste domande. 🙂 Questo non è un hack politico, a me del comportamento del partito non frega niente. Se vuoi è una battaglia di principi informatici. Se ti riferisci ai numeri dei ministri è solo perché fanno rumore, a scapito di Davide [Casaleggio, ndr]. Povero Davide. lol

Si evince la totale e reiterata incapacità a proteggere la piattaforma su cui sono ospitati i dati degli utenti. A valle del data breach condotto dal gruppo LulzSecITA su INAS, in molti hanno contestato che alcuni dati erano stati ottenuti utilizzando SQL Map, un penetration test tool parecchio conosciuto da chi si occupa di cyber security. Parliamo di uno strumento che è stato immesso sulla rete nel 2006 e la cui ultima edizione (la 1.1) risale a gennaio 2017. SQL Map è noto per la sua semplicità di utilizzo e altro non fa che lanciare una raffica diversificata di attacchi contro una banca dati per saggiarne la resistenza; per questo motivo, ad esempio, viene utilizzato per testare la qualità e la sicurezza di un sito web. Usare SQL Map per un attacco dovrebbe essere inutile, perché reso inefficace tramite il corretto sviluppo del codice sorgente. Portare e concludere con successo un attacco con tale strumentazione rivela la completa inadeguatezza tecnologica dell'attaccato e la totale

superficialità con cui viene fatta la manutenzione del codice sorgente e dei database. Torniamo al concetto dei controlli: chi scrive ha profondo rispetto e stima per il Garante ma si rende anche conto che probabilmente la struttura di quest'ultimo è pesantemente sotto-organico rispetto a ciò che servirebbe per fronteggiare eventi di questo tipo. Il ruolo del Garante rischia di essere relegato a quello di semplice ammonitore quando invece la completezza delle sue funzioni sono fondamentali per una gestione corretta delle informazioni.



Il cinque novembre si avvicina: il gruppo hacker LulzSecITA ha già lasciato intendere che ci sarà un altro nuovo e pesante attacco, magari anche con la collaborazione di Anonymous. I due gruppi hanno collaborato spesso insieme e lo hanno fatto dando vita ad AntiSec, un nome che racchiude un concetto fin troppo chiaro (Anti Security). È ragionevole pensare che LulzSecITA sia già in possesso delle informazioni e le stia elaborando per presentarle in maniera massiccia in quella data. Il tweet che hanno pubblicato è abbastanza eloquente e cita un passaggio di "La tempesta" (Shakespeare-Angeli) /Atto primo/Scena seconda. Inoltre, come è stato fatto notare più volte su internet (l'ultima dalla Dott.ssa Claudia Cofini), il 5 novembre è una data rilevante:

"Il 5 novembre rimanda anche alle congiure delle polveri di cui uno dei protagonisti è Guy Fawkes, da cui prende ispirazione la maschera di Anonymous e il film V for Vendetta"

Questa guerra, perché di questo si tratta, è nel pieno svolgimento ed obiettivamente trova fondamento sulla superficialità tecnica e professionale di chi dovrebbe tutelare i dati dei cittadini; citando Sun Tzu: "il generale esperto attacca la strategia del meno esperto. Questa è la prima cosa da fare." La speranza è che il vento cambi e che vi sia maggiore senso di responsabilità nel trattare queste

informazioni, tenendo sempre a mente che il valore di un'azienda è data dalle informazioni in suo possesso e speriamo che il vento cambi in fretta.

Riferimenti utili

Intervista dell'hacker R0gue0 al sito Motherboard.it: https://motherboard.vice.com/it/article/3ke8qj/rousseau-hack-rogue0-intervista-movimento-5-stelle

A cura di: **Edoardo Limone**

L'articolo La silente guerra degli hacker italiani proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/la-silente-guerra-degli-hacker-italiani/

Cybersecurity, Trump lancia la nuova strategia nazionale per 'difendere' le elezioni di midterm

Il presidente Trump ha firmato la nuova strategia nazionale di cybersecurity. *"La prima strategia informatica completamente articolata per gli Stati Uniti dal 2003"*, si legge nell'introduzione della "National Cyber Strategy"

L'annuncio è stato dato dal consigliere per la sicurezza nazionale, **John Bolton**: *"Non avremo più le mani legate"*, ha

detto. A cosa si riferisce? L'amministrazione Trump ha abolito la norma dell'era Obama, nota come PPD-20, che ha reso più stringente il processo che consente alle agenzie governative di svolgere gli attacchi informatici offensivi. Secondo Bolton la cancellazione della norma fornisce maggiore margine di manovra per rispondere alle minacce informatiche straniere.

Trump vuole mettere al sicuro le elezioni del 6 novembre, dalle urne il giudizio sulla prima metà del suo mandato

Così, la Casa Bianca ha messo in atto la nuova strategia nazionale di sicurezza informatica per fronteggiare soprattutto gli attacchi hacker in vista delle elezioni di 'midterm'. Infatti martedì 6 novembre, i cittadini americani saranno chiamati a rinnovare tutta la Camera – 435 seggi, i deputati hanno mandati biennali – e un terzo del Senato – 100 seggi, i senatori restano in carica sei anni -, oltre che a votare per numerosi governatori e assemblee statali e a esprimersi su tutta una gamma di referendum e consultazioni locali. Ma l'esito della consultazione sarà soprattutto letto come un giudizio sulla prima metà del mandato di **Donald Trump**, in chiave 2020. Dunque le prossime elezioni potrebbe portare a un intensificarsi dei cyberattacchi, che sono già iniziati. *"Hacker sponsorizzati da governi stranieri hanno preso di mira gli account Gmail di senatori Usa e di loro collaboratori".* Lo ha detto un portavoce di **Google** alla **Cnn**, dopo che il senatore democratico **Ron Wyden** aveva denunciato l'episodio in una lettera all'ufficio per la sicurezza del Congresso. Anche **Microsoft** all'inizio dell'anno aveva identificato e bloccato tentativi di hackeraggio contro tre candidati al Congresso alle elezioni di midterm. L'intelligence americana ha attribuito a Mosca gli hackeraggi ai danni del partito democratico durante le presidenziali Usa del 2016 mentre lo speciale procuratore che indaga sul Russigate, Robert Mueller, ha incriminato 12 militari russi per l'attacco informatico

contro il partito democratico durante le presidenziali. Wyaden ha accusato il Cremlino anche di quest'ultimo cyber attacco.

Gli americani nel cyberspazio *"sono sotto attacco ogni giorno* – ha detto il consigliere per la sicurezza nazionale Usa, *"attori non statali, criminali e terroristici cercano di rubare la nostra proprietà intellettuale e le nostre informazioni personali, cercano di rubare le nostre infrastrutture e anche di indebolire la nostra democrazia",* ha concluso Bolton.

National Cyber Strategy degli Usa in 4 punti

Dunque Trump ha paura di un'interferenza esterna in grado di influenzare il voto del 6 novembre così ha dato vita alla nuova strategia nazionale di cybersecurity. Ecco i 4 punti fondamentali scritti direttamente da Trump nella prima pagina del piano:

1. Difendere la patria proteggendo reti, sistemi, funzioni e dati;
2. Promuovere la prosperità americana alimentando un'economia digitale sicura e prospera e promuovendo una forte innovazione interna;
3. Preservare la pace e la sicurezza rafforzando la capacità degli Stati Uniti – di concerto con alleati e partner – di scoraggiare e, se necessario, punire chi usa strumenti informatici per scopi malevoli;
4. Espansione dell'influenza americana all'estero per estendere i principi chiave di un Internet aperto, interoperabile, affidabile e sicuro.

In sostanza gli obiettivi sono proteggere le infrastrutture critiche e sistemi governativi, combattere il crimine informatico e migliorare la segnalazione degli attacchi coltivando nuovi talenti americani nella cybersecurity.

“Il popolo americano si aspetta che la nostra nazione sia un leader mondiale su tutti i fronti, incluso il cyberspazio. La prosperità e la sicurezza della nostra gente e la conservazione del nostro stile di vita dipendono dalla nostra riuscita di questa strategia. Abbiamo molto lavoro da fare e non c’è tempo da perdere. Faremo l’America a prova di Cybersecurity”, si conclude così l’introduzione del testo della “National Cyber Strategy”.

“La National Cyber Strategy dimostra il mio impegno nel rafforzare le capacità di sicurezza informatica dell’America e nel proteggere l’America dalle minacce informatiche. È un invito all’azione per tutti gli americani e le nostre grandi aziende ad adottare le misure necessarie per migliorare la nostra sicurezza informatica nazionale. Continueremo a guidare il mondo nel garantire un prospero futuro informatico” ha scritto Trump nella presentazione della strategia nazionale di cybersecurity.

Per approfondire:

- National Cyber Strategy, il testo completo in PDF

The post Cybersecurity, Trump lancia la nuova strategia nazionale per ‘difendere’ le elezioni di midterm appeared first on Key4biz.

https://www.key4biz.it/cybersecurity-trump-lancia-la-nuova-strategia-nazionale-per-difendere-le-elezioni-di-midterm/232457/

Sextortion, Polizia Postale ‘In corso massivo spamming a scopo estorsivo via email’

La Polizia Postale ha lanciato l’allarme: *“è in corso una massiva attività di spamming a scopo estorsivo con l’invio di email in cui gli utenti vengono informati dell’hackeraggio del proprio account di posta elettronica ad opera di un gruppo internazionale di Criminali. L’account sarebbe stato hackerato attraverso l’inoculamento di un virus mentre venivano visitati siti per adulti. Da qui scaturisce la minaccia di divulgare a tutti il tipo di siti visitati e la conseguente richiesta di denaro in criptovaluta”.*

Nulla di tutto ciò è reale: rappresenta un’invenzione dell’autore del reato, elaborata al solo scopo di gettarci nel panico ed indurci a pagare la somma illecita: è tecnicamente impossibile, infatti, che chiunque, pur se entrato abusivamente nella nostra casella di posta elettronica, abbia potuto – per ciò solo – installare un virus in grado di assumere il controllo del nostro dispositivo, attivando la webcam o rubando i nostri dati.

Ecco dunque alcuni consigli della Polizia Postale su come comportarsi:

Mantenere la calma. Il criminale non dispone, in realtà, di alcun filmato che ci ritrae in atteggiamenti intimi né, con tutta probabilità, delle password dei profili social da cui ricavare la lista di nostri amici o parenti

Non pagare assolutamente alcun riscatto: l’esperienza maturata con riguardo a precedenti fattispecie criminose (come

Sextortion e Ransomware) dimostra che, persino quando il criminale dispone effettivamente di nostri dati informatici, pagare il riscatto determina quale unico effetto un accanimento nelle richieste estorsive, volte ad ottenere ulteriore denaro:

- Proteggere adeguatamente l'email (ed in generale i nostri account virtuali): cambiare – se non si è già provveduto a farlo – la password, impostando quelle complesse.
- Non utilizzare mai la stessa password per più profili.
- Abilitare, ove possibile, meccanismi di autenticazione "forte" ai nostri spazi virtuali, che associno all'inserimento della password, l'immissione di un codice di sicurezza ricevuto sul nostro telefono cellulare.
- Tenere presente che l'inoculazione (quella vera) di virus informatici capaci di assumere il controllo dei nostri dispositivi può avvenire soltanto se i criminali informatici abbiano avuto disponibilità materiale dei dispositivi stessi, oppure qualora siano riusciti a consumare, ai nostri danni, episodi di *phishing* informatico: è buona norma quindi non lasciare mai i nostri dispositivi incustoditi (e non protetti) e guardarsi dal cliccare su link o allegati di posta elettronica sospetti.

The post Sextortion, Polizia Postale 'In corso massivo spamming a scopo estorsivo via email' appeared first on Key4biz.

https://www.key4biz.it/sextortion-polizia-postale-in-corso-massivo-spamming-a-scopo-estorsivo-mia-email/232387/

It-sa 2018, dal 9 all’11 ottobre a Norimberga la fiera di it-security più grande d’Europa

Dal **9 all’11 ottobre 2018** il mondo dell’IT-security si incontrerà al polo fieristico di **Norimberga**, dove sarà possibile partecipare gratuitamente all’evento più grande d’Europa del settore.

In seguito al grande processo di trasformazione digitale, la sicurezza informatica e la cybersecurity stanno assumendo un’importanza sempre più rilevante, sia in ambito sociale, economico e politico. Siamo di fronte a una sfida che chiunque si trovi in posizioni di vertice, sia che si tratti di uno Stato o di un’azienda deve affrontare con consapevolezza e determinazione.

Product Groups (Main interest of visitors)

Nell’ultima edizione dell’evento **it-sa** quasi 13.000 visitatori da tutto il mondo hanno incontrato più di 600 aziende internazionali. Per questa nuova edizione l’obiettivo è migliorare ancora.

Anche quest’anno sarà ricco il ciclo di conferenze **Congress@it-sa**, dove esperti del settore approfondiranno i temi più attuali, il focus si concentrerà maggiormente su scenari di applicazioni concrete, come ad esempio l’Industria 4.0, le infrastrutture critiche, l’amministrazione pubblica fino al sistema sanitario. I visitatori troveranno per il 2018 proposte e format specifici di settore nel programma collaterale che si terrà a margine dell’evento.

Chi sarà presente in fiera avrà quindi modo di partecipare a forum in cui gli espositori parleranno degli aspetti gestionali, della pianificazione e realizzazione di un sistema informatico sicuro. E’ possibile scaricare l’App ufficiale di it-sa per organizzare al meglio la visita e gli appuntamenti

rimanendo aggiornati su tutte le novità della fiera.

Clicca su questo link, iscriviti alla newsletter e potrai così creare l’ingresso omaggio per l’evento B2B più grande d’Europa dedicato alla sicurezza informatica.

Per informazioni in lingua italiana e per partecipare alla fiera, rivolgetevi alla filiale italiana della Fiera di Norimberga:

Carolina D’Alessandro

NürnbergMesse Italia S.r.l.

Via Fucini 5 – 20133 Milano

Tel. +39 02 36753263

e-Mail: carolina.dalessandro@nm-italia.it

The post It-sa 2018, dal 9 all’11 ottobre a Norimberga la fiera di it-security più grande d’Europa appeared first on Key4biz.

https://www.key4biz.it/it-sa-2018-dal-9-all11-ottobre-a-norimberga-la-fiera-di-it-security-piu-grande-deuropa/231262/

‘In Italia centinaia di reati informatici al giorno, il

Digital Forensics Expert mestiere sempre più strategico’. Intervista a Paolo Dal Checco

Informatica forense, una professione in fase di esplosione nel mondo del digitale, tanto più che ormai in Italia ci sono centinaia di reati informatici al giorno a fronte di squadre di informatici in numero limitato. Una professione che però è ancora un po’ oscura al grande pubblico anche se è in crescita esponenziale la domanda di **perizie informatiche forensi** per processi civili o penali, a fini legali e per utilizzo in Tribunale o in sede stragiudiziale. I temi d’informatica forense possono essere molteplici e includono tra gli altri computer, hard disk, pendrive, smartphone, tablet e navigatori, Internet, social network, criptovalute, malware, celle telefoniche, centralini, email, analisi antropometriche o fotografiche. Ne abbiamo parlato con l’esperto **Paolo Dal Checco**, titolare di uno Studio di consulenza d’Informatica Forense a Torino **attivo da anni a tempo pieno** su Perizie Informatiche per Tribunali, Procure, Forze dell’Ordine ma anche studi legali, privati o aziende. Dal Checco è Consulente Informatico Forense Albo dei CTU e dei Periti del Tribunale, Ruolo Periti ed Esperti CCIAA Prof. a Contr. di Sicurezza Informatica all’Università degli Studi di Torino.

Key4biz. ***Cos’è l’Informatica Forense e come si diventa un professionista in questo ambito?***

Paolo Dal Checco. L'informatico forense è colui che si occupa di supportare dal punto di vista tecnico chi ha conferito l'incarico nella fase di acquisizione delle prove digitali, analisi tecnica e produzione di perizie informatiche che possono essere utilizzate in Tribunale, in processi civili o penali durante i quali il perito potrà presenziare all'udienza come consulente (di parte, del pubblico ministero o del giudice).

La professione di Informatico Forense in Italia non è regolamentata da titoli o certificazioni. Rispetto ad altre professioni come il medico, l'architetto o l'ingegnere non ci sono albi od ordini specifici che abilitino all'attività professionale. E' anche per questo motivo che si tratta di una professione "oscura", perché puoi scontrarti in una causa con qualcuno che ha la terza media (senza con questo denigrare chi non ha potuto studiare) o che magari negli ultimi anni ha fatto l'idraulico (anche in questo caso, nulla contro gli idraulici appassionati d'informatica) per poi decidere di fare il perito informatico. Questo per esempio in ambito medico non può succedere: un idraulico non può fare e firmare un'autopsia.

Key4biz. ***Che strada si deve percorrere per diventare perito informatico forense?***

Paolo Dal Checco. Si parte dalle competenze informatiche che sono fondamentali. Poi ci si specializza sul fronte legale. Ci sono degli albi "generici" ai quali ci si può iscrivere: in primo luogo quelle delle Procure dei Tribunali, come perito e consulente tecnico. In alternativa o in parallelo, ci si può iscrivere al Ruolo della Camera di Commercio, come esperto e perito in un particolare settore e da lì avere poi accesso

agli albi del Tribunale, con tempistiche più o meno lunghe e documentazione da produrre per attestare le proprie competenze professionali.

Key4biz. ***L'informatica forense è una professione in ascesa?***

Paolo Dal Checco. E' così. Oltre a quelle dei clienti, ricevo numerosissime chiamate da persone di svariata provenienza professionale che mi domandano come fare a diventare informatico forense. In alcuni casi, tra l'altro, diventa piuttosto paradossale rispondere perché è come se un chirurgo ricevesse lo stesso tipo di richieste da persone senza il titolo adatto convinte di poter esercitare. La risposta in genere è che per quanto non servano titoli specifici non si può cominciare da un giorno all'altro a fare l'informatico forense: ci sono diverse strade per diventare professionisti ma nessuna è facile come sembra e forse anche per questo i competitor sul mercato sono ancora pochi.

Key4biz. ***Perché l'Informatica Forense, o Digital Forensics, è così in crescita?***

Paolo Dal Checco. Perché ogni tipo di reato informatico (ma anche reati non commessi tramite la tecnologia) in un modo o nell'altro va a impattare sul nostro ambito di attività. Qualunque cosa succeda che coinvolge un computer, un cellulare un profilo sui social network, Internet, la posta elettronica, messaggi **Whatsapp** – cose che usiamo tutti i giorni, tutto il

tempo della nostra vita – può diventare oggetto di analisi di un informatico forense. Questo perché per acquisire prove digitali o produrre una perizia informatica non puoi chiamare il tecnico che installa i programmi o ripara i PC, visto che non ha esperienza di studio di reati informatici, standard, iter processuali. E soprattutto perché si tratta di perizie che potrebbero portare ad un ambito giudiziale: una denuncia in ambito penale, una richiesta di risarcimento in ambito civile. Un tecnico informatico potrebbe intervenire, magari rimettendo a posto il computer e rischiando così di cancellare le prove di un reato, rendendo persino l'attività d'indagine più difficile se non impossibile. Al contrario, il cliente in genere vuole capire cosa è successo e portare in Tribunale eventuali responsabili o corresponsabili di un reato, oppure difendersi da accuse. Per questo motivo, la nostra professione è strategica, perché meglio viene fatta la perizia, fin dall'inizio, più facilmente si istruiscono le cause.

Key4biz. ***Quali sono le casistiche di reato più diffuse per le vostre perizie?***

Paolo Dal Checco. In ambito aziendale, furti da parte di dipendenti che possono aver copiato materiale riservato, proprietà intellettuale, elenco clienti per passarli alla concorrenza o per usarli di persona aprendo un'altra società autonoma. Questo succede molto spesso, è un fenomeno crescente con la crisi degli ultimi anni che rende i dipendenti o i soci più aggressivi nel passaggio da una società all'altra e coinvolge spesso progetti, prezzi, elenco clienti da portare in dote nella nuova azienda.

Key4biz. ***Tutto gira intorno al valore delle informazioni digitali. Altri tipi di reati?***

Paolo Dal Checco. Ci sono poi casi di reati non informatici ma nei quali l'informatica è elemento investigativo rilevante: omicidi, suicidi, furti, truffe, incidenti navali, aerei o stradali. Molto diffusi sono poi gli attacchi malware e ransomware o ancora attacchi sui conti bancari, per cui le persone perdono soldi a causa di phishing o truffe di vario genere. Sempre più frequenti i casi di "Ceo fraud", "business email compromise" o "man in the mail", nei quali ignari dipendenti vengono persuasi a eseguire bonifici anche ingenti verso coloro che ritengono essere i fornitori aziendali ma in realtà sono criminali. Tutto comincia con l'azienda che viene spiata in modo da acquisire informazioni sulle attività commerciali in corso: a un certo punto i delinquenti si intromettono nella posta, fingendosi il fornitore o il cliente, e cominciano a chiedere pagamenti di fatture su conti diversi da quello corretto.

Lo stesso tipo di attacchi può essere rivolto ai dati personali dei soggetti, per acquisire l'identità e creare finti profili online usati per altre truffe, per fare dei finanziamenti, aprire siti Internet, proporre vendite o investimenti. Spesso vengono portate avanti vere e proprie estorsioni, come ad esempio il cosiddetto "*sexting*", a seguito di truffa o furto di dati personali, prelevati da PC o Smartphone infetti o forniti dalle vittime a seguito di phishing. Tutti casi in cui la vittima fa denuncia e nello stesso tempo viene chiesta una perizia informatica perché la Polizia Postale, la Procura, la Questura chiede alla vittima di portare delle prove. Troppo spesso però le prove non sono state preservate, anzi, vengono persino inavvertitamente rimosse per evitare il reiterarsi del reato, riducendo in

questo modo anche la possibilità di far valere i propri diritti.

Key4biz. ***Quali sono i principali clienti dell'informatico forense?***

Paolo Dal Checco. Dal lato istituzionale, le Procure, i Tribunali e le Forze dell'ordine per collaborare con le indagini. Purtroppo, diventa sempre più difficile gestire gli aspetti burocratici ed economici nei rapporti con la Pubblica Amministrazione. I lavori diventano sempre più complessi e impegnativi ma nel contempo i compensi vengono tagliati e calcolati con sistemi basati su tabelle ormai non più adeguate che premiano non la rapidità di esecuzione ma la durata dell'incarico.

Ho avuto e ho l'onore di lavorare con personale altamente qualificato presente presso Tribunali, Procure, Polizia Postale, Guardia di Finanza e Carabinieri ma il problema è che rispetto alla quantità di lavoro gli esperti sono pochissimi e spesso non dotati di strutture adeguate per mancanza di fondi. Per questo motivo sono costretti a ricorrere a consulenti esterni, con la problematica accennata sopra dei tempi e dei compensi.

Poi ci sono le aziende e gli studi di avvocati, che assistono i loro clienti. Molto spesso ci chiedono perizie per dimostrare che la controparte ha falsificato delle mail, producendo false prove, per provare accessi abusivi, furti di dati, frodi o reati che senza una perizia informatica sarebbero difficili da documentare.

The post 'In Italia centinaia di reati informatici al giorno,

il Digital Forensics Expert mestiere sempre più strategico’. Intervista a Paolo Dal Checco appeared first on Key4biz.

https://www.key4biz.it/in-italia-centinaia-di-reati-informatici-al-giorno-il-digital-forensics-expert-mestiere-sempre-piu-strategico-intervista-a-paolo-dal-checco/231852/