29/05/2021

guiomarparada.nova100.ilsole24ore.com

Argomento: Exprivia: si parla di noi

EAV: € 5.358
Utenti unici: 258.300

https://guiomarparada.nova100.ilsole24ore.com/2021/05/29/cybersicurezza-aziende-exprivia/

Cybersicurezza – Tra Sparta e Atene il fronte aperto delle aziende: l'opinione di Domenico Raguseo di Exprivia

29 maggio 2021 Guiomar Parada

App, Best practices, Big data, Consumatori, Cyber crime, Digitalizzazione, Fabbriche, Governo, IIoT, Imprese, Industria, Industria 4.0, Infrastrutture, Innovazione, Internet, Investimenti, IoT, Manifattura, Piattaforme, Privato, Pubblico, Regolamentazione, Reti, Salute, Security, Senza categoria, Sicurezza, Virus

"La più grande campagna di **spionaggio** dei tempi recenti ", ha detto dell'attacco **SolarWinds** Thomas Rid, professore di Studi strategici alla **Johns Hopkins**. Istallando una **backdoor** nel sistema SolarWinds, un fornitore di **it** a molti enti del **governo** e società private tra cui **Microsoft**, i molto sofisticati **hacker** si sono aperti l'accesso a una intera **filiera dell'approvvigionamento** it e a migliaia di **sistemi** diventati potenziali **obiettivi**. Mentre pubblichiamo Microsoft ha denunciato un altro grave mega attacco di **cyberspionaggio**.

Quello **ransom** all'**oleodotto Colonial**, sempre negli Usa, ha lasciato a secco pompe di **benzina**, **porti** e altre **infrastrutture** lungo tutta la Costa Est.

BIO BLOGGER

Guiomar Parada
Se non fosse prevalsa una inclinazione per i media e il giornalismo sarei stata una felice e dedita e geologa (ho studiato geologia [...]
@GuiomarParada

ARCHIVIO POST

« MAGGIO 2021 »

Lu	Ma	Me	Gi	Ve	Sa	Do
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

POST RECENTI

29 maggio 2021
Cybersicurezza – Tra Sparta e Atene il fronte aperto delle aziende: l'opinione di Domenico Raguseo di Exprivia

12 maggio 2021
Industria 4.0 – I quattro ecosistemi industriali per la digitalizzazione e l'inclusione in catene del valore globali

4 maggio 2021
Industria 4.0 - La biforcazione tra imprese digitali e non: si amplifica per le pmi, ma gli ecosistemi aiutano la digitalizzazione

SEGUI ANCHE SU

FACEBOOK

Cybersicurezza – Tra Sparta e Atene il fronte aperto delle aziende: l'opinione di Domenico Raguseo di Exprivia

"La più grande campagna di spionaggio dei tempi recenti ", ha detto dell'attacco SolarWinds Thomas Rid, professore di Studi strategici alla Johns Hopkins. Istallando una backdoor nel sistema SolarWinds, un fornitore di it a molti enti del governo e società private tra cui Microsoft, i molto sofisticati hacker si sono aperti l'accesso a una intera filiera dell'approvvigionamento it e a migliaia di sistemi diventati potenziali obiettivi. Mentre pubblichiamo Microsoft ha denunciato un altro grave mega attacco di cyberspionaggio.

Quello ransom all'oleodotto Colonial, sempre negli Usa, ha lasciato a secco pompe di benzina, porti e altre infrastrutture lungo tutta la Costa Est.

La nota quasi incredibile, che dà una idea dell'intensità e la dimensione degli attacchi, è che DarkSide, l'organizzazione criminale che ha chiesto il riscatto a Colonial per sbloccarle i dati e il sistema, è stata hackerata a sua volta, a quanto pare, nel suo sistema di "pagamenti".

Risulta altrettanto che Colonial abbia pagato $ 5 milioni, proprio ciò che il governo voleva evitare, perché adesso DarkSide ha altri $ 5 milioni freschi freschi per espandere e migliorare le operazioni criminali.

Chiedo una opinione a Domenico Raguseo, direttore Cybersecurity Exprivia che pubblica l'Osservatorio Cybersecurity. L'ultimo rapporto, quello del primo trimestre 2021, registra in Italia un aumento del 56% degli attacchi rispetto all'ultimo trimestre 2020, quando erano già cresciuti del 47% rispetto ai primi due.

Secondo alcuni esperti, il vero obiettivo del gigante ransom hack all'oleodotto sono stati i soldi, nonostante le enormi conseguenze economiche e reputazionali, come nel caso SolarWinds o altri attacchi DDoS che bloccano un sito web. Come li interpretate?

Il denaro è la motivazione della maggior parte dei crimini nel mondo reale, non ci dovrebbe sorprendere che su internet le priorità non cambino.

Parliamo di aziende e industria. Nel rapporto Exprivia 2020 si legge che l'incremento degli attacchi negli ultimi sei mesi viaggia di volta in volta a oltre il 40%. Le aziende hanno mancato di individuare le vulnerabilità nei propri sistemi o di investimenti o visione quanto al cyberrischio?

Il paradosso è che gli attaccanti hanno a disposizione armi sofisticate e grandi risorse, ma spesso gli attacchi hanno successo perché sfruttano vulnerabilità conosciute o truffe banali, come campagne di phishing. Questo potrebbe suggerire che le aziende non abbiano fatto investimenti sufficienti, ma che cosa vuol dire "sufficiente"? Se da un lato l'information Technology (it) nasce per ottimizzare operazioni ripetitive e reversibili – quindi strettamente collegata al concetto classico di ritorno dell'investimento (Roi) – nel corso degli anni si trasformata in un driver fondamentale dell'innovazione supportando servizi non reversibili. Ciò oltre ad allargare il divario tra chi attacca e chi difende, ha reso spesso difficile applicare il concetto di Roi. Si può spendere tanto ed essere vittima di un

attacco, o nulla e non essere colpiti. Noi lavoriamo per ridurre il rischio e identificare quanto sia necessario spendere e quanto sia possibile ridurre le probabilità di un attacco. Non è un esercizio semplice.

Qual è dunque la più grande difficoltà all'interno di un'azienda quando si tratta di allocare risorse alla sicurezza?

Intanto il fatto che non sia possibile stabilire un Roi chiaro. Inoltre, per quanto sia piccolo il budget allocato, esso va dimensionato alla mission critical dell'azienda o istituzione. Nel caso degli ospedali, la loro mission è salvare la vita delle persone. Dunque, ogni centesimo verrà speso per farlo e per investire in cybersecurity sì sottrarranno risorse al budget destinato a quella missione – e questo senza avere ben chiaro il Roi.

Tuttavia, c'è un altro aspetto da considerare: da un lato abbiamo i responsabili nelle aziende che devono decidere un investimento senza un Roi chiaro per avere in cambio la sola riduzione del rischio di un attacco; dall'altra, abbiamo persone fortemente motivate ed esperte nell'appropriarsi di denaro altrui.

Per analogia penso sempre al film '300'. Quando l'ateniese si vanta con lo spartano di avere molti più uomini, lo spartano gli risponde chiedendo il mestiere dei soldati ateniesi solo per scoprire che erano artisti, vasai, eccetera; gli spartani, invece, erano tutti soldati, persone addestrate per combattere.

Gli attaccanti sono soldati, persone che ogni singolo giorno studiano come rendere più distruttivo un attacco.

Inoltre, gli attaccanti oltre a essere professionisti esperti e specializzati, scelgono loro quando attaccare. La mission critical di chi difende, invece, di solito è tutt'altra cosa. Chi si difende non sa quando l'attacco arriverà e magari in quel momento sta operando a cuore aperto.

È l'evoluzione digitale degli ultimi 20 anni che ha disegnato questo scenario: l'essere umano non ha avuto il tempo per adeguarsi alle nuove minacce.

Se oggi parliamo di cybersecurity è perché i servizi forniti dall'it sono irreversibili e fortemente intrinsechi alla quotidianità. Dai servizi it e dalla loro connettività dipende ormai la vita su questo Pianeta – difficile pensare ad aerei che volano, all'utilizzo di corrente elettrica o a fare una vaccinazione in assenza di connettività e intelligenza connessa.

Potremmo considerare questa marea di dispostivi connessi e intelligenti come l'acqua, l'aria, il fuoco o la terra, con la differenza che l'essere umano ha avuto millenni per comprendere le minacce degli elementi naturali, e solo pochi decenni per i rischi del mondo digitale.

Si torna sempre al dibattito su quale aspetto migliori la sicurezza. Per esempio, sempre in campo sanitario, le decine di migliaia di dispositivi attivi sono certificati, ma ciò è inutile se poi l'utente si collega a reti non sicure. L'unico modo di migliorarla per tutti, bambini inclusi, anche su piattaforme o per strumenti non ancora inventati, sembra essere quello della consapevolezza-formazione-responsabilità. È un elemento da recuperare?

Questo non è un elemento da recuperare, questo è l'elemento. Nel nostro ultimo rapporto abbiamo contato più o meno 7 milioni di dispositivi esposti su internet – it classica, ma anche frigoriferi, smart tv, telecamere di videosorveglianza, ecc.

Un tema da non sottovalutare è pertanto la certificazione sulla cyber-resilienza dei dispositivi messi sul mercato: e questo spetta

alle istituzioni. Non si può chiedere (per ora) al consumatore, che sia consapevole o meno, di doversi preoccupare della sicurezza del frigorifero o del robottino. I dispositivi devono essere certificati per non lasciare solo l'utente finale in tema cybersicurezza.

Nell'industria, le reti e l'it, come diceva, sono essenziali e pervasivi. La comunicazione machine to machine (m2m) poteva fare meno danni che oggi l'Internet of Things (IoT). Le aziende hanno molto da perdere se attaccate...

E non dimentichiamoci che spesso l'it classica è utilizzata al servizio dell'operation technology (Ot) che è a sua volta funzionale all' erogazione di servizi essenziali come la produzione di energia e la sua distribuzione. Siamo di fronte a un mare di dispositivi, qualcuno critico altri meno, e tutti insieme funzionali alla vita digitale (e non solo) nel mondo.

L'IoT pone due ordini di problemi: il primo è la governance, quindi chi è il responsabile di questi dispositivi? In un'azienda chi si deve preoccupare che le telecamere di videosorveglianza non siano compromesse da un malware?

La mancanza di consapevolezza dei rischi cui la trasformazione digitale ci espone è un ulteriore problema per le aziende, oltre all'assenza di Roi. Se proprio dovessi dare loro dei suggerimenti, il primo sarebbe di affidarsi a persone molto competenti, perché il nostro mestiere è quello di ottimizzare l'investimento: il budget è limitato e quindi non va sprecato. Il secondo sarebbe di investire in consapevolezza.

La tecnologia evolve da sempre, ma prima lo faceva in maniera aritmetica, ora lo fa esponenzialmente – per esempio, nei dati. Regolamentazioni virtuose possono da un giorno all'altro diventare non applicabili perché sono sorte nuove interconnessioni tra tecnologie o perché le catene del valore sono diventate complesse. Come si stabilisce un sistema di sicurezza che sia dinamico e nel quale tutti siano responsabili?

Il dato è il carburante della nuova economia. Se un'azienda investe in servizi che utilizzano dati, non può non investire per proteggerli in maniera consistente e coerente. Questo è suggerito dal buon senso, ma adesso esistono regole chiare: il Gdpr. Qua non si tratta di Roi, ma di rispettare leggi che danno indicazioni anche sul valore delle multe per violazioni. Chiaro che non si possono fare investimenti per paura di una multa, ma spesso ciò suggestiona.

Ovviamente non si tratta solo del Gdpr. La forte dipendenza dall'ecosistema digitale rende necessario l'intervento delle istituzioni con leggi, direttive e regolamentazioni.

Qualche mese fa c'è stato un gigantesco blackout in Texas e ho immaginato le enormi falle che potevano aprirsi durante un evento durato settimane – soprattutto tra le pmi, per esempio, nei collegamenti con il cloud. Come si affrontano questi scenari?

Lo scorso anno si è verificata un'accelerazione dello spostamento di carichi di lavoro verso il cloud. I vantaggi sono evidenti se questo processo è fatto rispettando le policy di sicurezza. Uno dei problemi che abbiamo affrontato è che tali policy sono spesso legate alla segmentazione fisica e non possono essere spostate sul cloud così come sono.

Abbiamo dovuto pertanto dovuto pensare a progetti per la micro-segmentazione, dove le policy di sicurezza si disaccoppiano dalla segmentazione fisica.