ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Anno 3 / Numero 5
2022

CYBER MAGAZINE

In questo numero:

Fai la cosa giusta:

perché i Responsible Disclosure sono fondamentali

Odio e incitamento:

la proposta europea per estendere l'elenco dei crimini europei di hate speech ad hate crime

Internet Of Things:

c'erano una volta gli oggetti

INDICE

01. **Fai la cosa giusta:** perché i Responsible Disclosure sono fondamentali
di Pierguido Iezzi — **Pg. 04**

02. **La babele della cybersecurity:** un'azienda italiana ha in media 37 soluzioni di sicurezza installate, ma molte non vengono utilizzate
di Trend Micro — **Pg. 06**

03. **La cybersecurity come leva per la trasformazione digitale**
di Fabio Panada — **Pg. 07**

04. **Odio e incitamento:** la proposta europea per estendere l'elenco dei crimini europei
di hate speech ad hate crime — **Pg. 08**

05. **Internet Of Things: c'erano una volta gli oggetti**
di Valentina Arena — **Pg. 11**

06. **Cinque trend di cui le aziende dovranno tenere conto durante la pianificazione dei budget per la cybersecurity 2022**
di Evgeniya Naumova — **Pg. 14**

REDAZIONE:
Federico Giberti , Melissa Keysomi

L’editoriale del Presidente Assintel Paola Generali

Dicembre 2021

La sicurezza informatica è stata un’area di investimento importantissima per le aziende italiane nel corso degli ultimi 12 mesi, spinta dall’accelerazione al digitale contestuale agli episodi di lock down. Con la progressiva apertura delle reti agli accessi da remoto e con la crescente adozione di servizi di cloud computing è aumentata la consapevolezza da parte delle imprese della necessità di proteggere i propri dati, sistemi e risorse interne da possibili incidenti o attacchi informatici.

La mappatura di Assintel Report ci restituisce un mercato ICT in crescita costante, in cui cresce di pari passo l’investimento in cyber security. Circa l’80% delle aziende utenti intervistate ha dichiarato di aver investito anche in sicurezza, mentre il 30% di loro conferma il potenziamento anche per i prossimi 12 mesi.

Un altro fenomeno interessante per la cyber security è legato all’area delle operations aziendali, che sta evolvendo attraverso un utilizzo crescente di tecnologie di automazione e di analisi dei dati: con la progressiva connessione di sistemi e macchinari produttivi in rete, infatti, cresce anche il perimetro aziendale da proteggere da eventuali attacchi informatici che possono portare a un’interruzione dell’operatività o al furto di dati sensibili.

Quello che ci sta dicendo il mercato è chiaro: la trasformazione digitale sta accelerando la sua corsa e le aziende – non solo grandi ma anche PMI - stanno progressivamente comprendendo l’importanza della protezione dei dati e dei sistemi IT.

Fai la cosa giusta: perché i Responsible Disclosure sono fondamentali

A cura di Pierguido Iezzi, Swascan

Nel vasto mondo della cyber security esiste un processo conosciuto e riconosciuto chiamato Responsible Disclosure.
Detto in maniera sintetica, per Responsible Disclosure intendiamo il modello di divulgazione delle vulnerabilità in cui questa viene resa pubblica solo dopo un determinato periodo di tempo. Ciò rende possibile al vendor interessato il processo di risoluzione della criticità e il rilascio di una patch.
Volendo fare un esempio, l'azienda di cyber security che rileva la criticità informa il vendor di quanto rilevato e da a questo tutto il tempo necessario a risolvere la problematica. Una volta risolta i primi procedono alla diffusione di tutti i dettagli.
In termini pratici, la Responsible Disclosure è un compromesso tra ciò che i vendor vorrebbero (nessuna divulgazione pubblica) e la divulgazione completa che li renderebbe altamente vulnerabili.

La comunicazione è la chiave: Log4j

Se si crea un software o un'applicazione, non è possibile sperare che questa sia per sempre perfetta ed immune a qualsiasi tipo di vulnerabilità: alla fine qualcuno troverà una vulnerabilità di sicurezza in essa - minore o maggiore che sia. In quel caso è fondamentale essere aperti e recettivi ad ogni comunicazione che arrivi in questo senso.
Il processo di Responsible Disclosure è molto specifico e ci sono delle scadenze chiaramente definite per il rilascio di una patch del vendor in modo che gli utenti possano avere tutto il tempo per implementarla (90 giorni è lo standard accettato).
È anche spesso stabilito che un PoC (proof of concept – ovvero un esempio di come può essere sfruttata la vulnerabilità) può essere rilasciato pubblicamente solo con l'approvazione del vendor. Occasionalmente le aziende richiedono ai ricercatori di sicurezza di accettare un accordo di non divulgazione, il che significa che i PoC potrebbero non finire mai per essere pubblicati anche se la vulnerabilità è stata risolta da tempo.
Il processo di Responsible Disclosure al vendor interessato di solito segue questa sequenza (se tutto va bene):

- Il ricercatore o l'azienda di sicurezza informa il vendor della vulnerabilità e fornisce un PoC di accompagnamento
- Il vendor conferma l'esistenza della vulnerabilità e fornisce una linea temporale approssimativa per il rilascio di una correzione
- Una volta che una correzione è stata sviluppata, il vendor chiede al ricercatore di confermare se la correzione funziona
- Dopo che il ricercatore "conferma" la correzione, il vendor implementa la patch
- Se il vendor è d'accordo, un certo tempo dopo che la patch è stata rilasciata, i dettagli della vulnerabilità possono essere pubblicati (qualsiasi cosa fino a 90 giorni è normale)

Per quanto riguarda la vulnerabilità di Log4j che ha causato caos e panico durante la fine del 2021, il processo di Responsible Disclosure era già in corso quando è stata rivelata pubblicamente (come evidenziato dalla richiesta di pull su GitHub che è apparsa il 30 novembre).
Mentre i commenti degli utenti sulla pagina del progetto GitHub di Apache Log4j hanno indicato la frustrazione per la velocità della correzione, questo è normale quando si tratta di risolvere vulnerabilità. Dimostrazione, comunque, di quanto sia importante questo paradigma nella cyber security di oggi.

Il caso Swascan

A differenza di Log4j, in Italia, Swascan è da tempo protagonista di iniziative di Responsible Disclosure di successo; da ultimo la collaborazione con il colosso dell'IT MSI.

Micro-Star International (MSI) è una multinazionale taiwanese dell'informatica con sede a Nuova Taipei e filiali nelle Americhe, in Europa, in Asia, in Australia e in Sudafrica. Essa progetta, sviluppa e fornisce hardware per computer, prodotti e servizi correlati, tra cui: computer portatili, computer desktop, schede madri, schede grafiche, computer All-in-One, server, computer industriali, periferiche per PC, prodotti di infotainment per auto, e altri. L'azienda produce inoltre chipset di schede grafiche sia per AMD che per nVidia. Alcuni produttori di computer come Alienware e Falcon Northwest vendono PC equipaggiati con schede madre MSI. MSI produce anche schede madri adatte all'overclock. I prodotti MSI sono venduti al dettaglio, parti OEM, o ad altre imprese
Dopo aver rilevato gravi vulnerabilità legate all'azienda durante una scansione di Threat Intelligence, infatti, Swascan ha avviato il processo di Responsible Disclosure con successo.
Le grandi aziende, per natura, sono ambienti complessi ed eterogenei. MSI non è diversa, un vasto perimetro può presentare una serie di complessità che potrebbero far scivolare alcune vulnerabilità attraverso la rete del proprio dipartimento di sicurezza. Ecco perché la cooperazione è così importante. Non appena abbiamo scoperto queste vulnerabilità, abbiamo contattato MSI e fornito prove e PoC per spiegare meglio le possibili conseguenze di questi CVE. Da parte loro, MSI è stata eccezionale nel ricevere e riconoscere il problema e nel lavorare insieme per risolvere il problema in linea con la migliore pratica di Vulnerability Disclosure. Ancora una volta, l'intero processo dimostra quanto sia diventata fondamentale la Cyber Threat Intelligence. Senza di essa, questa criticità sarebbe probabilmente rimasta dormiente per mesi o anche più a lungo, e avrebbe potuto essere trovata dal Criminal Hacker prima che il CIST avesse il minimo sentore che potesse essere un problema. La sicurezza informatica è prima di tutto prevenzione, non dobbiamo dimenticarlo...

La babele della cybersecurity: un'azienda italiana ha in media 37 soluzioni di sicurezza installate, ma molte non vengono utilizzate

Una ricerca Trend Micro rivela che sempre più organizzazioni esternalizzano i servizi di cybersecurity per riuscire a contrastare le minacce IT. ***A cura di Trend Micro***

In Italia le aziende hanno una media di 37 soluzioni di cybersecurity installate a protezione della propria infrastruttura, ma nel 51% dei casi non vengono utilizzate tutte. Il dato emerge dallo studio "Managing the secops tool sprawl challenge", a opera di Trend Micro, leader globale di cybersecurity.

Queste le principali motivazione che spingono la maggior parte degli addetti alla cybersecurity a non utilizzare determinate soluzioni:

- Le soluzioni sono obsolete (39%)
- Mancanza di personale qualificato in grado di utilizzarle (35%)
- Mancanza di fiducia nella soluzione (29%)
- Difficoltà di integrazione con altre soluzioni (25%)

La gestione della security rimane critica, in caso di violazioni o mancata compliance alla normativa GDPR, il campione rivela che l'azienda perderebbe una media di 230.000 euro.

"La proliferazione di diversi strumenti è sempre più comune in tutte le aziende, ma quando si tratta di rilevamento e risposta agli incidenti, c'è un costo crescente che a volte non viene riconosciuto". Ha affermato Salvatore Marcis, Technical Director di Trend Micro Italia.

La ricerca rivela anche che il 96% del campione ha preso in considerazione la modalità managed service – servizi gestiti, per esternalizzare le capacità di rilevamento e risposta. Questi servizi possono aiutare a superare le criticità interne, determinando una migliore strategia di gestione e risposta agli incidenti.

"Le organizzazioni non solo devono pagare per le licenze e la manutenzione, ma i team SOC sono sempre più stressati e rischiano il burnout nel tentativo di gestire troppe soluzioni. La mancanza di capacità nel mettere in ordine di priorità gli avvisi può anche esporre l'organizzazione a violazioni. Per questo non sorprende che molte aziende utilizzino servizi gestiti esternamente". Ha concluso Salvatore Marcis.

Metodologia e campione della ricerca

La ricerca, commissionata da Trend Micro a Sapio Research, ha coinvolto 2.303 IT security decision maker in 21 Paesi, provenienti da aziende con più di 250 dipendenti. In Italia il campione è stato di 100 intervistati.

Ulteriori informazioni sono disponibili a questo link.

La cybersecurity come leva per la trasformazione digitale

A cura di Fabio Panada, Cisco Italia

I nuovi modelli di lavoro e l'aumento dei dispositivi collegati alla rete hanno spinto le aziende a utilizzare nuove soluzioni tecnologiche in grado di garantire la continuità aziendale. Oggi ci troviamo di fronte ad una rete sempre più estesa e complessa, fatta non solo di dispositivi, ma anche di persone.

Una rete più ampia genera, purtroppo, maggiori opportunità di essere attaccati. I criminali informatici utilizzano strumenti sempre più sofisticati in grado non solo di fermare completamente l'operatività, ma anche di prendere possesso dei dati aziendali: il ransomware resta la minaccia numero uno e rappresenta quasi la metà di tutti gli attacchi a livello globale, come rilevato recentemente da Cisco Talos, la più grande organizzazione privata di intelligence sulle minacce informatiche al mondo.

Uno dei motivi principali che spingono i criminali informatici ad utilizzare il ransomware come metodo di attacco è la velocità con cui le vittime tendono a pagare il riscatto, spesso solo per poter ripristinare i servizi e i dati il prima possibile. I settori più colpiti sono quello della sanità, subito seguito da quello della pubblica amministrazione, a questi si aggiungono i trasporti, le telecomunicazioni, la produzione e l'istruzione.

Cosa possono fare le aziende per difendersi in modo adeguato? Consapevolezza, prevenzione, maggiore controllo degli accessi, semplicità d'uso e integrazione delle soluzioni di sicurezza utilizzate in azienda.

La crescita del lavoro da remoto e dell'utilizzo delle soluzioni cloud hanno evidenziato l'importanza dell'autenticazione degli utenti e dei dispositivi che si collegano alla rete aziendale. Username e password non sono mai stati un metodo particolarmente sicuro e la loro compromissione resta ancora uno dei metodi più utilizzati dai criminali informatici. Abilitare un'autenticazione a più fattori (MFA) è una delle difese più efficaci che le aziende hanno a disposizione: sarà così possibile prevenire la maggior parte dei tentativi di attacchi semplicemente abilitando l'MFA sui servizi aziendali critici. Ma non solo: gli utenti potranno accedere alla rete utilizzando semplicemente il loro telefono e sfruttando, ad esempio, le funzionalità biometriche del device. Le soluzioni Passwordless, come quella di Cisco DUO, garantiscono un elevato standard di sicurezza e semplificano notevolmente il processo di autenticazione.

Le soluzioni Cisco Security sono facilmente integrabili, anche in situazioni dove sono già presenti soluzioni di terze parti: questo approccio, inserito in un processo Zero Trust, è la chiave per creare una strategia di cybersecurity che sia funzionale, semplice e adattabile.

Utenti, risorse e applicazioni sono parte integrante della strategia di sicurezza e sono il motivo per cui gli investimenti in cybersecurity dei prossimi mesi dovranno prendere in considerazione piattaforme integrate, semplici da usare e che siano in grado di rilevare le attività non autorizzate e porre rimedio in modo tempestivo.

Odio e incitamento: la proposta europea per estendere l'elenco dei crimini europei

A cura di Hate speech ad hate crime

La Commissione europea ha recentemente presentato un'iniziativa per estendere l'elenco dei "crimini europei" ai discorsi d'odio e ai crimini d'odio, coerentemente con quanto annunciato dalla Presidente von der Leyen nel suo discorso sullo stato dell'Unione del 2020, con riferimento al pieno rispetto dei valori europei fondamentali sanciti dall'articolo 2 del Trattato sull'UE.
Si tratta di una importante iniziativa che segnerà un svolta epocale nel monitoraggio e conseguenziale repressione dei discorsi di odio o di istigazione all'odio, nonché dei crimini di odio che hanno ormai raggiunto una portata e tendenza davvero preoccupanti in ecosistema online ed offline.
Tale fenomeno è invero emerso con particolare evidenza durante la pandemia e si è manifestato spesso attraverso un progressivo aumento del livello di odio manifestato contro, ad esempio, rom, ebrei, musulmani e persone di origine asiatica, o percepite come di tale origine, inclusi attacchi e percosse razziste, bullismo violento, minacce e abusi razzisti.
Fonti europee hanno rilevato che il 52% delle giovani donne e ragazze ha subito violenza online, comprese minacce e molestie sessuali, mentre le persone con disabilità sono più a rischio di essere vittime di crimini violenti, inclusi crimini d'odio, rispetto ad altre persone e di subire molestie.
Per queste ragioni, a norma dell'articolo 83, paragrafo 1, del trattato sul funzionamento dell'UE ("TFUE"), il Parlamento europeo e il Consiglio europeo possono stabilire norme minime sulla definizione dei reati e delle sanzioni nei settori della criminalità particolarmente grave, come ad esempio, il terrorismo (anche on line), la tratta di

esseri umani e lo sfruttamento sessuale di donne e bambini.
In tale scenario, sulla base della progressione di fenomeni legati alla proliferazione della criminalità grave, il Consiglio europeo può adottare una decisione che identifichi altri settori, consentendo alla Commissione europea, in una seconda fase, di proporre un quadro solido per affrontare l'incitamento all'odio e i reati di odio a livello dell'UE.
Va detto tuttavia, che a livello dell'UE, la decisione quadro del Consiglio europeo sulla lotta a determinate forme ed espressioni di razzismo e xenofobia mediante il diritto penale ha già rappresentato e, tuttora rappresenta, una forte risposta comune all'incitamento all'odio razzista e xenofobo e ai crimini ispirati dall'odio.
La decisione quadro mira infatti a garantire che le gravi manifestazioni di razzismo e xenofobia siano punibili con sanzioni penali efficaci, proporzionate e dissuasive in tutta l'UE e, soprattutto, richiede agli Stati membri di criminalizzare l'incitamento all'odio per motivi di razza, colore della pelle, religione, discendenza o origine nazionale o etnica, garantendo altresì che, per reati diversi dall'incitamento all'odio, la motivazione razzista e xenofoba sia considerata un'aggravante o, in alternativa, determinare un aumento delle sanzioni.
Malgrado ciò, è ancora necessaria un'azione comune dell'UE per affrontare questa sfida poiché attualmente non esiste una base giuridica per criminalizzare l'incitamento all'odio e i crimini ispirati dall'odio a livello dell'UE e va auspicabilmente ampliato l'elenco esistente di reati dell'UE nel trattato sul funzionamento dell'Unione europea (TFUE) al fine di garantire norme comuni minime su come definire i reati e le sanzioni applicabili in tutti gli Stati membri dell'UE.
Pertanto, l'iniziativa di estendere l'elenco dei crimini a livello UE, è un primo passo per una risposta europea più efficace alle minacce contro il pluralismo e l'inclusione e, in questa direzione, intende ulteriormente, sia sostenere gli sforzi degli Stati membri per attuare efficacemente la decisione quadro, attraverso il lavoro del gruppo ad alto livello sulla lotta al razzismo, alla xenofobia e ad altre forme di intolleranza, sia sostenere il piano d'azione dell'UE contro il razzismo 2020-2025 e la strategia per combattere

l'antisemitismo e promuovere la vita ebraica nell'UE, nonché la strategia per l'uguaglianza di genere 2020-2025.
L'iniziativa inoltre, fa parte di una serie più ampia di azioni dell'UE per contrastare l'incitamento all'odio illegale e le ideologie estremiste violente e il terrorismo online, come il codice di condotta dell'UE per contrastare l'incitamento all'odio illegale online, la proposta di legge sui servizi digitali, il regolamento sulla lotta ai contenuti terroristici online e il Forum Internet dell'UE.
A tal riguardo, si ricorda che l'Unione europea, in coerenza con la European Security Union Strategy, ha adottato lo scorso 16 marzo il nuovo regolamento relativo al contrasto della diffusione di contenuti terroristici online, preordinato a impedire ai terroristi di utilizzare la rete del web e i social network per l'attività di reclutamento e incitamento alla radicalizzazione e alla violenza.
Scopo della strumento normativo è evidentemente quello di fornire agli Stati membri uno strumento che legittimi la richiesta ai providers di pronta rimozione dal web dei contenuti di matrice terroristica.
Del resto, i social network e le piattaforme online sono ormai da tempo strumenti di rapida diffusione dell'incitazione alla violenza finalizzata alla radicalizzazione e, spesso anche alla realizzazione ovvero allo sharing (live) di atti e attacchi terroristici.
L'iniziativa proposta dalla Commissione europea, come di seguito indicato, fornisce in definitiva una serie di presupposti ed evidenze al fine di procedere legislativamente verso l'estensione normata dell'elenco dei crimini dell'UE ai discorsi d'odio e ai crimini ispirati dall'odio, alla luce dei criteri di cui all'articolo 83, paragrafo 1, TFUE:

- Considerazione della **dimensione transfrontaliera** dell'incitamento all'odio e dei crimini d'odio: l'incitamento all'odio online si diffonde rapidamente ed è accessibile a tutti e ovunque. Le ideologie alla base dell'incitamento all'odio e dei crimini d'odio possono essere sviluppate a livello internazionale e possono essere rapidamente condivise online. I crimini di odio possono essere commessi da reti con membri di diversi paesi.

- Considerazione dell'incitamento all'odio e crimini di odio come **area di criminalità**: la Commissione europea ritiene infatti che l'incitamento all'odio e i crimini di odio siano un'area di criminalità in quanto condividono una caratteristica intrinseca, ovvero l'"odio" nei confronti di persone o gruppi di persone che condividono (o sono percepiti come condivisione) le stesse caratteristiche protette.

- Considerazione dell'incitamento all'odio e crimini ispirati dall'odio come **ambito di criminalità particolarmente grave:** l'incitamento all'odio e i crimini ispirati dall'odio sono reati particolarmente gravi poiché minano i valori comuni e i diritti fondamentali dell'UE, come sancito dagli articoli 2 e 6 del trattato sull'Unione europea. Hanno impatti dannosi sugli individui, sulle loro comunità e sulla società in generale.

- Considerazione degli **sviluppi nella criminalità:** C'è stato un aumento costante nei due fenomeni a causa di vari cambiamenti e sviluppi economici, sociali e tecnologici. La pandemia di COVID-19 è stato uno dei fattori che hanno contribuito a questo aumento.

- Considerazione dell'ulteriore circostanza oggettiva che **non sussiste alcuna alternativa all'estensione dell'elenco dei crimini dell'UE:** i discorsi d'odio e i crimini d'odio sono criminalizzati in varia misura negli Stati membri dell'UE. Solo l'estensione dell'elenco dei crimini dell'UE ai discorsi d'odio e ai crimini d'odio può consentire un approccio penale efficace e globale a questi fenomeni a livello dell'UE, insieme a una protezione coerente delle vittime di tali atti.

A questo punto, il Consiglio europeo è chiamato ad adottare all'unanimità, previa approvazione del Parlamento europeo, una decisione che identifichi l'incitamento all'odio e i crimini ispirati dall'odio come un'altra area di criminalità che soddisfa i criteri di cui all'articolo 83, paragrafo 1, del TFUE e, solo successivamente, la Commissione europea potrà proporre l'adozione, da parte delle istituzioni europee, di una normativa che stabilisca norme minime sulle definizioni e sulle sanzioni di incitamento all'odio e reati di odio in linea con la procedura legislativa ordinaria.

Internet Of Things: c'erano una volta gli oggetti

A cura di Valentina Arena, Encyberisk

C'era una volta un orologio, un'automobile, un frigorifero e un pneumatico. Solo a vederli, tutti desideravano incontrarli, specialmente la piccola Rete.
Un bel giorno la Rete inciampò negli oggetti e si innamorò perdutamente di essi.
Passarono i giorni e poichè capì che stava bene con tutti... ma proprio con tutti, decise di non abbandonarne alcuno.
Nacque così l'Internet of Things.

L'**Internet delle cose**, o la rete degli oggetti connessi è qualcosa che oggi impatta sulla vita di tutti noi, che sta trasformando profondamente molti aspetti dell'economia e della nostra quotidianità, anche se spesso non ce ne rendiamo conto.
Il concetto di IoT si riferisce a un'infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano ("oggetti" a sé stanti oppure oggetti connessi ad altri o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete.

I MOMENTI IMPORTANTI

Il termine è comparso per la prima volta nel 1999 in una presentazione di **Kevin Ashton**, ricercatore del MIT, alla Procter & Gamble.
Ashton stava lavorando con dei colleghi ai tag RFID (etichette elettroniche che possono essere applicate più o meno dappertutto e che possono essere lette da remoto con speciali apparecchi radio).
Quasi 20 anni dopo quei tag si sono trasformati in sensori in grado di leggere dall'ambiente le informazioni più diverse: dalla temperatura, al movimento, alla posizione GPS, al peso di un oggetto o di un corpo, alla composizione chimica, all'umidità del suolo, e di trasmetterle ovunque nel mondo utilizzando i protocolli e le infrastrutture di Internet.
Nel 2011, l'imprenditore e star-

tupper statunitense Marc Andreessen con il suo "In short, software is eating the world" sentenziava al WALL STREET JOURNAL come il mercato dell'epoca si stesse accingendo a vivere una importante transizione. Evidenziava in particolare come le organizzazioni maggiormente virtuose erano quelle che avevano deciso di fondare i propri asset aziendali non solo sulle "macchine" ma soprattutto sui software. Andreesen sottolineava come i più grandi imprenditori dell'epoca avessero intuito che un business "software based", di per sé immateriale, avrebbe permesso loro di conoscere maggiormente la propria azienda e di massimizzarne l'efficienza oltre che i profitti.
Nel 2015, anche il Mckinsey Global institute, società internazionale di consulenza manageriale, nel suo report cavalcava la visione entusiasta ed ottimista dello startupper stimando che entro il 2025 l'IoT avrebbe rappresentato l'11 % dell'economia globale.

ALCUNI ESEMPI DI BUSINESS BASATO SULL'IOT

IL CASO MICHELIN

Anche se è l'esempio sicuramente meno "software based" è certamente il più calzante in quanto ci fa comprendere come l'implementazione di sensori negli oggetti possa trasformarsi in una importante opportunità di business.
Leader nella produzione di pneumatici, Michelin fino a poco tempo fa non sapeva assolutamente nulla dei propri clienti lasciando ai Dealers, disseminati su tutto il territorio, la vendita diretta dei propri prodotti.
Michelin ha introdotto il concetto di "tires as a services" partendo dalle flotte di grandi autocarri, dotando i propri pneumatici di una serie di sensori che consentono di monitorare lo stile di guida e lo stato di usura del pneumatico stesso. Tale implementazione ha portato diversi vantaggi tanto per i clienti quanto per la stessa azienda tra cui:
- **il monitoraggio dei consumi**
- **la prevenzione dei malfunzionamenti**
- **la trasformazione di un bene in un servizio**

IL CASO BIOS INCUBE

Con l'obiettivo di cambiare il modo in cui le persone affrontano la fine della vita, BIOS INCUBE è la prima urna biodegradabile al mondo che ha introdotto l'idea di piantare un

albero con i resti ottenuti dopo la cremazione dei propri cari o animali. Collegata direttamente tramite dei sensori Wireless all'abitazione del possessore e al suo smartphone permette di tenere sotto controllo lo stato di salute della pianta.

BUGS, BUGS EVERYWHERE

Ci sono però molti interrogativi. In particolar modo questi concernono la vulnerabilità dei dispositivi, spesso utilizzati al di fuori di una infrastruttura informatica tradizionale e quindi non dotati di sufficiente sicurezza. Ebbene, tra i molti rischi in cui è possibile imbattersi durante l'utilizzo degli stessi riscontriamo

- **la perdita di dati,**
- **i malware,**
- **l'accesso non autorizzato ai dati,**
- **la sorveglianza illegale.**

Ricordiamoci che gli IOT sono user friendly cioè creati appositamente per dare a tutti la possibilità di utilizzarli immediatamente senza particolari difficoltà. In questo senso è importante che anche gli utenti apportino le cautele necessarie per evitare che gli stessi possano essere "bucati" per esempio impostando misure di sicurezza quali password forti per prevenire possibili hackeraggi.

Cinque trend di cui le aziende dovranno tenere conto durante la pianificazione dei budget per la cybersecurity 2022

A cura di Evgeniya Naumova, Kaspersky

Le aziende che in questo periodo stanno pianificando i budget per il nuovo anno dovranno tenere ancora conto dell'impatto che la pandemia continua ad avere su ogni settore di business. La sempre maggiore digitalizzazione dei processi aziendali imporrà alle organizzazioni di inserire tra le priorità anche gli investimenti in cybersecurity.

Lo scorso anno la pianificazione dei budget è avvenuta alla fine del 2020, nel bel mezzo della pandemia, e questo ha portato molte aziende a muoversi con cautela. Infatti, guardando ai dati dell'ultimo report di Kaspersky IT Security Economics, il budget medio di cybersecurity per il 2021 è rimasto praticamente invariato per le piccole aziende: 267.000 dollari, rispetto ai 275.000 dollari dell'anno precedente. Ma nelle grandi aziende, l'allocazione è diminuita - da 14 milioni di dollari nel 2020 a 11,4 milioni di dollari nel 2021. Anche se l'impatto finanziario delle violazioni di sicurezza informatica non è aumentato significativamente (per le PMI è cresciuto di poco nel 2021, mentre per le enterprise è diminuito del 15%), questo non significa che non sia più necessario prevedere un piano di protezione per le aziende. La violazione dei dati per un'azienda può portare a perdite notevoli come la perdita di contratti o multe, ma anche a perdite indirette come la necessità di richiedere supporto a consulenti di relazioni pubbliche nel caso il breach diventi di pubblico dominio. Dall'indagine di Kaspersky è emerso, infatti, che il costo medio di una violazione dei dati per una enterprise il cui data breach non sia stato diffuso dai media è stato di 827.000 dollari. Sale a 1,2 milioni nei casi in cui la violazione viene divulgata. Nel 2021, il numero di aziende che ha dichiarato di aver subito una violazione dei dati è stato inferiore rispetto agli scorsi anni. Questo si può attribuire agli investimenti significativi in cybersecurity in risposta alle precedenti violazioni dei dati - come il miglioramento dei software e dell'infrastruttura IT o la formazione dei dipendenti – che hanno dato i loro frutti. Un altro tema che rende prioritaria la spesa in cybersecurity è la crescente adozione dei servizi cloud. La nostra ricerca annuale ha dimostrato che, con l'inizio della pandemia, l'uso dei servizi cloud da parte delle aziende è aumentato. Nel 2019, ad utilizzare un servizio cloud – privato, pubblico o infrastrutture desktop virtuali (VDI) - è stato il 72% delle imprese. Nel 2020-2021, questa percentuale è aumentata all'88%. Questo nuovo trend ha portato alla nascita di nuove esigenze per la protezione dell'infrastruttura in-the-cloud e la necessità di dotarsi di soluzioni di cybersecurity dedicate.

Inoltre, il lavoro a distanza e la digitalizzazione dei processi aziendali hanno reso la sicurezza di un'infrastruttura molto più difficile poiché più un sistema diventa complesso e più è difficile tenere traccia di ciò che accade al suo interno. Questo ha portato molte aziende non solo a pianificare ulteriori investimenti in sicurezza ma anche ad affidare la sicurezza a fornitori esterni specializzati. La necessità di una forza lavoro qualificata e di competenze specifiche non è certo una novità ma quest'anno per la prima volta è stata una delle principali motivazioni che ha convinto le aziende a esternalizzare la gestione della cybersecurity aziendale. Infatti, con la rapida adozione di nuove tecnologie e il cambiamento dei modelli di lavoro, combinati con la crescita esponenziale della complessità IT, le imprese di medie e grandi dimensione (52% e 56%) hanno affidato la gestione della sicurezza a un MSP. Non sappiamo con certezza quali nuove sfide porterà il prossimo anno. Nonostante il naturale desiderio umano di voler andare sul sicuro, esiste la grande opportunità di cambiare e prendere decisioni coraggiose. Questo vale anche per il processo di budgeting: l'approccio del "facciamo come l'anno scorso" non fun-

zionerà più. La valutazione e la modellazione del rischio dovrebbero essere fatte in base alle tendenze più recenti, ai cambiamenti che avvengono nell'infrastruttura aziendale e nei processi di business e, soprattutto, in base alle esigenze del business. Andando oltre, per poter mantenere sicuri sistemi specifici, è necessario un nuovo approccio in cui la protezione sia considerata fin dall'inizio dello sviluppo. Questo approccio "secure by design" aiuterà le aziende a raggiungere la Cyber Immunity dalla maggior parte dei rischi.

Anno 3 / Numero 5
2022

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSINTEL CYBER SECURITY

CYBER MAGAZINE

In questo numero:

Fai la cosa giusta:

perché i Responsible Disclosure sono fondamentali

Odio e incitamento:

la proposta europea per estendere l'elenco dei crimini europei di hate speech ad hate crime

Internet Of Things:

c'erano una volta gli oggetti