Accenture. Blackout e hacker, i timori delle utilities per smart grid e reti elettriche

Nel settore delle Utilities il 63 per cento degli executive ritiene che nei prossimi cinque anni il proprio paese possa essere, a vari gradi, esposto al rischio di interruzione dell'erogazione di elettricità a causa di un attacco cibernetico alle reti di distribuzione. Questo dato – che emerge da un nuovo rapporto di Accenture, Outsmarting Grid Security Threats, realizzato nell'ambito del programma di ricerca Digitally Enabled Grid – sale al 76 per cento in Nord America.

L'indagine, svolta su un campione di più di 100 dirigenti di aziende del settore in oltre 20 paesi, evidenzia inoltre che la maggiore preoccupazione a fronte di un attacco informatico sia l'interruzione dell'erogazione di elettricità (il 57 per cento si ritiene molto preoccupato a tale proposito), seguito dalla sicurezza per dipendenti e/o clienti (53 per cento) e dai danni agli asset fisici della rete (43 per cento).



"Il rapido sviluppo di malware sempre più sofisticati e facilmente utilizzabili da cyber criminali costituiscono una chiara minaccia per i sistemi di distribuzione dell'energia elettrica" afferma **Mauro Marchiaro**, Responsabile Settore Energia di Accenture in Italia, Europa Centrale e Grecia. *"In assenza di un'efficace protezione, i ricchi flussi di informazioni trasportati dalle reti digitali potrebbero essere manipolati per causare malfunzionamenti ed interruzioni dell'erogazione di energia elettrica causando disagi, danni economici e commutandosi in una reale minaccia per il paese e l'intera comunità".*

Se da un lato la maggiore connettività dei sistemi di controllo abilitati dalla rete intelligente porterà notevoli benefici in termini di sicurezza, produttività, qualità dei servizi e efficienza operativa, dall'altro l'88 per cento degli intervistati ritiene che la cyber security sia una forte fonte di preoccupazione nello sviluppo delle smart grid.

Inoltre, le utilities sono sempre più esposte alla crescita di dispositivi domestici connessi all'Internet of Things (IoT), quali centraline domestiche e elettrodomestici intelligenti. L'esposizione al rischio introdotto da tali dispositivi in

questo settore è difficile da quantificare, tuttavia il 77 per cento degli interpellati ritiene che l'IoT veicoli nuovi potenziali minacce di natura cyber.

In Asia ed in Europa, circa un terzo degli interpellati vede il rischio principale per le attività di distribuzione nelle azioni da parte di cyber criminali. Per il Nord America invece il pericolo maggiore è rappresentato dagli attacchi da parte dei governi (32 per cento).

"Lo sviluppo della rete intelligente e dell'IoT potrebbe aprire nuove vie d'attacco se la Cyber Security non è parte integrante della sua progettazione", aggiunge Marchiaro. "Le reti intelligenti devono essere dotate di meccanismi di protezione molto sofisticati e complessi in grado di evolvere rapidamente nel tempo ed in grado pertanto di adeguarsi al continuo sviluppo di malware; ciò al fine di garantire un miglior controllo ed al contempo una maggior capacità / velocità di risposta nel ripristino della rete in caso di attacchi cibernetici".

Le Utilities devono rafforzare i propri modelli operativi di cyber security e sviluppare un sistema di distribuzione resiliente

Sono tante le utilities che devono recuperare terreno per sviluppare un sistema robusto di sicurezza informatica, dato che più di 4 interpellati su 10 hanno affermato che i rischi per la cyber security non erano o erano solo parzialmente integrati nei processi di gestione del rischio.

Inoltre, la crescente convergenza fra minacce fisiche e informatiche richiede lo sviluppo di presidi che vanno ben oltre i semplici requisiti nazionali di conformità alla sicurezza. Le utilities devono investire per rendere la loro rete intelligente più resiliente e per sviluppare capacità di

reazione e recupero più efficaci.

Data la complessità delle reti di distribuzione elettrica e il numero crescente di hacker sempre più preparati e con grandi risorse finanziarie, molte utilities non sono adeguatamente protette e preparate. Se si guarda alla capacità di riportare alla normalità le attività della rete dopo un cyber attacco, solo il 6 per cento ha affermato di sentirsi assolutamente preparato e il 48 per cento adeguatamente preparato.



"La cyber security deve diventare una competenza distintiva nel settore, proteggendo l'intera catena del valore e l'ecosistema esteso end-to-end. Le utilities, già esperte nel distribuire in modo affidabile l'elettricità e nelle operazioni di ripristino, necessitano di agilità e rapidità nel creare un'adeguata consapevolezza di fronte a un attacco informatico e far leva sulla stessa per intervenire prontamente e proteggere la rete", afferma **Paolo Dal Cin, Responsabile di Accenture Security per Italia, Europa Centrale e Grecia**. *"Lo sviluppo di questa nuova capacità richiederà innovazione costante, oltre a un approccio pratico alla scalabilità e alla collaborazione con i partner per realizzare valore".*

Interventi per costruire e scalare la difesa informatica

Anche se non c’è una sola strada per procedere, ci sono alcuni interventi che ogni utility dovrebbe considerare per rafforzare la resilienza e il responso ai cyber attacchi, fra cui:

- Integrazione della resilienza nella progettazione delle risorse e dei processi, con l’inclusione della sicurezza fisica e informatica;
- Condivisione di dati e informazioni come attività indispensabile per aiutare a creare consapevolezza sul panorama delle minacce informatiche e su come prepararsi di conseguenza
- Sviluppo di modelli di governance della gestione della sicurezza e delle emergenze.

Il programma di ricerca annuale Digitally Enabled Grid di Accenture valuta le implicazioni e le opportunità di una rete sempre più digitale. Lo studio del 2017 contiene interviste con più di 100 dirigenti di utility di oltre 20 paesi. I dirigenti intervistati sono coinvolti nel processo decisionale per le questioni relative alle reti intelligenti. I paesi rappresentati sono Arabia Saudita, Australia, Belgio, Brasile, Canada, Cina, Emirati Arabi Uniti, Filippine, Germania, Giappone, Italia, Malesia, Norvegia, Olanda, Portogallo, Regno Unito, Spagna, Stati Uniti, Sudafrica, Svizzera, Tailandia.

Accenture. Blackout e hacker, i timori delle utilities per smart grid e reti elettriche

Android, scoperto malware che ascolta le conversazioni. Le vittime tutte in Italia

È in grado di ascoltare le conversazioni sugli smartphone **Android** e di origliare tutto ciò che accade nell'ambiente circostante. In più ha nel mirino anche gli utenti **Windows**. Il *malware* è stato scoperto dai ricercatori di **Kaspersky Lab** ed è stato chiamato **Skygofree** perché deve il proprio nome a una parola usata in uno dei domini: non ha legami con **Sky**, Sky Go o qualsiasi altra società controllata da Sky e non coinvolge il servizio o l'app Sky Go.

Skygofree è uno spyware sofisticato e multilivello che concede ai cyber criminali il pieno controllo remoto del dispositivo infettato.

Skygofree come fa a spiare?

Dopo la creazione della prima versione alla fine del 2014, ha subìto costanti aggiornamenti e ora include la possibilità di "origliare" le conversazioni e i rumori dell'ambiente circostante quando il dispositivo entra in un luogo specifico – una funzionalità che non era mai stata trovata in *the wild*. Altre innovative funzionalità avanzate includono la possibilità di usare le impostazioni di accessibilità per rubare i messaggi **WhatsApp** e la capacità di collegare il dispositivo infettato alle reti wi-fi controllate dai cyber criminali.

Il malware include diversi *exploit* per ottenere i permessi di *root* ed è in grado di catturare immagini e registrare video, ottenere l'elenco delle chiamate, SMS, informazioni sulla geolocalizzazione, eventi nel calendario e dati aziendali archiviati nella memoria del dispositivo. Una funzionalità

speciale consente di aggirare una funzionalità per il risparmio della batteria implementata da uno dei maggiori vendor: il malware si inserisce nell'elenco delle "app protette" per non venire disattivato automaticamente quando lo schermo è spento.

Malware progettato da un'azienda italiana e le vittime colpite tutte nel nostro Paese

I cyber criminali sembrano interessati anche agli utenti **Windows** e i ricercatori hanno scoperto diversi moduli sviluppati recentemente che prendono di mira questa piattaforma.

La maggior parte delle *landing page* nocive usate per diffondere il malware sono state registrate nel 2015, quando, secondo la telemetria di *Kaspersky Lab*, la campagna di distribuzione è stata più attiva. La campagna nociva è ancora in atto e il dominio più recente è stato registrato a ottobre 2017. I dati indicano che attualmente sono state colpite diverse vittime, tutte in Italia.

"I malware mobile di alto profilo sono estremamente difficili da identificare e bloccare e gli sviluppatori di Skygofree hanno sfruttato questo fattore a proprio vantaggio, creando e sviluppando uno spyware in grado di spiare gli obiettivi senza destare sospetti. In base agli artefatti scoperti nel codice del malware e alla nostra analisi dell'infrastruttura, siamo piuttosto sicuri che il malware Skygofree sia stato sviluppato da un'azienda IT italiana che offre soluzioni di sorveglianza, come HackingTeam", ha commentato **Alexey Firsh**, Malware Analyst, Targeted Attacks Research, di Kaspersky Lab.

I ricercatori hanno scoperto 48 comandi differenti che possono essere implementati dai criminali, offrendo la massima flessibilità d'uso.

Come proteggersi

Per proteggersi dalle minacce mobile più avanzate, Kaspersky Lab consiglia fortemente di implementare una soluzione di sicurezza affidabile in grado di identificare e bloccare queste minacce sugli *endpoint*. Gli utenti dovrebbero inoltre fare attenzione alle email ricevute da persone o aziende sconosciute o con richieste o allegati inattesi – e verificare sempre l'integrità e l'origine dei siti web prima di cliccare sui link. In caso di dubbio, è sempre meglio chiamare il service provider per una verifica. Gli amministratori di sistema, a loro volta, dovrebbero attivare la funzionalità di *Application Control* della propria soluzione di sicurezza mobile per controllare i programmi potenzialmente dannosi vulnerabili a questi attacchi.

Le soluzioni Kaspersky Lab rilevano le versioni di Skygofree per Android come HEUR:Trojan.AndroidOS.Skygofree.a e HEUR:Trojan.AndroidOS.Skygofree.b e i sample per Windows come UDS:DangerousObject.Multi.Generic.

https://www.key4biz.it/android-scoperto-malware-ascolta-le-conversazioni/210112/

---

38 previsioni sulla cybersecurity nel 2018

Le 38 previsioni che seguono sono il frutto di dichiarazioni di analisti, manager e tecnici di importanti società del settore, raccolte sulla base dei temi caldi della cybersecurity: gli attacchi alle autorità governative e alle infrastrutture critiche, la determinazione dell'autenticità nell'era delle **fake news**, la privacy dei consumatori e il

GDPR, l'Internet of Things, l'intelligenza artificiale intesa come nuovo tool nelle mani dei criminali informatici quanto in quelle di chi si occupa della protezione dal cybercrime, le **criptovalute**, la biometrica, la crescita delle imprese IT e della cybersecurity, la persistente carenza di competenze digitali.

Attacchi alle autorità governative e alle infrastrutture critiche

La tensione tra Stati Uniti e Corea del Nord vedrà un'escalation online, diventando una guerra sulla sicurezza informatica. La Corea del Nord ha un vantaggio "difensivo" grazie allo stretto controllo della rete del suo Paese, e inoltre la Cina e la Russia non prenderanno parte a questa guerra a causa dei reciproci legami e interessi.

Gli analisti prevedono il diffondersi di attacchi simili alla strategia utilizzata dai russi: campagne di phishing mirate e accompagnate da "fake news" sui social, nel tentativo di destabilizzare gli avversari.

Soprattutto negli ultimi mesi si sono registrati sempre più diffusi furti di dati a danno di aziende di settori critici quali energia, nucleare, acqua, aviazione e costruzioni. Le industrie delle infrastrutture critiche sono in ritardo nella preparazione delle loro strutture operative per affrontare gli attacchi informatici – e questo le rende un facile bersaglio per aggressori politicamente motivati.

È molto probabile che nel 2018 assisteremo a importanti violazioni delle procedure online di agenzie governative. Potrebbero presentarsi sotto forma di violazione dei dati personali, manomissione di siti web, disattivazione di sistemi interni o di una combinazione di questi attacchi. Sappiamo che i governi sono obiettivi e gli attori delle minacce sono implacabili.

La determinazione dell'autenticità nell'era delle fake news

Le notizie false sono diventate un grosso problema nel 2017 che probabilmente peggiorerà nel 2018. Con la tecnologia CGI, Photoshop e voice-over, è quasi impossibile stabilire se una foto o un video siano reali o falsi. Soluzioni come le firme digitali e la crittografia abilitate su dispositivi di registrazione fidati potrebbero aiutare a combattere questo problema, ma l'industria delle macchine fotografiche deve includere queste opzioni sulle apparecchiature utilizzate dai mezzi di informazione.

Per fronteggiare le fake news, l'industria tecnologica svilupperà uno schema di gestione della reputazione che permetterà alle persone di verificare la propria identità attraverso un'operazione che registra un'interazione che solo un umano può avere. Questo schema di reputazione sarà universale e seguirà un individuo attraverso piattaforme, domini e siti online, anche se la persona desidera rimanere anonima.

La privacy dei consumatori e il GDPR

La privacy e la sicurezza dei dati sono stati a lungo considerati due missioni distinte con due obiettivi separati, ma tutto cambierà nel 2018. Con l'entrata in vigore dei regolamenti globali seri e con l'aumento delle risposte normative alle violazioni dei dati, le organizzazioni costruiranno una nuova gestione dei dati incentrata sul controllo di essi, monitorando chi vede i dati, in quale stato e per quale scopo.

Il 2018 dimostrerà che la sicurezza informatica senza privacy è un ricordo del passato.

Nel 2017 ci sono state numerose violazioni su larga scala che coprivano tre aree chiave: informazioni sanitarie sensibili, informazioni sulle autorizzazioni governative e dati finanziari e di credito. Nel 2018, questo genere di dati potrebbero essere resi disponibili sul *dark web* in modo

aggregato, dando a qualsiasi individuo o gruppo l'opportunità di condurre attacchi su piccola scala e altamente mirati come la corruzione, o causando atti illegali.

Nel 2018 alcune istituzioni finanziarie cominceranno a utilizzare i chatbot per facilitare i pagamenti e attireranno i criminali informatici che impersoneranno i veri utenti e acquisiranno i loro account, eventualmente utilizzando l'accesso remoto nel normale PC dell'utente per neutralizzare qualsiasi riconoscimento basato sui dispositivi.

Assisteremo ad un aumento della legislazione e dei regolamenti sul modello del GDPR. Lo stato di preparazione e applicazione del nuovo regolamento saranno le principali preoccupazioni informatiche per i dirigenti e le organizzazioni aziendali. Con il nuovo GDPR, l'Ue è diventata un precursore della privacy dei dati globali e anche altri paesi cercheranno di allinearsi alle leggi sulla privacy dell'Unione Europea.

L'assistenza sanitaria è diventata un obiettivo di alto valore in quanto la tecnologia in questo settore è molto variegata ed è collegata a reti in ritardo dal punto di vista della sicurezza. Si prevedono altri attacchi *ransomware* che potrebbero avere un impatto sulla cura del paziente o sui dati dei pazienti.

Internet of things (IoT)

I marchi globali stanno cominciando a implementare IoT, aprendo nuove falle nei nostri già malconci spazi informatici. Gli hacker continueranno a sfruttare i **dispositivi non protetti** per spiare gli utenti e irrompere nelle reti domestiche e aziendali. *Botnet* multipli che sfruttano dispositivi IoT vulnerabili saranno nuovi veicoli negli attacchi DDOS e minacceranno di smontare le notizie e i siti web governativi. I produttori IT dovranno affrontare queste vulnerabilità di sicurezza o rischiano di perdere il confronto con aziende tecnologicamente più affidabili. Il GDPR potrebbe

accelerare questo processo, costringendo le aziende a riconsiderare la raccolta di dati personali tramite IoT, ma non vedremo effetti su questo fronte almeno fino al 2019.

Il 2018 sarà un anno impegnativo per **l'industria IoT**. Gli hacker sanno che queste aziende sono online e connesse più che mai, il che aumenta la loro vulnerabilità. La sicurezza è fondamentale, perché un hack potrebbe significare vita o morte per i consumatori. Ad esempio, se la catena di montaggio di un costruttore di automobili è stata compromessa, potrebbe causare malfunzionamenti del veicolo, mettere in pericolo i passeggeri e causare problemi di reputazione e di responsabilità per l'azienda produttrice. Per queste ragioni, inizieremo a vedere più aziende che si occupano di sicurezza informatica con soluzioni specifiche per mercati verticali. Per gestire efficacemente questo nuovo corso, le organizzazioni che si occupano di IoT dovranno aumentare gli investimenti sulla cybersecurity.

Dal 2015 abbiamo assistito a un'enorme diffusione **degli usi commerciali dei droni**: rilevamento delle costruzioni, rilevamento delle mine, servizi di consegna, monitoraggio agricolo, valutazione di disastri e assicurazioni, ecc. Questi dispositivi economicamente accessibili (possono costare anche pochi euro), sono guidati da un pilota collegato o tramite un sistema autonomo: in entrambi i casi suscettibili di influenza o interruzione da parte di attori esterni. I produttori di droni sono ora in una gara per creare la "GoPro" del settore dei droni, il prodotto che definisce l'intero mercato, e in questa gara la sicurezza sarà probabilmente determinante.

Le **case intelligenti** (*smart home*) sono la tendenza più recente a cresceranno a passi da gigante quest'anno. E' possibile collegare qualsiasi cosa alle nostre reti domestiche: luci, tostapane, serrature, telecamere, termostati e persino frigoriferi. Gli hacker possono sfruttare vulnerabilità sconosciute dei dispositivi connessi per violare le reti domestiche o per ottenere l'accesso non autorizzato alle

abitazioni senza dover ricorrere ai metodi tradizionali di irruzione in casa.

Intelligenza Artificiale e Machine Learning

La modalità di utilizzo dell'Intelligenza Artificiale da parte dei buoni e dei cattivi muterà. La sicurezza informatica è una corsa agli armamenti e la parte più debole ricorre a mezzi asimmetrici per raggiungere i suoi obiettivi. Alla stregua delle organizzazioni che stanno adottando l'apprendimento automatico e l'intelligenza artificiale per migliorare la loro sicurezza informatica, anche i criminali informatici svilupperanno la stessa strategia. Gli aggressori stanno utilizzando l'apprendimento automatico per accelerare il processo di individuazione delle vulnerabilità nei prodotti commerciali, con il risultato che gli aggressori useranno sempre nuovi *exploit* senza che vi sia traccia dell'utilizzo dell'AI nella loro creazione. L'intelligenza artificiale aumenterà anche il numero di professionisti della cybersicurezza qualificati, in quanto riduce le barriere all'ingresso nella professione e consente agli individui meno preparati di essere efficaci nell'arena della sicurezza informatica.

In generale, più criminali useranno l'intelligenza artificiale e l'apprendimento automatico per condurre i loro crimini. Il *ransomware* sarà automatico e il furto bancario sarà condotto da bande organizzate che utilizzano l'apprendimento automatico per condurre i loro attacchi attraverso modalità più intelligenti. I gruppi più piccoli di criminali saranno in grado di causare maggiori danni utilizzando queste nuove tecnologie per violare le aziende e rubare i dati. Allo stesso tempo, le grandi imprese si rivolgeranno all'AI per rilevare e proteggersi contro nuove minacce sofisticate. L'intelligenza artificiale e l'apprendimento automatico consentiranno loro di aumentare i tassi di rilevamento e di ridurre drasticamente i falsi allarmi.

Le stesse tecnologie che migliorano le difese aziendali saranno probabilmente utilizzate per attaccarle. I progressi nell'AI e nell'apprendimento automatico sono un'arma a doppio taglio, migliorano l'esperienza del prodotto ma sono anche utili per hacker e cybercriminali.

L'analisi basata sull'intelligenza artificiale dei dati biometrici comportamentali sarà la prossima grande tendenza della sicurezza informatica e della protezione dei dati. Gli algoritmi sofisticati di apprendimento automatico sono in grado di costruire un profilo del comportamento tipico di un utente, identificare modelli di attività insoliti ed evidenziare potenziali minacce in tempo reale, prima che abbiano la possibilità di materializzarsi. Identificando automaticamente i dati sospetti, l'intero processo di sicurezza diventa più efficiente, ovviando alla necessità di una scrupolosa revisione manuale dei dati registrati.

Criptovalute

La *Cryptocurrency* è stata una "killer app", anche in negativo, e ha consentito e alimentato la crescita del *ransomware* e delle relative minacce di riscatto nel 2017. Nel 2018 questo fenomeno continuerà a crescere includendo l'identità per il riscatto. Gli utenti riceveranno e-mail o telefonate in cui sapranno che i loro dati sono stati rubati e poi saranno istruiti a pagare tramite bitcoin per impedire che i vengano trafugati o diffusi.

Nel 2018, una vulnerabilità importante farà cadere il valore di una delle criptovalute più popolari, causandone l'effettiva "morte". Le criptovalute, tra cui Bitcoin, Ethereum, Litecoin e Monero, mantengono un capitale di mercato miliardario, il che le rende un obiettivo più attraente per gli hacker man mano che il loro valore di mercato aumenta. È possibile che nel 2018 un importante attacco contro una di queste criptovalute danneggerà la fiducia del pubblico.

Un’altra grave violazione dello scambio di criptovalute potrebbe portare a un sostanziale declino del valore di Bitcoin e di altre principali criptovalute. Vedremo maggiore coinvolgimento dei governi con normative che inizino a rimuovere alcuni dei principi fondamentali intorno all’anonimato per ridurre l’uso fraudolento delle criptovalute. Le banche saranno le prime a creare una valuta regolamentata seguite da Russia e Cina e plausibilmente dalle 5 grandi aziende tecnologiche.

Biometrica e autenticazione multi-fattore

Le password sono uno strumento impersonale e inadeguato per la sicurezza, impersonali e mettono gli utenti in difficoltà per dimostrare l’identità. Con il lancio di Face ID, dopo l’enorme successo dei lettori di impronte digitali negli iPhone e nei dispositivi Android, vedremo altre funzionalità di autenticazione biometrica pronte per il consumatore. In combinazione con i progressi nell’autenticazione push (Google ha appena impostato l’autenticazione tramite SMS) e la massa dei dati del dispositivo, vedremo finalmente i nostri dati biometrici sempre più connessi alle nostre identità digitali.

Nel 2018, si comincerà a ragionare oltre l’autenticazione a due fattori per considerare le prospettive per la salvaguardia dei nostri sistemi. Le organizzazioni inizieranno ad adottare strumenti automatici per analizzare la loro presenza sui social media per minacce e comportamenti sospetti, proprio come fanno ora sulla rete aziendale. Inoltre, il metodo tradizionale di formazione dei dipendenti diventerà ancora più cruciale per le organizzazioni.

Uso crescente dell’autenticazione multi-fattore e biometrica: attraverso la maturazione di tecnologie come i chip neurali e l’apprendimento approfondito, stiamo riscontrando miglioramenti significativi nell’accuratezza e affidabilità di una varietà di dati biometrici che possono rendere l’autenticazione di conducenti, passeggeri e terze parti come

servizi di consegna, rivenditori, personale di servizio, ecc. più sicuri e più convenienti. Man mano che diventano più economici e più efficaci, le tecnologie di autenticazione più forti possono essere incorporate nei veicoli e persino nelle infrastrutture, consentendo nuove modalità di commercio "senza attrito". Apple Face ID è un esempio, in cui la possibilità di accesso non autorizzato è diminuito da 1 su 10.000 per le impronte digitali Touch ID a 1 su 1.000.000 per il riconoscimento facciale. Inoltre, la varietà di dati biometrici si sta espandendo oltre i metodi più tradizionali come impronte digitali o riconoscimento facciale e voce a cose come l'andatura e persino la forma del cuore. Insieme alla fusione dei sensori, è possibile combinare una varietà di dati biometrici per fornire un'autenticazione forte con il minimo inconveniente.

Il 2018 sarà un anno interessante per la biometria con il passaggio da Apple a Face ID su iPhone. Sarà probabilmente la più grande adozione della tecnologia di riconoscimento facciale nella storia. È interessante vedere il mercato dei consumatori guidare il mercato delle imprese nell'adozione della biometria. I principali fornitori di smartphone stanno rendendo più facile per il mercato aziendale spostarsi verso una password senza password.

Crescita delle imprese dell'IT e della cybersecurity

Gli hacker inizieranno a esaminare i *mainframe* come una futura fonte di attacchi. Trascurata dai team di sicurezza, la cui attenzione viene assorbita per proteggere le ultime innovazioni mobili o basate su cloud, i *mainframe* sono l'epicentro dei servizi finanziari per migliaia di organizzazioni globali tra cui 92 delle 100 più importanti banche del mondo. Questi sistemi attualmente supportano 29 miliardi di transazioni ATM al giorno e l'87% di tutte le transazioni con carta di credito. I *mainframe* possono anche essere utilizzati per diversi scenari di attacco, in particolare lo spionaggio. Da una singola posizione, un utente

malintenzionato potrebbe raccogliere importanti informazioni competitive o strategiche.

Nel 2018, i criminali informatici sfrutteranno i software di sicurezza e gli antivirus. Puntando su questi programmi e sulla catena di fornitura di software e hardware, gli hacker possono assumere il controllo dei dispositivi e manipolare completamente gli utenti. Così, però, la percezione del pubblico e del business dei software di sicurezza, e in particolare delle soluzioni antivirus, si deteriorerà ulteriormente.

Il ransomware aziendale diventerà una tendenza importante. Gli attacchi dirompenti e distruttivi sono venuti alla ribalta nel 2017 con le epidemie di malware *WannaCry*, *NotPetya* e *BadRabbit* che hanno costretto le aziende offline per giorni e, in alcuni casi, persino per settimane. Questi attacchi hanno evidenziato il potenziale per gruppi criminali di trattenere intere reti in ostaggio chiedendo milioni di dollari di riscatto. Questi attacchi virali "enterprise ransomware" diventeranno probabilmente una delle principali tendenze tra gli attori e-crime nel 2018.

Nel 2017, le frodi **e-commerce** sono aumentate del 300-600% rispetto ai tassi di frode nel 2016. Il tasso di frode è cresciuto considerevolmente soprattutto a partire da luglio 2017, contemporaneamente alla violazione di *Equifax*. Questa crescita drammatica dei tassi di frode varia in base al settore, e tuttavia l'aumento è direttamente correlato con le recenti violazioni dei dati, in cui i truffatori hanno accesso a e-mail e password dei consumatori e li utilizzano per effettuare acquisti prima che il consumatore abbia realizzato il furto. Nel 2018, possiamo aspettarci che i cyber-criminali continueranno a indirizzare le aziende con strategie sempre più sofisticate e i rivenditori dovranno rispondere con misure di protezione maggiori come il *machine learning* e la biometria.

Il panorama complessivo della sicurezza nel 2018 sarà incentrato su due aspetti: il *cloud* e l'IoT. Ognuno di questi porta a una sfida globale per i team di sicurezza: scalare le proprie soluzioni di sicurezza per mantenere il passo con l'enorme richiesta di banda. La rapida decentralizzazione della forza lavoro e delle applicazioni cloud aziendali aumenterà esponenzialmente la complessità, poiché proteggere questa larghezza di banda distribuita rappresenterà una sfida se si utilizza un approccio centralizzato alla sicurezza informatica. Le organizzazioni dovranno trovare rapidamente una soluzione in grado di proteggere questa enorme quantità di larghezza di banda improvvisamente senza dover affrontare aumenti di costo proibitivi.

Le tecniche standardizzate di hacking renderanno l'identificazione dei colpevoli ancora più difficile: nel 2018, più operatori di minacce adotteranno strumenti progettati per rimuovere qualsiasi segno rivelatore dei loro attacchi. Ad esempio, vedremo le *backdoor* con meno funzionalità e diventeranno più modulari, creando impronte di sistema più ridotte e rendendo l'attribuzione più difficile a tutti i livelli. E, poiché un'attribuzione accurata diventa più impegnativa, la porta viene aperta per attacchi informatici ancora più ambiziosi e campagne di influenza da parte sia degli stati-nazione che dei criminali informatici.

La persistente carenza di competenze in tema di sicurezza informatica

Nel 2018 il ruolo del CISO continuerà ad evolversi per comprendere la politica pubblica, l'applicazione della legge, la privacy e una comprensione del panorama delle minacce.

Secondo una recente ricerca, solo l'11% della forza lavoro mondiale per la sicurezza delle informazioni è costituita da donne. Un certo numero di organizzazioni sono dedicate ad aiutare le donne ad avere successo nella sicurezza informatica, come la *Women's Society of Cyberjutsu (WSC)*.

Nel 2018, un numero maggiore di aziende adotterà un approccio basato sulla sicurezza. Immagina un fossato che circonda un castello, proteggendo il re, la regina e altri abitanti dagli invasori. Solo in questo caso, invece delle persone, si hanno informazioni personali identificabili (PII), file proprietari, capitale intellettuale, informazioni mediche, documenti legali e altre informazioni che dovrebbero essere viste e condivise solo con le persone e le organizzazioni autorizzate. Per adottare tale cultura nella tua organizzazione, sarà sempre più necessario diffondere i temi della sicurezza con campagne di sensibilizzazione periodiche, attacchi di sicurezza simulati (con phishing o altri vettori di attacco) e migliori politiche di conservazione della documentazione per gestire e crittografare i dati chiave.

L'attuale carenza di competenze in sicurezza informatica è davvero massiccia e nel 2018 si amplierà. Il settore continuerà a richiedere una serie diversificata di competenze man mano che i progressi della strategia di resilienza cibernetica. Le organizzazioni inizieranno a considerare i ruoli non tradizionali, l'esperienza e l'educazione, basati sull'atteggiamento e l'attitudine giusti, per colmare queste tanto necessarie posizioni di sicurezza informatica.

Le aziende creeranno il proprio talento informatico: man mano che la carenza di cyber-competenze continua ad aumentare, le imprese riconosceranno la necessità di creare il proprio talento cyber piuttosto che aspettare che appaia. Nel 2018, le organizzazioni diventeranno più proattive nell'affrontare il divario tra cyber-talento e implementare la formazione interna per creare più talento. Le aziende inizieranno anche a spingere il dialogo pubblico verso un'istruzione più cybernetica in età precoce.

Fonti: *The Cyber Avengers, DomainTools, Cyberbit, Dyadic, Gigamon, Immuta, West Monroe Partners, BioCatch, TrustArc, Attivo Networks, Carousel Industries, American Express Global Business Travel, Duck Creek Technologies, Varonis, Safe-T,*

Thales eSecurity, Enlightened, Enlightened, Vectra, ThetaRay, PKWARE, Balabit, ProtectWise, IntSights, WatchGuard Technologies, Aperio Systems, Webroot, Twilio, ZeroFOX, TrustArc, Lumileds, Cisco, SecureAuth, Illusive Networks, Attivo Networks, ProtectWise, Malwarebytes, SiteLock, CrowdStrike, Nyotron, Radial, Signal Sciences, Cylance, SAP, ObserveIT, GigaTrust.

Articolo tratto dall'eBook di key4biz' **I Tech trend 2018**'. Per scaricare l'eBook clicca qui.

38 previsioni sulla cybersecurity nel 2018

Information security, la spesa globale nel 2018 sarà di 93 miliardi di dollari

I costi della criminalità informatica continuano a guidare la domanda di prodotti e servizi in ambito informatico. Secondo Cybersecurity Ventures, il mondo subirà 6 trilioni di dollari in danni dai cybercriminali ogni anno entro il 2021, rispetto ai 3 trilioni di dollari nel 2015.

Secondo le previsioni, si prevede che la spesa per la sicurezza informatica globale superi 1 trilione di dollari nei prossimi tre anni, dal 2018 al 2021.

Inoltre, le ultime previsioni di **Gartner** indicano che la spesa per la **sicurezza delle informazioni** a livello mondiale aumenterà del 7% fino a raggiungere quest'anno la quota di 93 miliardi di dollari di investimenti.

La previsione di Gartner si concentra sulla sicurezza IT corporate, e comprende categorie quali; managment dei servizi di sicurezza, la consulenza e implementazione, protezione dell'infrastruttura, applicazioni dei test di sicurezza, prevenzione della perdita dei dati (DLP), protezione degli endpoint, informazioni sulla sicurezza e gestione degli eventi (SIEM), sicurezza email e web, governance e amministrazione dei dati.

Il segmento di sicurezza consumer del mercato coperto dalle previsioni di Gartner comprende suite di prodotti per la sicurezza degli endpoint, tra cui antivirus, anti-spyware, firewall personali e sistemi di prevenzione dal attacchi hacker basati su host (HIPS), controllo parentale, rilevamento delle frodi, più antivirus per desktop e abbonamenti venduti o noleggiati al per gli uffici e per uso domestico.

La sicurezza nell'IoT e la sicurezza Industrial Control Systems (ICS) saranno i mercati in più rapida crescita. Insieme, si stima che solo quei due settori della sicurezza valgano al rialzo di un totale di 43 miliardi di dollari all'anno entro il 2022, secondo le recenti ricerche di mercato.

Nel complesso, si prevede una crescita del mercato della cybersecurity anno dopo anno pari al 12-15%.

Nell'ambito del settore della sicurezza delle informazioni, si ha un notevole coinvolgimento dei consigli di amministrazione delle grandi aziende, a causa dei mandati regolatori imminenti come l'ingresso del GDPR nel maggio 2018.

"La crescente consapevolezza tra amministratori delegati e consigli di amministrazione sull'impatto commerciale negativo a causa di incidenti di sicurezza informatica e un panorama normativo in evoluzione hanno portato a spese continue per prodotti e servizi di sicurezza", ha affermato **Sid Deshpande**, analista principale di Gartner Singapore.

Inoltre e conclude, *“le organizzazioni possono migliorare significativamente la propria posizione semplicemente affrontando elementi di igiene fondamentali legati alla sicurezza come la gestione delle vulnerabilità incentrate sulle minacce, la gestione centralizzata dei registri, la segmentazione interna della rete, i backup e il rafforzamento del sistema”.*

Secondo Gartner, i servizi di sicurezza continueranno ad essere il segmento con più rapida crescita, in particolare l’outsourcing IT, i servizi di consulenza e implementazione. Questo causerà la carenza di forza lavoro legata alla sicurezza informatica. Entro il 2021 ci saranno 3,5 milioni di posti di lavoro nella rispetto a 1 milione di posti presenti nel 2014.

> *Information security, la spesa globale nel 2018 sarà di 93 miliardi di dollari*

Cybersecurity, i 9 articoli più letti del 2017

Il 2017 è stato l’anno degli attacchi informatici, che hanno rappresentato un *vulnus* ai dati dei cittadini, delle imprese e dello Stato. Dal *Ransomware* che prende “in ostaggio” Pc e smartphone chiedendone il riscatto in bitcoin fino ai casi più eclatanti di **Bad Rabbit**, **Petya** e **Wannacry**.

Ecco i 9 articoli più letti quest’anno sulla cybersecuriy.

Cybersecurity: come difendere i router dal rischio hacker

Router e web cam su rete IP vanno costantemente difesi con l'aggiornamento dei parametri di sicurezza per evitare che diventino portatori di attacchi informatici. Vincenzo Luciano Lucrezia (TIESSE): 'Certo l'operazione di cambio password da sola non garantisce l'immunità'.

PA digitale, in Gazzetta le misure minime di cybersecurity da adottare entro il 2017

Pubblicate in Gazzetta Ufficiale le misure minime di sicurezza ICT che tutte le amministrazioni pubbliche dovranno adottare entro fine anno.

Cybersecurity, Gentiloni vara decreto e piano nazionale anti-hacker

Il decreto attribuisce al direttore generale del Dipartimento delle informazioni per la sicurezza, Alessandro Pansa, il compito di proteggere i sistemi e le reti di interesse strategico, sia pubblici sia privati: sì al coinvolgimento di università e ricerca.

Cybersecurity, cosa fare dopo l'attacco 'WannaCry' nei vademecum della Polizia postale e dell'AgID

Online le guide del Cnaipic e dell'AgID per proteggere i nostri computer dal malware "Wannacry o WCry". La situazione in Italia, a livello mondiale e le previsioni: "Non abbassare la guardia, non si escludono altri attacchi".

I 5 malware più diffusi in Italia (il primo viaggia su Chrome)

Si chiama ‘Submelius’ il virus più diffuso in Italia nel mese scorso, colpisce specialmente siti famosi per la visione di film online. Ha minacciato 4 utenti su 10 e viaggia attraverso Google Chrome. Ecco come rimuoverlo.

Cybersecurity, la situazione italiana e gli scenari futuri: la relazione del Ce.S.I.

Vi proponiamo alcune riflessioni sull’evoluzione del quadro di sicurezza in ambito cyber nel nostro Paese, sviluppate dal Ce.S.I. (Centro Studi Internazionali) in occasione dell’audizione presso la Commissione Difesa della Camera dei Deputati.

CeBIT 2017, i consigli di Edward Snowden per la cybersecurity dell’Internet delle cose

Secondo Snowden, l’ex agente dell’Nsa: “Si devono offrire sul mercato soluzioni per la trasparenza e l’affidabilità”. Il 40% degli oggetti connessi in ambiente IoT sarà aziendale. “I produttori devono introdurre livelli di sicurezza tali da rendere più costose le operazioni di hackeraggio”.

Cybersecurity, Firefox e Chrome: ‘lucchetto verde e rosso’ per siti sicuri e non

Per garantire una navigazione online più sicura i browser Firefox e Chrome hanno pensato bene di utilizzare una sorta di semaforo, un lucchetto verde per un sito sicuro e un lucchetto rosso per una pagina web rischiosa.

Cybersecurity, Italia nella top ten dei Paesi sott’attacco. Fake news +117% nel 2016

Rapporto Clusit: ‘Il 2016 è stato l’anno peggiore nell’evoluzione dei cyberattack: Sanità e Banking i settori più colpiti’. Internauti troppo ingenui con le mail: Phishing globale +1.166% in un anno.

Cybersecurity, i 9 articoli più letti del 2017

Direttiva europea NIS e GDPR, attuazione e bug applicativi nel mercato digitale

La prossima attivazione dei due dispositivi normativi del 2016 per la **sicurezza cibernetica** e la protezione dei dati, prevista per maggio 2018, sollecita una riflessione sulle complesse logiche e intersezioni applicative sottese che potrebbero comportare una rivoluzione del mercato digitale nazionale ed europeo come lo conosciamo.

Lo scenario quantitativo degli attacchi *cyber* segnala tendenze preoccupanti: l’80% delle aziende europee ha subito almeno un incidente *cybersecurity* nel 2015 e nello stesso anno Il numero di incidenti di sicurezza per tutte le industrie nel mondo è cresciuto del 38%.

Per il 2016-2017 il Rapporto **CLUSIT** ci informa che la tendenza è drammaticamente peggiorativa.

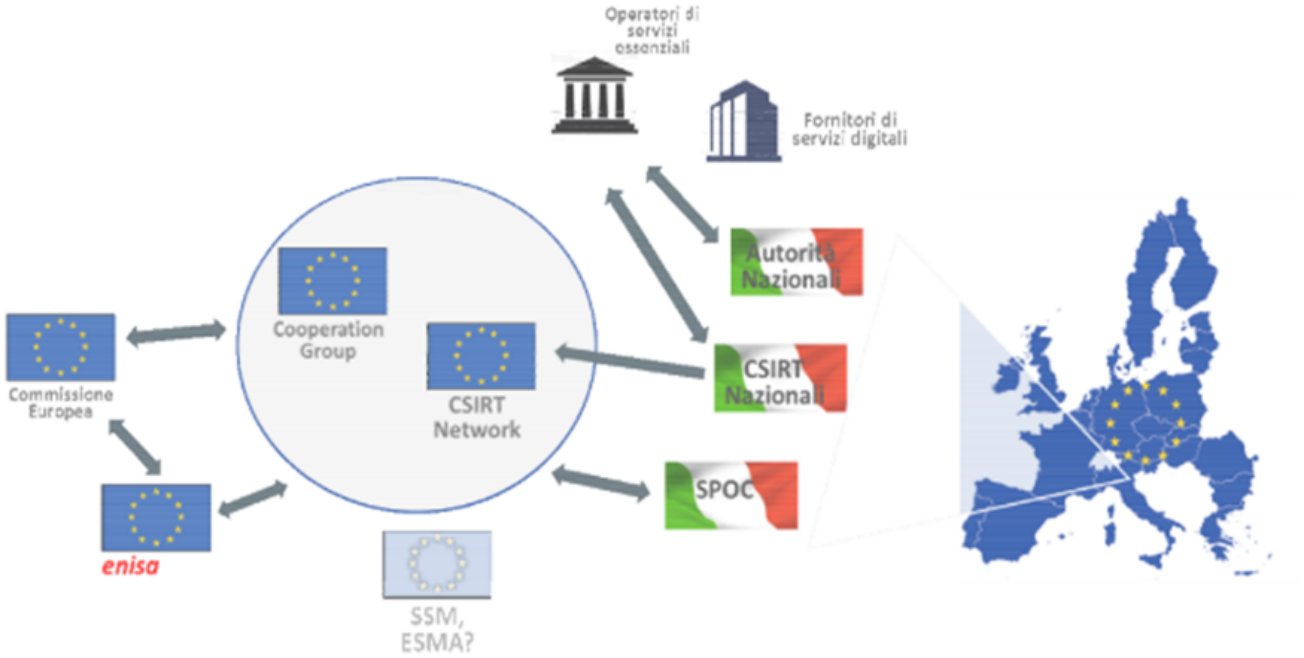
In questo scenario, la **Direttiva UE 2016/1148** del 6 luglio 2016 (per brevità NIS, sicurezza delle reti e dei sistemi informativi) e il **Regolamento generale sulla protezione dei dati** (**GDPR**) intervengono a normare da un lato l'ambito dell'economia digitale più gravemente esposto per le conseguenze agli attacchi *cyber*, quello delle cosiddette 'infrastrutture critiche' cui sono correlati i *vendor* di soluzioni digitali con relativi obblighi e sanzioni; dall'altro quello relativo ai dati 'personali' detenuti da enti, aziende, studi professionali, ecc. oggi rivisitato alla luce del mercato dei dati anch'esso connesso all' obbligo della difesa *cyber*.

Veniamo, anzitutto, a riassumere le logiche attuative per la NIS: scadenze, soggetti attuatori, competenze e tipologie di soggetti aziendali cui perterranno obblighi di *compliance* ovvero gli operatori di servizi essenziali e i fornitori di servizi digitali.

Ricordiamo, anzitutto, le scadenze:

- la Direttiva NIS è in vigore da agosto 2016 e in attesa di recepimento dagli stati membri della UE;
- gli stati membri hanno 21 mesi per adottare le necessarie misure di implementazione a livello di legislazione nazionale e 6 mesi supplementari per identificare gli operatori delle infrastrutture critiche nazionali;
- la scadenza per il recepimento è il 9 maggio 2018;
- nella transizione, il gruppo di cooperazione e la rete CSIRT sono operativi dal 9 febbraio 2017.

L'architettura NIS europea è riassunta nell'infografica che segue.



Va notato subito il ruolo fondamentale del gruppo di cooperazione che avrebbe dovuto/dovrebbe assistere gli stati membri per l'identificazione degli operatori dei servizi essenziali e gli effetti negativi in un periodo di tempo appena scaduto ovvero dal 9 febbraio 2017 al 9 novembre 2018; va, ancora, ricordato il supporto tecnico di Enisa tanto per la Commissione quanto per gli organismi di coordinamento ovvero il gruppo di cooperazione e la rete dei CSIRT. Vanno comunque designati la/le Autorità nazionale/i di riferimento, il/i CSIRT nazionale/i e il punto unico di contatto nazionale.

Mentre ci giunge notizia che alcuni stati membri avrebbero già concluso l'*iter* formale di recepimento della NIS, registriamo un ritardo nazionale evidente nella recente Delega al Governo per il recepimento delle direttive europee entrata in vigore il 21 novembre scorso. La situazione nazionale dispone sì di un aggiornamento del Quadro strategico nazionale a febbraio 2017 e del Piano operativo che, tuttavia, mancano dell'implementazione prevista dai due dispositivi normativi citati.

Su dubbi della Commissione in merito all'applicazione della NIS vanno segnalate, a mio avviso, le varie previsioni di riesame della direttiva.

L’art. 23 prevede che entro il 9 maggio 2018 la Commissione presenti al Parlamento europeo e al Consiglio una relazione sulla coerenza nell’identificazione degli operatori dei servizi essenziali. Due anni dopo l’entrata in vigore della direttiva NIS e ogni 18 mesi successivi, la Rete CSIRTs produrrà una relazione per valutare l’esperienza acquisita con la cooperazione operativa, ivi comprese le conclusioni e le raccomandazioni emerse. La relazione sarà inviata alla Commissione ed è previsto il riesame periodico della direttiva stessa.

La prima osservazione di sistema inerisce il rapporto tra la Direttiva NIS e le norme di contesto connesse ovvero il GDPR e la protezione dei dati in genere, le norme settoriali della UE, ad esempio nei trasporti marittimi e nel bancario finanziario, le norme nazionali e le norme e accordi internazionali, tra i quali il *Privacy shield*. Non è chiaro, ad esempio, come si risolverà il tema delle *compliance* NIS e GDPR e delle sanzioni previste in relazione al *Privacy shield* che dovrebbe sottostare alle norme europee.

Vediamo, intanto, obblighi e sanzioni previsti per gli operatori di servizi essenziali.

“Gli operatori di servizi essenziali sono aziende private o enti pubblici con un ruolo importante per la società e l’economia nei seguenti settori:

Energia: elettricità, petrolio e gas.

Trasporto: aereo, ferroviario, marittimo e stradale.

Bancario: gli istituti di credito.

Infrastrutture dei mercati finanziari: le sedi di negoziazione e le controparti centrali.

Salute: ambienti sanitari.

Acqua: fornitura di acqua potabile e distribuzione.

Infrastruttura digitale: specificamente gli Internet Exchange point, i fornitori di servizi DNS (Domain Name System) e i registri TLD (Top Level Domain).”

Ma i ‘considerando’ della Direttiva ci informano che settori quali il bancario finanziario e il trasporto marittimo dispongono di norme di settore che andranno valutate e integrate eventualmente ai fini dell’applicazione della nuova norma.

Partendo dal presupposto che alle scadenze si tenga fede, gli stati membri dovrebbero avere già redatto le liste degli operatori di servizi essenziali previste per il 9 novembre scorso (art. 23).

A tale fine la norma recita:

“1. Entro il 9 novembre 2018, gli Stati membri identificano, per ciascun settore e sottosettore, gli operatori di servizi essenziali con una sede nel loro territorio.

2. I criteri per l’identificazione degli operatori di servizi essenziali sono i seguenti:

   - un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
   - la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
   - un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Ciascuno Stato membro istituisce un elenco dei servizi.”

Così formulato il testo lascerebbe intendere che gli operatori di servizi essenziali vanno identificati con un ‘nome e cognome’ specifico.

Tralasciando la tautologia dell’ ‘essenziale’, si intende immediatamente la delicatezza del tema, il primo *bug/vulnus*

potenziale per il quale l'identificazione eventualmente selettiva degli operatori di servizi essenziali, inclusi le multinazionali europee e internazionali, potrebbe dar luogo a trattamenti esoneranti a seconda delle liste dei diversi stati membri, della stabile organizzazione e/o della localizzazione territoriale del 'rappresentante' delle medesime, come previsto dalla NIS.

Un quesito per tutti poi. Poiché le grandi aziende di servizi si avvalgono di reti di aziende di intermediazione dei servizi stessi, a cascata, ad esempio nell'energia, nell'acqua, nelle telecomunicazioni, ecc. come si comporteranno in materia le Autorità nel caso di incidenti a questi soggetti e non alle case madri? E come dovrà intendersi l'obbligo di *compliance* a standard di sicurezza? E, ancora, fino a che livello dovranno attuarsi analisi per il *risk assessment* e la *risk evaluation*?

La vaghezza quantitativa e qualitativa degli effetti negativi rilevanti rende, poi, assai precaria, in partenza, la definizione della soglia di impatto.

La norma così prevede:

tra i fattori intersettoriali per la definizione degli "effetti negativi rilevanti:

- il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;
- la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;
- l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
- la quota di mercato di detto soggetto;
- la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
- l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della

disponibilità di strumenti alternativi per la fornitura di tale servizio.”

Nonché “fattori settoriali: ove opportuno”.

C’è da chiedersi chi, tra i primi della classe europea, abbia già provveduto a dati e stime econometriche e sociali di questa portata relative al proprio territorio e/o a stabilimenti localizzati altrove o i cui rappresentanti nel caso di multinazionali eroghino servizi sul territorio nazionale, ma siano localizzati altrove. A meno che non si pensi di agire, caso per caso nel caso di incidenti, ma, in questo caso, mancherebbero i presupposti chiari per le notifiche degli incidenti stessi. E qui si apre il grande tema *bug* della giurisdizione e territorialità e delle connesse sanzioni in caso di incidenti, tema che toccheremo tra poco.

Veniamo ora alle *compliance* che si possono riassumere nel modo seguente.

Obblighi di *risk assessment* e *risk evaluation* devono correlarsi alla *compliance* a norme UE e internazionali: per intenderci linee guida e standard quali il framework NIST, COBIT, ISO, ISA, ecc. Ma a quali delle decine di standard sarà data la preferenza nei singoli stati membri? E qui si apre il terzo *bug* applicativo per il quale si potrebbe scatenare una ‘guerra’ degli standard per i *vendor* di prodotti e servizi digitali essendo le norme europee e statunitensi diverse e di diverso impatto nei prodotti e servizi stessi. E’ ovviamente immaginabile la pressione lobbistica delle aziende che erogano servizi digitali nei singoli stati membri.

Obbligatorie le notifiche cui gli stati membri dovranno far corrispondere le sanzioni, se e del caso. Il tutto dovrà corrispondere a criteri oggettivabili di impatto, ovvero a criteri condivisi di valutazione del rischio e a verifiche di giurisdizione e territorialità. Insomma un bel vespaio giuridico e pragmatico ovvero un quarto *bug* applicativo.

Per intendere meglio il tema, occorre rivolgersi ora alla seconda categoria di aziende alle quali si riferisce la norma ovvero i fornitori di servizi digitali.

I fornitori sono identificati dalla norma in relazione alla tipologia di servizi digitali erogati ovvero del:

2. Mercato online
3. Motore di ricerca online
4. Servizi nella nuvola (cloud computing).

In questo caso, gli obblighi sono così rappresentati:

“ *I fornitori di servizi digitali devono* ***identificare e adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi*** *posti alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell’offerta di servizi…*”

Elementi da considerare:

1. La sicurezza dei sistemi e degli impianti;
2. Trattamento degli incidenti;
3. Gestione della continuità operativa;
4. Monitoraggio, audit e test;
5. Conformità con le norme internazionali.

Anche in questo caso, l’impatto da valutare deve tener conto di:

1. a) Il **numero di utenti** interessati dall’incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;
2. b) La **durata** dell’incidente;
3. c) La **diffusione geografica** relativamente all’area interessata dall’incidente;
4. d) La **portata della perturbazione del funzionamento del servizio**;
5. e) La **portata dell’impatto sulle attività economiche e**

sociali.

Si noti che l' "obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente nei confronti dei parametri di cui al primo comma."

Oltre ai riferimenti di impatto analoghi a quelli individuati per i fornitori di servizi essenziali, resta vago il concetto di 'portata' che presumiamo darà disambiguato dal gruppo di cooperazione.

Piccolo *bug/vulnus* potenziale, per quanto esposto sopra in relazione alle aziende che intermediano i servizi con attività di fornitura e consulenza, poi, troviamo nell'articolato al comma 11 del Capo V che esclude l'applicazione del Capo v medesimo inerente gli obblighi in materia di sicurezza alle microimprese e alle piccole imprese.

Veniamo, ora, al tema della giurisdizione e territorialità previsto nell'art. 18. Il fornitore che non è stabilito nell'Unione deve designare un 'rappresentante' in uno degli stati in cui il fornitore eroga servizi. E' l'annosa questione posta, ad esempio, anche ai fini contrattuali, per la localizzazione dei dati *cloud* su server localizzati o meno in Europa, 'risolta' temporaneamente con l'accordo *Privacy shield* che, tuttavia, dovrebbe sottostare al nuovo GDPR.

Ma il *bug/ vulnus* più specioso è altro.

Infatti, dovendo una multinazionale designare un 'rappresentante' senzalocalizzazione europea sul territorio di uno degli stati membri della UE dove eroga servizi, essa sceglierà lo stato che irroghi sanzioni meno onerose nel caso di violazioni della norma e di incidenti. Sarà pertanto vitale una reale armonizzazione che eviti fughe delle mltinazionali sui territori alla ricerca delle soluzioni più vantaggiose.

In conclusione e riassumendo, vanno sciolti per tempo potenziali *bug* applicativi quali:

- la disomogeneità possibile nell'identificazione da parte degli stati membri degli operatori di servizi essenziali e degli operatori di servizi digitali (liste di servizi e di operatori)
- le sanzioni: potenzialmente diverse per stato membro e da armonizzare
- le notifiche con la definizione chiara dei parametri di effetti negativi e referenti (punti di contatto, Autorità e/o CSIRT)
- il riferimento a standard internazionali (europei e non) con la potenziale concorrenza tra i *vendor*
- la *compliance* vs la sicurezza ovvero il riferimento a requisiti minimi non verificabili

La giurisdizione ovvero la localizzazione della sede e/o del rappresentante delle aziende multinazionali prive di stabile organizzazione in Europa

- e, infine, l'ottimizzazione dell'Interazione tra Commissione, gruppo di cooperazione, Autorità, rete dei CSIRT, Enisa, punti unici di contatto.

Restiamo in attesa di eventi e di risposte nazionali ed europee.

Direttiva europea NIS e GDPR, attuazione e bug applicativi nel mercato digitale

Criptovalute, la frode del software di mining sui nostri pc

Durante quest'anno i *miner* di criptovaluta si sono affermati come una delle principali tendenze nel panorama economico finanziario internazionale. Un dato che va letto non solo in termini di valute virtuali e possibili bolle, ma anche di sicurezza e di cyber crimine.

Sono sempre dipiù i criminali informatici che prendono come obiettivo questo settore, mercato in costante crescita, trainato dal successo di criptovalute come il bitcoin, ormai sulla soglia dei 20 mila dollari di valore.

La scorsa estate un'indagine Chainalysis rivelò che **i danni da phishing per gli investitori in criptovalute ammontavano a 225 milioni di dollari**. Più di 30 mila sono state le vittime, perdendo a testa più di 7.500 dollari.

Si trattava di siti web o social account del tutto simili alle piattaforme di offerta di moneta iniziale (ICO), mezzo molto utilizzato per raccogliere fondi per nuove criptovalute. In tal modo si sollecitava gli investitori ad inviare denaro, che poi veniva illecitamente sottratto.

Una delle tecniche di frode utilizzate ultimamente consiste invece nel creare siti web che offrono agli utenti la possibilità di fare il **download gratuito di versioni pirata di software per pc e applicazioni**. Per risultare più credibili, si legge in un recente *Report* di Kaspersky Lab, "*i criminali hanno utilizzato nomi per i domini simili a quelli reali. Dopo aver scaricato il software, l'utente riceve un archivio che contiene anche un programma di mining. Questo programma viene quindi installato automaticamente insieme al software desiderato*".

Il funzionamento è così descritto dai ricercatori di *cybersecurity*: "***dopo essere stati installati, i miner iniziano a operare silenziosamente sul PC della vittima, generando cripto monete per i criminali****. In tutti i casi rilevati, è stato utilizzato il software del progetto NiceHash, che ha recentemente subito una grave violazione della sicurezza informatica con conseguente furto di cripto valuta per milioni di dollari. Alcune delle vittime erano collegate a un pool di mining con lo stesso nome*".

In termini di danni reali non sembra che questi software pirata siano particolarmente virulenti: "*anche se ad alcune persone potrebbe andar bene che uno sconosciuto diventi più ricco a spese proprie, noi consigliamo agli utenti di opporsi a questi tentativi perché anche se non vengono condotti con software nocivi standard rappresentano comunque un'attività fraudolenta*", ha affermato **Morten Lehn**, General Manager Italy di Kaspersky Lab.

Sostanzialmente, tali software di *mining* riducono le performance di sistema del dispositivo, in alcuni casi lo rendono anche più vulnerabile ad altri malware e aumentano il consumo di energia elettrica, influendo inevitabilmente sull'esperienza utente nel suo complesso.

https://www.key4biz.it/criptovalute-la-frode-del-software-mining-sui-nostri-pc/208698/

Protect Your Business! The 7 Cybersecurity Tools You Need

as an Entrepreneur.

If you aren't taking active steps to secure your business's digital assets, pure and simple, *you're putting yourself at risk.* Approximately 43 percent of all cyberattacks, according to Symantec, focus on small businesses – in part because they're a big enough target to be valuable, but also small enough to be vulnerable.

Related: Cybercriminals Are Targeting Small Businesses That Don't Take Cybersecurity Seriously

As if that weren't enough, according to the National Cyber Security Alliance, as many as 60 percent of small- to medium-sized businesses that have been hacked go out of business within six months of the attack.

Now, you could describe an intuitive correlation here: Businesses that don't invest enough in their cybersecurity probably aren't investing enough in other areas of their business.

But the statistic is still worrying, so if you want to protect your business, you need to make the investments and upgrades necessary to keep it secure.

The problem is that, to an inexperienced entrepreneur, or a business without a formal IT department, the cybersecurity world is confusing and intimidating. Fortunately, you don't need to be a tech expert to make wise investment and protection decisions. In fact, there are a handful of tools that can keep you safe from the vast majority of potential attacks.

The most important security tools

These are some of the most important security tools you'll need for your business:

Password tools. Your passwords are one of the biggest points of vulnerability in your business, with 90 percent of passwords, according to Deloitte, weak enough to be vulnerable to hacking. Choosing strong passwords, managing them effectively and changing them often are some of the best ways to prevent any cybercrime. The problem is that it’s tough to keep everything organized in a business. That’s why a security tool like 1Password can help ; it gives you a centralized, secure location to manage all your passwords, and update them to keep them safe.

Related: Here’s How Taking Cybersecurity Very Seriously Enhances Your Brand

A VPN. You should also employ a virtual private network (VPN), which can encrypt all your network traffic so you don’t have to worry about outside forces spying on your work. A single network vulnerability is all it takes for a cybercriminal to gain access to all your data, so invest in a tool like SaferVPN, which is ideal if you have multiple users on multiple devices.

Antivirus software. You should also invest in some antivirus software for your devices. Antivirus software isn’t a surefire bet to protect you from hackers, but it will keep you alert if your computer is infected with malware and will scan email attachments to ensure they aren’t scams. AVG Technologies offers free antivirus software for individual users and special packages for businesses. There are also McAfee and tother options on the market.

A firewall. Next, you’ll want to invest in a firewall, which will monitor incoming and outgoing traffic, filter out certain threats and even block some sites altogether. A strong firewall alone won’t protect you from all the threats on the internet, but it’s an added layer of insurance you shouldn’t be without.

Better hardware. Older computers, servers and other pieces of hardware may be less expensive, but they pose much bigger security risks. They tend to run older software and have security holes that have been known and exploited for years. Make sure you upgrade your hardware routinely, every few years.

Better software (for everything). You'll also need to pay careful attention to what type of software and applications you use for tasks like data storage, communication and project management. Each individual platform has its own strengths and weaknesses, so choose vendors you trust, with a long history of protecting customers' data.

Education. Finally, invest in educational tools you can use to train and update your employees. Most hacks are attributable to human error, so the more educated your employees are on the best practices for cybersecurity, the less vulnerable you're going to be. Set aside time every month to go over new updates, and remind your employees about the importance of habits like regularly changing passwords and avoiding suspicious links.

Related: 4 Vital Cyber Security Measures Every Safety-Conscious Entrepreneur Needs to Take

Staying vigilant

Over 14 million businesses were "hacked" in 2016, but your business doesn't have to be next in line. As long as you make wise investments, routinely monitor and improve the habits of your employees and commit to staying abreast of the latest digital threats, you'll minimize your vulnerabilities significantly. Even non-techies have the power to protect their businesses from cyber threats.https://www.entrepreneur.com/article/306294

WannaCry, gli Stati Uniti lanciano l’accusa ‘Dietro i cyber attacchi c’è la Corea del Nord’

A maggio di quest’anno un’ondata di attacchi informatici di tipo ransomware ha preso di mira i pc e i dispositivi elettronici di mezzo mondo. Un attacco su vasta scala, denominato ***WannaCry***, mirato a sequestrare letteralmente i computer, con l’obiettivo di chiedere un riscatto, molto spesso inutilmente pagato dalle vittime.

Secondo dati Europol di metà maggio, più di 200 mila pc di 150 Paesi sono stati attaccati dai cyber criminali, subendo danni di varia gravità, più altre 1,3 milioni di macchine che in quei giorni erano ancora considerate sotto attacco e da monitorare.

Insomma, un’operazione di cyber criminalità davvero ingente, ampia, pericolosa e ben congegnata, che contò vittime eccellenti, tra cui aziende (in Francia è stata colpita la Renault, in Spagna la compagnia telefonica Telefónica), ospedali (come il sistema sanitario nazionale britannico, quindi mettendo a rischio potenzialmente vite umane), scuole e sistemi di trasporto.

Ora la Casa Bianca torna sulla faccenda e lo fa con un articolo sul *Wall Street Journal* a firma di **Thomas Bossert**, consigliere di **Donald Trump** per la sicurezza interna e l’antiterrorismo, secondo il quale “*Dietro il cyberattacco ‘Wannacry’, che ha paralizzato tutto il mondo lo scorso maggio, c’è la Corea del Nord*”.

“*Non siamo gli unici a sostenere” la responsabilità di Pyongyang, altri governi e società private sono d’accordo con noi*“, ha sentenziato Bossert.

“*Le nostre accuse non sono fatte a cuor leggero, abbiamo delle prove schiaccianti. Assieme a noi c’è la Gran Bretagna e Microsoft ha tracciato gli attacchi, che portano inevitabilmente alla Corea del Nord e al suo Governo*”, ha spiegato l’autore dell’editoriale, che ha poi aggiunto un appello mondiale: “*Unitevi a noi nel combattere i cattivi del web*”, identificando in questi cattivi, oltre la Corea del Nord, anche con la Russia e l’Iran.

La Corea del Nord, precisa il consigliere di Trump, “*continua a minacciare l’America, l’Europa e il resto del mondo non solo con le sue aspirazioni nucleari. Sta usando sempre più i cyberattacchi per alimentare il suo comportamento e causare distruzioni*“.

Che poi conclude ammonendo tutti: “*Gli hacker maligni appartengono al carcere, e i governi totali devono pagare un prezzo per le loro azioni*“.

https://www.key4biz.it/wannacry-gli-stati-uniti-lanciano-laccusa-dietro-cyber-attacchi-ce-la-corea-del-nord/208308/

Cloud, il 70% delle imprese nel mondo non ha una strategia di cybersecurity

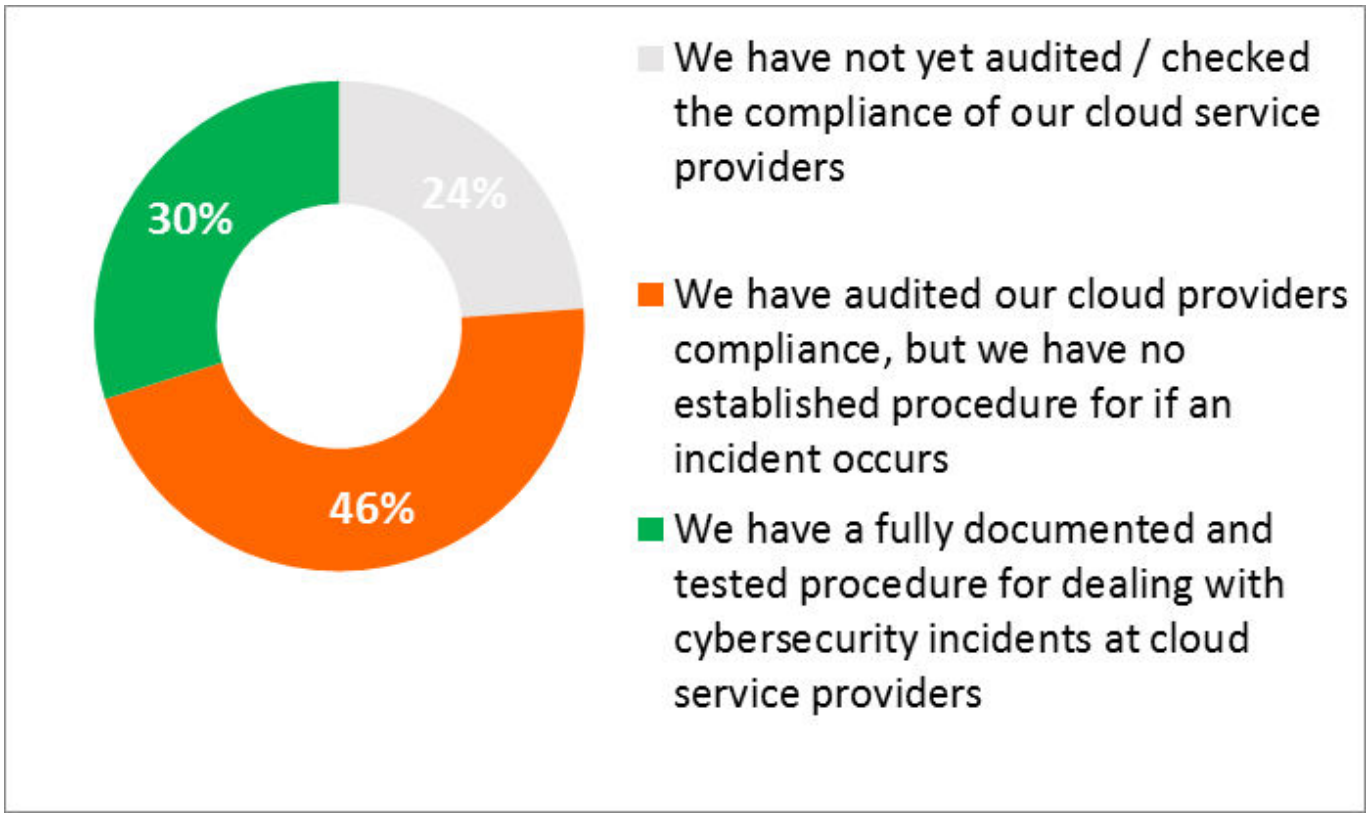
A livello globale, quasi otto aziende su dieci stanno già utilizzando almeno una piattaforma basata su un modello

Software-as-a-Service (SaaS). Lo stesso numero di aziende (75%) prevede in futuro di spostare più applicazioni nel ***cloud***.

D'altronde, i servizi della nuvola consentono alle aziende di sfruttare le principali tecnologie a supporto delle operazioni quotidiane e i piani di crescita, senza preoccuparsi della manutenzione o dei costi elevati. Ma non solo SaaS, per quanto riguarda l'***Infrastructure-as-a-Service*** (IaaS), quasi la metà delle grandi aziende (49%) e delle PMI (45%) intende delegare la gestione dell'infrastruttura e dei processi IT a terze parti.

Il problema è nella sicurezza, sia delle infrastrutture, sia dei servizi e quindi dei dati. Stando a una recente ricerca di Kaspersky Lab, **sette aziende su dieci (70%) che si affidano a provider SaaS e di servizi cloud non hanno un piano per gestire gli incidenti di sicurezza** che potrebbero interessare i propri partner.

Un'azienda su quattro ammette di non aver nemmeno controllato le credenziali di conformità del proprio service provider, dando per scontato che le conseguenze di eventuali incidenti siano a carico del provider stesso.



Questo perché la velocità di adozione e la riduzione dei costi operativi hanno portato molte organizzazioni a tralasciare gli aspetti della sicurezza: "L'*andamento rapido con cui viaggia la trasformazione digitale sta portando maggiore efficienza e flessibilità alle operazioni aziendali ma presenta anche nuove sfide alla sicurezza che mettono in pericolo le aziende*", ha dichiarato **Morten Lehn**, General Manager Italy di Kaspersky Lab.

Affidarsi ai server provider per una protezione completa è evidentemente un rischio, non certo una soluzione.

Ecco perché è fondamentale trovare un modo per tenere sotto controllo i servizi cloud.

"*Ogni dato deve essere protetto ovunque si trovi e in qualsiasi momento* – si legge nel commento all'indagine – *per fare ciò, le aziende devono individuare le anomalie all'interno delle proprie infrastrutture cloud e questo si può ottenere solo attraverso una combinazione di tecniche come il machine learning e l'analisi comportamentale*".

Ricordiamo che a livello mondiale **le grandi imprese subiscono in media un danno finanziario di 1,2 milioni di dollar**i, in seguito a un incidente di sicurezza legato al cloud, rispetto ai 100.000 dollari per le PMI.

Ancora, **il 42% delle aziende non si sente adeguatamente protetta dagli incidenti che potrebbero interessare il proprio fornitore di servizi cloud** e il 24% ha subito, negli ultimi 12 mesi, un incidente di sicurezza che ha colpito l'infrastruttura IT di terze parti.

Le tre tipologie di dati maggiormente colpite riguardano: informazioni sui clienti altamente sensibili (rilevate dal 49% delle PMI e dal 40% delle grandi aziende); informazioni di base sui dipendenti (25% per le PMI, 36% per le grandi imprese), e-mail e comunicazioni interne (31% per le PMI, 35% per le grandi imprese).

https://www.key4biz.it/cloud-70-delle-imprese-nel-mondo-non-strategia-cybersecurity/208231/