



Il tuo browser (Apple Safari 4) non è aggiornato e potrebbe non visualizzare correttamente le pagine di questo e altri siti. [Aggiorna il tuo browser!](#) Ti consigliamo di scaricare [Google Chrome](#) o [Mozilla Firefox](#) X



[abbonati](#) | [Accedi](#) | [Paywall](#) | [conosci i foglianti](#) | [Newsletter](#) | [FAQ](#) | [🔍](#)



LEGGI EDIZIONE



FOGLIO SPORTIVO



FOGLIO WEEKEND

IL FOGLIO

SALVINI | BANKITALIA | AIRBUS | VENEZUELA

[home](#) [elefantino](#) [politica](#) [economia](#) [chiesa](#) [esteri](#) [editoriali](#) [cultura](#) [sport](#) [lettere](#) [meteo](#) [blog](#) [lo sfoglio](#) [sezioni](#) v

tecnologia

NUOVA JEEP RENEGADE

ANTICIPO ZERO

VALORE FUTURO GARANTITO

FINO A 6.000€ DI ECOBONUS GARANTITO

RICHIEDI PREVENTIVO ▶

FCA BANK

Jeep



Tofalo spiega perché all'Italia serve una vera Cyber Strategy

Il sottosegretario alla Difesa intervistato da Breakingtech.it: "È imperativo restare al passo con i tempi e investire nella sicurezza informatica"

18 Febbraio 2019 alle 17:36



Foto di Blogtrepreneur via Flickr

NUOVA JEEP RENEGADE

Pubblichiamo



Servizi di Media Monitoring

[LINK ALL'ARTICOLO](#)



**ANTICIPO ZERO
VALORE FUTURO**

GARANTITO

**FINO A 6.000€
DI ECOBONUS**

GARANTITO

FCA BANK Jeep

RICHIEDI PREVENTIVO ►

*l'intervista al
sottosegretario alla
Difesa con delega alla
cybersecurity, Angelo
Tofalo, di Federico
Lobuono, direttore di
[Breakingtech.it](#)*

Secondo gli ultimi dati, odiernamente le aziende lamentano il fenomeno degli attacchi informatici. In uno scenario come quello odierno, dove i dati sono fondamentali per il mercato, secondo lei questi player finanziari investono abbastanza risorse nel settore della cyber-sicurezza? Girano molti dati in rete che il mercato della cyber-security sia ancora poco sviluppato. Secondo lei quale sarebbe l'aspetto più importante su cui un'azienda dovrebbe puntare per poter ritenersi al sicuro? Quale potrebbe essere la soluzione per poter espandere il mercato italiano per quanto concerne la sicurezza informatica?

Prima di iniziare la mia esperienza politica ho lavorato per circa cinque anni come ingegnere progettista di Opere Strategiche, Telecomunicazioni, Sicurezza e progettualità richiedenti un livello elevato di Nulla Osta di Sicurezza. Oggi, da Sottosegretario di Stato alla Difesa pro tempore, ho una specifica delega per la trattazione di problematiche relative alla sicurezza cibernetica. Nel settore pubblico e in quello privato, la difesa cibernetica è un tema di grande importanza e attualità. È più costoso difendersi da un attacco cyber che attaccare. Purtroppo le aziende, soprattutto quelle più piccole che non dispongono di grandi capitali, considerano il costo della sicurezza cibernetica una spesa piuttosto che un investimento. In tanti casi invece una scarsa prevenzione e una debole capacità di difesa sono la causa del declino di un'azienda che, senza nemmeno

PIÙ VISTI

E' finita l'età dello sharing, adesso il digitale arriva alle industrie serie >

Intelligenza artificiale, il meglio deve ancora venire >

Balene volanti: decolla il primo Airbus Beluga XL >

Perché il gran debutto di Apple sui servizi (lo streaming!) è pieno di problemi >

POTREBBE INTERESSARTI

Morte agli F-35, viva gli F-35 >

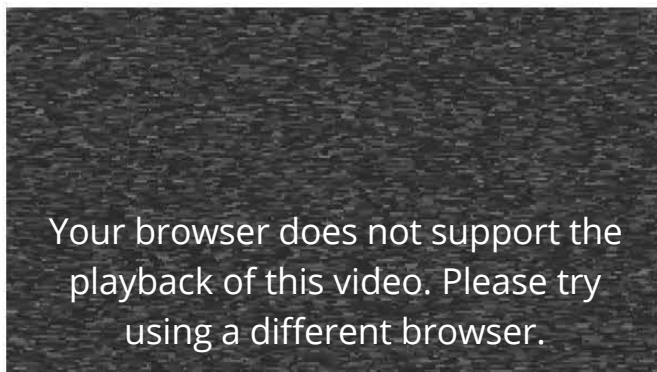
Le mani dei Cinque stelle sui servizi. Ma la Lega non ci sta >

Così la regola dei due mandati assilla il M5s >

L'inadeguatezza del grillino Tofalo al Copasir >



rendersene conto, subisce esfiltrazioni di dati sensibili. È pur vero che le Aziende, nei casi in cui si accorgano di aver subito un attacco informatico (quale ad esempio un data breach), talvolta tendono a nascondere gli incidenti occorsi, per i motivi più disparati, per il timore di veder rovinata la propria reputazione (con conseguenti impatti anche economici): occorre quindi ragionare per costruire un modello virtuoso che possa rafforzare la condivisione delle informazioni, che siano attacchi informatici subiti o contromisure attuate con successo. Gli aspetti più importanti su cui puntare sono quello tecnologico e il fattore umano. Non dobbiamo mai dimenticare che l'elemento più debole del sistema è quello seduto tra la sedia e il computer: la persona. Pertanto è molto importante investire nella diffusione della cultura della sicurezza. Nel corso della mia esperienza ho notato, purtroppo, che in tante occasioni si presta più attenzione a proteggere la mail privata rispetto quella istituzionale. Ciò rappresenta una "falla" del sistema di un'azienda, di una Pubblica Amministrazione. Bisogna pertanto coltivare il concetto che cittadino, azienda (pubblica o privata), istituzioni (Stato) sono tutti nodi fondamentali del Sistema Paese. Per quanto concerne la sicurezza informatica, il mercato italiano è presente ma ha ancora notevoli difficoltà a confrontarsi con i principali attori che oggi sono Stati Uniti, Cina. È imperativo restare al passo con i tempi e investire nella sicurezza informatica e nelle nostre realtà aziendali specializzate nel settore.



Penso che sia adeguatamente informato riguardo



l'hacker, di soli 20 anni, che è riuscito a risalire ai dati di migliaia politici in Germania e rilasciarli all'opinione pubblica. A quanto pare l'attività di "spionaggio" e divulgazione va avanti da circa 2 anni. Ma non è tutto qui, già dal 2015 la stessa Germania aveva segnalato delle grosse problematiche di sicurezza digitale per quanto concerne vari attacchi informatici che sarebbero provenienti dal territorio Russo. Analizzando queste dinamiche appare quindi spontaneo pensare che la tematica della cybersicurezza non venga presa abbastanza in considerazione, oppure che non sia ancora ben delineata la strada da intraprendere per poter contrastare efficacemente queste minacce. Lei cosa ne pensa in merito? Secondo lei che attitudine dovrebbe seguire una nazione per poter tenere al sicuro i dati dei suoi cittadini da attacchi esterni? Quali sono le difese che l'Italia ha in questo settore?

Il vero potere del nuovo millennio sono i dati da immagazzinare, analizzare, e utilizzare per diversi scopi. Per questo, oggi, la protezione dei dati è un tema molto sensibile, strategico direi. Gli attacchi si fanno sempre più numerosi e sofisticati, grazie allo sfruttamento di nuove risorse o di strategie già note. Un attacco può arrivare da ogni dove e nella maggior parte dei casi è molto complicato risalire all'esecutore materiale. Il problema dell'attribution è quindi uno dei principali aspetti che vanno studiati e approfonditi. Per adesso è un problema non del tutto risolto. Per quanto riguarda i mandanti, sono mossi da motivi sociali, economici, politici, militari e industriali. Ciò che oggi serve al Paese è una strategia cibernetica comune. È necessario individuare protocolli di cooperazione tra gli enti che fanno parte dell'architettura nazionale di cyber security e gli operatori privati ai quali è affidata la gestione delle infrastrutture di rete maggiormente critiche e strategiche. Una delle strade percorribili è un maggior dialogo e cooperazione tra Pubblico, Privato e Università. Personalmente, nell'ambito



della mia delega alla sicurezza cibernetica nel Dicastero della Difesa, sto analizzando l'organizzazione attuale al fine di proporre e individuare dei cambiamenti che permettano di essere più efficaci ed efficienti nel settore cyber, in ogni sua declinazione (formazione, protezione, analisi delle minacce, difesa).



Come sa, la nostra testata è gestita da millenials e in quanto tali ci piacerebbe essere coinvolti il più possibile all'interno della tematica della

sicurezza dei dati e di quella informatica. Secondo lei, non sarebbe meglio coinvolgere anche soggetti "millenials" per poter comprendere meglio le dinamiche della rete?

È molto importante coinvolgere le nuove generazioni, i cosiddetti nativi digitali. Voi, di certo, capite meglio di altri le dinamiche della rete. Inoltre, l'alfabetizzazione digitale deve diventare una priorità. È necessario insegnare materie digitali e far conoscere fin dalla scuola materna come ci si muove nello spazio cibernetico, individuando esperti da impiegare nel settore della sicurezza, risorse su cui investire a partire dalla tenera età.

Molti soggetti in Italia sono ignari dei rischi della rete o viceversa, demonizzano ogni esponente aziendale online poiché spaventati dalla questione privacy. Questo è sintomo di un'istruzione inadeguata sul tema della rete e soprattutto della sicurezza online. Secondo lei, da questo punto di vista, è necessario introdurre dei corsi formazione e campagne destinate ad ogni fascia di età? In questo modo si potrebbero evitare casi di disinformazione in merito e magari equilibrare



L'opinione pubblica in merito?

La minaccia cibernetica non nasce oggi ma con la nascita di intranet, la prima rete realizzata diversi decenni fa. Oggi iniziamo a percepirla più forte, pervasiva e sofisticata a causa di sempre più utenti che usufruiscono del dominio cibernetico ma è ancora poco quello che si fa per contrastarla. Se vogliamo creare il Sistema Paese dobbiamo puntare sulla formazione, ristrutturando il sistema scolastico, e investire nella diffusione della cultura della difesa e della sicurezza. Da rappresentate delle Istituzioni sento molto forte questa necessità.

Per concludere vorrei chiederle quali sono i suoi consigli per i giovani che fanno parte di questo Paese. Come possiamo essere in grado di proteggerci autonomamente? E soprattutto, qual è il suggerimento che darebbe alle altre istituzioni per far sentire i propri cittadini più al sicuro in questo campo?

Le scuola, a partire dai primissimi anni, dovrebbe essere in grado di fornire tutti gli strumenti per crescere e coltivare la cultura della sicurezza nell'era digitale. Il mio consiglio è di non sottovalutare la minaccia cibernetica sempre più difficile da prevedere e in continua evoluzione. La vostra generazione è e sarà la generazione protagonista di questo cambiamento epocale. Correte ragazzi e portateci nel futuro. L'Italia deve esserci grazie alla spinta di chi, come voi, segue attentamente que

TAG: angelo tofalo

Pubblicità

× CONTENUTI SPONSORIZZATI

Ad



Ad



Ad



Ad

