Cybersecurity, a Roma il 7 marzo convegno su sicurezza, regolamento UE e imprese

Mercoledì 7 marzo 2018 dalle ore 15:00 alle 18:00, presso il **Palazzo Origo** di Via di Torre Argentina, 21 a **Roma**, si terrà l'evento promosso da **BLB Studio Legale** '***Cyber Security e Regolamento UE 2016/679: Cosa cambia per le Imprese?'.*** Al convegno parteciperanno rappresentanti delle istituzioni, mondo accademico ed esperti in materia.

Il Convegno vuole costituire un'occasione di riflessione offrendo la parola a tutti i protagonisti: istituzioni, università, giuristi e associazioni riguardo i profili tecnico-giuridici della cybersecurity, le principali novità e l'impatto del regolamento UE 2016/679 e della Direttiva 1016/1148 sulle imprese.

Tra i vari ospiti saranno presenti **Raffaele Barberio**, Presidente dell'Associazione Privacy Italia, **Luigi Montuori**, Dirigente del Servizio Relazioni Comunitarie e Internazionali, Garante per la protezione dei dati personali, **Corrado Giustozzi**, Esperto Cyber Security, AgID (Agenzia per l'Italia Digitale) e **Paolo Galdieri**, Avvocato – BLB Studio Legale, Docente di Informatica Giuridica – Università LUISS Guido Carli.

L'evento è accreditato presso il Consiglio dell'Ordine degli Avvocati di Roma e da 3 crediti formativi ordinari.

Per iscriversi all'evento: info@key4biz.it

Cybersecurity, a Roma il 7 marzo convegno su sicurezza, regolamento UE e imprese

---

Hot web e ‘malattie informatiche trasmissibili’, 50% italiani contrae malware su siti a luci rosse

Nell’ecosistema digitale esistono “*malattie informatiche trasmissibili*”, tramite virus e malware. Basta entrare in un sito web per adulti e guardarsi un contenuto pornografico per mettere a repentaglio il proprio pc, laptop, tablet e smartphone.

Un adulto italiano su due circa, il 49%, è vittima di un virus informatico dopo aver visualizzato contenuti per adulti online. In media, i nostri connazionali guardano contenuti per adulti cinque volte alla settimana e **uno su cinque (21%) usa il proprio dispositivo di lavoro per accedere ai contenuti pornografici**.

Sono i dati contenuti in una recente indagine condotta da Kaspersky Lab, che ha coinvolto 1.000 adulti, secondo cui **quattro italiani su dieci (39%) credono di rimanere al sicuro dai virus semplicemente usando la modalità di navigazione in incognito** per guardare contenuti per adulti.

Molti inoltre si vergognano e **tre utenti su dieci (28%) tendono a incolpare parenti o amici dell'infezione contratta dopo aver visitato siti per adulti**.

Il problema vero è che **l'8% degli intervistati ha dichiarato di navigare in modo non sicuro**, non avendo installato alcuna soluzione di sicurezza internet sui propri dispositivi. **La stessa percentuale crede erroneamente di essere al sicuro navigando su siti per adulti via tablet o smartphone**, pensando che questi device non possano essere infettati.

Motivo per cui, come per le malattie trasmissibili per via sessuale nel mondo fisico, anche in quello digitale il meccanismo è lo stesso: se non ti proteggi da navigazione insicura in questo tipo di ambienti ad alto rischio, potresti infettare con un virus informatico il device del tuo partner e quelli dei tuoi famigliari.

"*Nel 2017 abbiamo identificato almeno 27 varianti di malware per PC specificatamente pensati per cercare le credenziali dei siti a pagamento di contenuti per adulti. Questo genere di siti è interessante per i cyber criminali perché hanno un elevato numero di utenti che possono essere presi di mira e che saranno meno disposti a riferire l'infezione per non dover spiegare come l'hanno contratta*", ha commentato **Morten Lehn**, General Manager Italy di Kaspersky Lab.

"*Con 323.000 bug malware scoperti, progettati per il furto d'identità, la corruzione dei file e il ricatto, è sempre più importante che gli utenti adottino comportamenti sicuri online e prendano le giuste precauzioni*".

Le minacce più diffuse sui siti web per contenuti pornografici sono trojan, malware diffusi tramite sistema *drive-by download*, soluzioni di *click-jacking*, bot di *Tinder*, *cat phishing*, *ransomware*, classici *worms*, *pomware*, *spyware* e i tradizionali anti virus ovviamente falsi.

Nel 2016, tanto per avere un'idea della minaccia informatica

di cui parliamo, **sono stati rubati oltre 72 milioni di set di credenziali di account privati per siti web destinati ad un pubblico adulto**. Tali blocchi di dati sono stati poi rivenduti in rete e comunque resi pubblici. Nel dettaglio, questi dati sono stati sottratti illecitamente da Cams.com (62,6 milioni di account), da Penthouse.com (7,1 milioni), da Stripshow (1,42 milioni), da xHamster (380 mila) e da Brazzers (791 mila).

Un'azione criminale di grandi proporzioni, che comunque non include quella condotta in grande stile contro AdultFriendFinder, che portò alla razzia di 400 milioni di set di credenziali relative agli account degli utenti.

Navigare da rete mobile, come erroneamente creduto da tanti utenti italiani del web, non ci mette al riparo dai cyber criminali e infatti, nel 2017, **oltre 1,2 milioni di utenti in tutto il mondo hanno contratto malware proprio guardando contenuti pornografici online via smartphone/tablet**.

I *mobile malware* sfruttano proprio tali siti a luci rosse per attrarre nuove potenziali vittime

> *Hot web e 'malattie informatiche trasmissibili', 50% italiani contrae malware su siti a luci rosse*

Digitanomalie. Apple rende accessibili i dati icloud

degli utenti cinesi al Governo di Pechino. Dov’è il problema?

Sta facendo rumore la non-notizia secondo la quale *Apple*, pur di vendere i propri prodotti in Cina, ha accettato di localizzare nel **Celeste Impero** i **data centre** che ospitano i dati degli utenti cinesi e di consegnare le chiavi per accedervi al Governo.

Le reazioni alla notizia hanno stigmatizzato la “doppia morale” dell’azienda di **Cupertino** che in Occidente si pone come “campione della privacy” e in Oriente come pragmatico operatore “business-oriented” che a **Roma** fa come i romani o, meglio, a **Pechino** fa come (il Governo dei) cinesi.

Apple non ha alcun “dovere” di proteggere la privacy – questo spetta alle istituzioni pubbliche ma prima ancora a ciascuno di noi – e se lo fa (quando è possibile) lo fa sulla base di ragionate strategie di marketing e non necessariamente in ossequio a “valori morali”

Dunque, non dovrebbe scandalizzare nessuno il fatto che in nome del “i soldi non puzzano” in Occidente e in Oriente la privacy sia un potente strumento di vendita che funziona sia in un senso (attiro gli utenti promettendo inviolabilità), sia nell’altro (tranquillizzo i governi mostrando che se spingono abbastanza, ottengono quello che vogliono).

Quindi, se proprio dobbiamo cercare un problema da risolvere in relazione a questa notizia, dovremmo orientarci verso la mistificazione del ruolo attribuito alla privacy da aziende private e istituzioni pubbliche, che la considerano

ipocritamente una reliquia – ma di plastica – da esibire e svendere a una platea ignorante per ottenere soldi e potere.

E se guardiamo a cosa sta accadendo su scala europea con la bolla del **GDPR**, la notizia dell'accordo fra Apple e il Governo cinese non fa poi così notizia…

> *Digitanomalie. Apple rende accessibili i dati icloud degli utenti cinesi al Governo di Pechino. Dov'è il problema?*

Phishing, come i cyber criminali fanno guadagni sulle nostre tasse

Via mail ormai ci arriva di tutto: documentazione da enti pubblici e privati, dal fisco, dalle amministrazioni locali, da organizzazioni di varia natura. Sono diverse le comunicazioni ufficiali che ci raggiungono grazie alla posta elettronica, soprattutto via mobile, e le frodi digitali sono all'ordine del giorno.

I cyber criminali di tutto il mondo hanno da tempo preso di mira queste "comunicazioni ufficiali", perché sanno bene che quando ci arriva una mail dall'Agenzia delle entrate e dalla banca va a finire che molti di noi la aprono, seguendo le indicazioni contenute.

Si va dalla richiesta di nuovi documenti, all'aggiornamento

dei dati personali, fino all'ingiunzione di pagamento per ritardi sulle imposte o addirittura, al contrario, all'offerta di rimborsi. Certamente nessuno rimane indifferente di fronte a messaggi del genere, provenienti da fonti di rilievo anche istituzionale, e che magari annunciano l'arrivo inaspettato di denaro (cosa che già dovrebbe far sorgere più di un sospetto).

Si tratta dell'abile lavoro di **truffatori online che sfruttano i sistemi fiscali locali col fine unico di impadronirsi di quantità enormi di informazioni personali** di utenti ignari. In un nuovo Report di Kaspersky Lab, con casi di attacco phishing rilvati in diversi Paesi, come Stati Uniti, Canada e Regno Unito, Francia, Italia, Ungheria e Russia, è emerso che questo tipo di attacchi è in forte aumento.

Nel commento all'indagine, **Nadezhda Demidova**, Lead Web Content Analyst di Kaspersky Lab, ha affermato: "*Le persone si fidano dei siti web governativi e dal momento che le questioni fiscali in genere comportano la condivisione di grandi quantità di informazioni personali, un messaggio dall'aspetto autentico, che chiede di condividere dati personali, non sempre desta sospetti*".

Nel 2016, nei mesi precedenti alla fine dell'anno fiscale, in Canada, Stati Uniti e Regno Unito sono stati rilevati **picchi notevoli di *phishing online* che aveva come focus centrale le imposte**. L'anno dopo, sono stati rilevati un numero crescente di attacchi che utilizzavano siti online di autorità fiscali falsi dall'aspetto autentico che promettevano un rimborso fiscale.

Ovviamente, ha spiegato la responsabile, "*non tutti i contribuenti possono riconoscere una truffa e persino gli utenti internet esperti possono essere ingannati dalla promessa di un rimborso fiscale*", quindi, si legge nella nota, **la raccomandazione è sempre quella di "*trattare qualsiasi offerta di denaro online con una buona dose di scetticismo* e** *di inserire nella sezione preferiti del loro browser il sito*

ufficiale del servizio fiscale del proprio paese per evitare di farsi ingannare dai phisher“.

Obiettivo dei cyber criminali, lo ricordiamo, è rubare agli utenti di rete più informazioni sensibili possibile, a partire dall’identità delle persone fino al denaro, “***attirandoli verso siti web falsi di agenzie governative ritenute affidabili***”.

Quando parliamo di **informazioni sensibili e dati privati**, ci riferiamo precisamente a carte bancarie (incluso il codice PIN), al numero di previdenza sociale, al numero di patente, all’indirizzo, al numero di telefono, alla data di nascita, al cognome da nubile della madre e al datore di lavoro.

I criminali informatici, inoltre, con l’ausilio di dispositivi malevoli recuperano anche l’indirizzo IP e le informazioni di sistema.

Tra i consigli più utili per evitare brutte sorprese, il documento suggerisce di controllare sempre l’indirizzo web quando si riceve la richiesta di inserire le proprie credenziali, di non smarrirsi di fronte a messaggi minacciosi (i phisher sfruttano prima di tutto la paura, la poca dimestichezza con l’argomento e l’ansia dell’utente), di non offrire mai spontaneamente nostre informazioni personali a nessuno, di non cliccare senza riflettere sui link all’interno di email provenienti da persone sconosciute o all’interno di messaggi inaspettati.

Phishing, come i cyber criminali fanno guadagni sulle nostre tasse

Se anche l’Https non è sinonimo di un sito sicuro

Una connessione sicura non vuol dire che anche un sito sia sicuro. Infatti il lucchetto verde indica che per il sito è stato emesso un certificato e che è stata generata una coppia di chiavi di cifratura. Questi siti cifrano le informazioni trasmesse tra l’utente e il sito. In questo caso, le URL delle pagine iniziano con **HTTPS**, dove la lettera S vuol dire “sicuro”.

Certamente cifrare la trasmissione dei dati è una buona pratica: in questo modo le informazioni scambiate tra il browser e il sito non sono accessibili a terze parti come ISP, amministratori di rete, intrusi, eccetera. Si possono digitare password o numeri di carte di credito senza preoccuparsi di occhi indiscreti.

Il problema, come segnala **Kaspersky Lab**, è che il lucchetto verde e il certificato non descrivono il tipo di sito. Una pagina di *phishing*, ad esempio, può comunque possedere un certificato e cifrare tutto il traffico in entrata e in uscita.

*(Un esempio di sito phishing Amazon considerato “sicuro” da Chrome, ma fate attenzione all’URL: è **Amzn**, non Amazon).*

In poche parole, il lucchetto verde indica che *dall'esterno* nessuno può spiare i dati che digitate, ma le password possono comunque essere rubate dalla pagina se si tratta di un sito contraffatto.

1/4 degli attacchi phishing è su siti Https

Chi si occupa del *phishing* ne fa un gran uso: secondo i dati di Phishlabs, un quarto di tutti gli attacchi di phishing al giorno d'oggi è effettuato su siti HTTPS (due anni fa si trattava di meno dell'1%). Inoltre, oltre l'80% degli utenti ritiene che la sola presenza di un lucchetto verde e la parola "Sicuro" accanto all'URL indichino un sito sicuro e non ha nessuna remora nell'inserire i propri dati.

(Fonte: Phishlabs – Dal 2015 al 2017 l'aumento dei siti di phishing con protocollo Https)

E se non c'è il lucchetto verde?

Se non c'è proprio il lucchetto, vuol dire che il sito non usa sistemi di cifratura e scambia informazioni con il browser mediante HTTP standard. **Google Chrome** ha iniziato a classificare questi siti come poco sicuri: possono anche essere immacolati, tuttavia non cifrano il traffico tra l'utente e il server. Poiché la maggior parte dei proprietari dei siti non vuole che Google etichetti i propri siti come non sicuri, sempre più pagine web stanno migrando all'HTTPS. **In ogni caso, è meglio non digitare dati sensibili in un sito HTTP, perché chiunque potrebbe provare a spiarvi.**

La seconda opzione è un lucchetto sbarrato da una croce in rosso e le lettere HTTPS sempre in rosso: questo simbolo

indica che il sito possiede un certificato ma non è verificato o non aggiornato. In sostanza, la connessione tra voi e il server è cifrata ma nessuno può garantire che il dominio appartenga realmente alla compagnia indicata sul sito. Si tratta dell'eventualità più sospetta, perché di solito si tratta di certificati di *prova*.

In alternativa, può essere che il certificato sia scaduto e che il proprietario del sito non lo abbia rinnovato. I browser classificano queste pagine come non sicure, normalmente avvisando con l'icona del lucchetto rosso. In entrambi i casi, prendete questi segnali come un avvertimento, evitate questi siti e non digitate dati personali.

Come non abboccare

Per riassumere, la presenza di un certificato e di un lucchetto verde indica solamente che i dati trasmessi tra l'utente e il sito sono cifrati e che il certificato è stato emesso da una *certification authority* affidabile. Ma non impedisce che si possa trattare di un sito dannoso, dettaglio di cui molti cybercriminali si servono per i propri siti di *phishing*.

Ecco i tre consigli di *Kaspersky Lab* per non abboccare:

- Non digitate mai username, password, credenziali bancarie e qualsiasi altra informazione personale a meno che non siate completamente sicuri della sua autenticità. A tal proposito, verificate sempre il nome di dominio (e con molta attenzione, a volte la differenza tra un nome vero e uno falso è minima, anche di un solo carattere). E cliccate solo su link affidabili;
- Chiedetevi sempre cosa offre quel sito in particolare, se ciò che propone sembra sospetto e se davvero avete

bisogno di registrarvi;
- Assicuratevi che i vostri dispositivi siano ben protetti.

https://www.key4biz.it/anche-lhttps-non-sinonimo-un-sito-sicuro/213710/

‘Cybersecurity, nel 2018 le tecnologie made in Italy di Tiesse’. Intervista a Vincenzo Luciano Lucrezia

Tiesse produce router e apparati M2M tra i migliori al mondo destinati alle principali Telco e ai maggiori System Integrator sul mercato. Il focus degli investimenti di Tiesse nel 2018 è targato Cybersecurity. Il contesto attuale, in cui si opera, richiede che la sicurezza non sia solo più una funzionalità ma diventi centrale nel disegno delle soluzioni di rete. Tiesse ha deciso di concentrare risorse e competenze in questa area collaborando con aziende specializzate ed inserendo nuovi profili con competenze specifiche. Di questa nuova strategia abbiamo parlato con **Vincenzo Luciano Lucrezia**, Chief Technology Officer di Tiesse, azienda che quest’anno compie 20 anni.

Key4biz. ***Lucrezia, perché questa svolta verso la cybersecurity?***

Vincenzo Luciano Lucrezia. Non si tratta di una svolta ma di un rafforzamento dell'attenzione a questa tematica che abbiamo sempre avuto ben presente. Il cybercrime è una minaccia sempre più grave e sentita da parte delle aziende. Il nostro paese è impegnato nella lotta al crimine cibernetico e noi di Tiesse, in quanto realtà italiana che da sempre sostiene il valore delle tecnologie made in Italy, vorremmo essere pronti a dare il nostro contributo attivo e diretto. Una strategia in linea con la strada percorsa fino ad ora con il nostro presidente ***Mario Ciofalo***, recentemente scomparso, fautore di una linea politica sistemica in difesa del made in Italy, a maggior ragione in ambito sicurezza.

Key4biz. ***Come intendete muovervi?***

Vincenzo Luciano Lucrezia. Intendiamo investire in risorse e competenze attraverso un piano di assunzioni, in parte già attuato, indirizzato a profili con formazione di ingegneria informatica e matematica ad alta specializzazione.

Key4biz*. In che modo?*

Vincenzo Luciano Lucrezia. Concretamente con investimenti interni, tra cui l'apertura di una nuova sede a Torino, ed anche attraverso collaborazioni con società esterne, autonome, atte ad effettuare l' assessment delle nostre soluzioni per quanto riguarda l'assenza di falle di progettazione e di configurazione dei router e con l'obiettivo di individuare e trovare qualunque soluzione che migliori la performance dei nostri prodotti.

Key4biz. ***Ci parli della nuova sede di Torino, che affiancherà quelle di Ivrea, Avezzano e Roma.***

Vincenzo Luciano Lucrezia. La scelta di investire in una nuova sede a Torino nasce dall'esigenza di una sempre migliore integrazione con i centri di ricerca e le competenze presenti nell'area metropolitana, soprattutto quelle che fanno capo al Politecnico e al Dipartimento di Informatica dell'Università degli Studi di Torino, con cui da anni si è instaurato un rapporto di collaborazione sia per i contenuti che per l'accesso a risorse qualificate da inserire in azienda.

La nuova sede sarà il luogo ideale per ampliare gli scambi, le collaborazioni e i progetti di ricerca con gli atenei torinesi, facilitata anche da una collocazione territoriale migliore di quella di Ivrea, che indubbiamente soffre per il noto isolamento infrastrutturale dell'area dell'eporediese.

Key4biz. ***Di cosa si occuperà la nuova sede di Torino?***

Vincenzo Luciano Lucrezia. Le aree di sviluppo in cui si concentreranno le attività della neo sede, basata presso l'Environment Park di Torino, saranno focalizzate sulle tematiche di SDN (software defined network) e NFV (network functions virtualization) ed ovviamente della sicurezza, per realizzare prodotti sempre più Secure by Design e idonei ad essere utilizzati in infrastrutture nazionali mission critical.

La nuova apertura è in linea con il disegno di rafforzare ulteriormente le capacità di R&S , che costituisce l'80% dell'impegno dell'azienda ed è fondamentale per sostenere il nostro vantaggio competitivo nel mercato dei router ed apparati M2M/IoT di fascia professionale in cui operiamo da 20 anni.

‘Cybersecurity, nel 2018 le tecnologie made in Italy di Tiesse’. Intervista a Vincenzo Luciano Lucrezia

---

Sicurezza nazionale, 007 lanciano l’allarme su possibili cyber-condizionamenti del voto del 4 marzo

“*A fronte del crescente grado di interconnessione che caratterizza le società moderne e di una minaccia che ha continuato ad essere sempre più sofisticata e persistente, l’architettura nazionale cyber ha conosciuto interventi di modifica miranti a potenziare ulteriormente le capacità di difesa cibernetica del Paese*”.

Si è tenuta stamattina a Palazzo Chigi la tradizionale presentazione della “***Relazione annuale sulla politica dell’informazione per la sicurezza***”, a cura del Dipartimento delle informazioni per la sicurezza (Dis). Sono intervenuti il Presidente del Consiglio, **Paolo Gentiloni**, e il Direttore generale del Dis, **Alessandro Pansa**.

Un documento che a cadenza annuale illustra la situazione del Paese e dello scenario internazionale dal punto di vista delle principali minacce alla sicurezza e la stabilità delle

Istituzioni democratiche e della convivenza civile.

"*Difendere lo spazio informatico è difendere il nostro territorio nazionale. La difesa dai rischi per la sicurezza informatica è la difesa dell'Italia*", ha spiegato il presidente del consiglio in occasione della presentazione.

Si è fatto prima il punto sui dieci anni della Relazione (2007 – 2017), quindi si sono affrontati gli argomenti più caldi in tema sicurezza nazionale, come il terrorismo internazionale specialmente jihadista, quindi le crisi regionali e gli attori globali, il fenomeno migratorio, le possibili minacce eversive interne e l'attività estremista, con in chiusura un allegato tutto dedicato alle capacità cibernetiche del Paese, lo stato delle cyber minacce e le possibili evoluzioni future.

Rilevante filone d'interesse è quello connesso con la "***minaccia ibrida***", che si traduce in **campagne di influenza** che, "*prendendo avvio con la diffusione online di informazioni trafugate mediante attacchi cyber, **mirano a condizionare l'orientamento ed il sentiment delle opinioni pubbliche, specie allorquando queste ultime sono chiamate alle urne***".

A seguito di questo tipo di minaccia, "*si ritiene possibile un aumento tanto delle campagne di spionaggio digitale da parte di attori statuali, con l'impiego di modalità operative di offuscamento per rendere più difficoltosa l'identificazione dell'attaccante (cd. attribution), quanto delle minacce ibride, specie in prossimità di passaggi cruciali per i sistemi democratici*".

Partendo da quanto accaduto nel 2017, la Relazione evidenzia due principali filoni di cyber minacce: il primo, quello tradizionale dei ***malware/ransomware***; un secondo più centrato sulle campagne di influenza e la concreta possibilità di influenzare e quindi "condizionare l'orientamento ed il sentiment delle opinioni pubbliche", soprattutto in prossimità della tornata elettorale del 4 marzo 2018.

In prospettiva, hanno precisato i nostri 007, "*si ritiene possibile un aumento del ricorso, da parte di attori statuali, a modalità operative di offuscamento*", anche per conseguire profitti volti a finanziare lo sviluppo di attività sanzionate dalla comunità internazionale. Al contempo, appare ragionevole ipotizzare "*la crescita del trend delle minacce ibride*".

In un contesto del genere, si legge nelle conclusioni e nei trend evolutivi del fenomeno, "***lo strumento cibernetico è destinato a divenire sempre di più un agevolatore di attività di influenza***", realizzate attraverso "*la manipolazione e la diffusione mirata di informazioni preventivamente acquisite attraverso manovre intrusive nel cyber-spazio*", così da "*orientare le opinioni pubbliche, fomentare le tensioni socio-economiche, accrescere l'instabilità politica dei Paesi dell'area occidentale, all'atto dell'adozione di decisioni strategiche, ritenute dall'attore ostile sfavorevoli ai propri interessi*".

Il capitolo blockchain e criptovalute: "*La crescente diffusione delle criptovalute (Bitcoin, Ethereum, etc.) prospetta criticità legate ad un loro potenziale utilizzo a fini di riciclaggio, evasione fiscale, esportazione illecita di capitali e finanziamento al terrorismo*".

Le *criptocurrencies* rappresentano, secondo la Relazione, solo una delle possibili applicazioni della tecnologia blockchain. Nel 2017, "*un numero crescente di istituzioni e aziende, soprattutto nel settore finanziario, ha avviato progetti basati su questa tecnologia con lo scopo di creare infrastrutture immateriali innovative che consentano, tra l'altro, di abbattere i costi delle operazioni di scambio di titoli di proprietà o di valori*".

Video della presentazione della Relazione 2017

[embedded content]
https://www.key4biz.it/sicurezza-nazionale-007-lanciano-lallar

me-possibili-cyber-condizionamenti-del-voto-del-4-marzo/213548/

Smart meters e sicurezza informatica, case a rischio cyber attacchi secondo l'intelligence britannica

Un piano da 11 miliardi di sterline per installare contatori intelligenti (***smart meters***) nelle case dei cittadini britannici. Il Governo del Regno Unito, come molti altri Paesi europei, punta così ad una trasformazione digitale sul territorio che faccia leva anche sull'**efficienza energetica**.

Gli *smart meters* consentono agli utenti di tenere sotto controllo i consumi e quindi ridurli. L'**inquinamento atmosferico** che sta soffocando le città e rendendo sempre più caldo il pianeta deriva in gran parte proprio da sistemi di riscaldamento scarsamente efficienti per sprechi, perdite e comportamenti poco virtuosi dei cittadini stessi.

Secondo quanto annunciato dal Governo di Londra a gennaio di quest'anno, i lavori per l'installazione di questi contatori di nuova generazione saranno terminati nel 2020. Al momento, ha riportato il quotidiano *The Telegraph*, le abitazioni con *smart meter* attivo sono 8 milioni di unità su 27 milioni totali.

Fin qui tutto bene, ma la *Government communications headquarters* (**Gchq)**, l'agenzia governativa che si occupa della sicurezza, nonché dello spionaggio e controspionaggio, nell'ambito delle comunicazioni del Regno Unito, ha lanciato un nuovo allarme nei giorni scorsi, relativo alla **cyber sicurezza** di queste apparecchiature. Essendo questi *smart meters* sempre connessi in rete, anche per l'invio di dati sui consumi ai fornitori di energia, il loro livello di sicurezza informatica è costantemente messo alla prova dai cyber criminali.

Proprio a causa dell'alto rischio di attacchi informatici è stato rimandato il lancio dei nuovi contatori digitali **Smets 2**.

L'Agenzia ha indirettamente puntato il dito anche sull'***internet of things*** e la sicurezza domestica: sfruttando le vulnerabilità dei contatori l'attacco informatico potrebbe rapidamente estendersi al resto della casa e dei device interconnessi tra loro.

I cyber criminali sono così messi in condizione di danneggiare i fornitori di luce elettrica e gas e i consumatori stessi, a cui peraltro potrebbero esser sottratti soldi sui conti correnti e qualsiasi tipo di informazione sensibile.

Come ha spiegato a *The Mail* l'esperto informatico di WiFore, **Nick Hunn**: "*Il problema è che il piano di attivazione degli smart meter è portato avanti da funzionari in carriera che poco sanno di cyber sicurezza e poco si curano delle possibili conseguenze in termini di danni economici e materiali che potrebbero subire aziende e cittadini*".

Completamente diversa è l'opinione dell'agenzia governativa **Smart Energy GB**, preposta alla realizzazione del piano *smart meter* per la Gran Bretagna: "*I contatori intelligenti sono assolutamente sicuri ed affidabili, solo i dati energetici sono registrati dal dispositivo, e comunque sono*

crittografati. Il resto delle informazioni personali, dall'indirizzo al conto bancario, non sono accessibili tramite contatore".

La Gchq, dal canto suo, ha precisato: "*Sicuramente lo Smart metering system troverà presto il giusto equilibrio tra sicurezza informatica e business, nel rispetto dei più ampi obiettivi di politica e sicurezza nazionale*".

> *Smart meters e sicurezza informatica, case a rischio cyber attacchi secondo l'intelligence britannica*

The Biennial Cyber-Threat: How to Keep Your Company Safe During the Olympics

With the 2018 Winter Olympics in full swing, these biennial Games may already be challenging the stamina and commitment of your security team almost as much as that of the athletes involved.

Related: This Is Why We Need To Focus More on Cybersecurity Strategy

How can the Olympics in faraway PyeongChang be a threat to you? Malicious actors know that many of your employees will be tuning in to the Games from work. Those actors can then use the Olympics to launch far-reaching malware campaigns as well

as more targeted attacks.

In fact, Olympic officials confirmed that the Games themselves were already the target of a sophisticated attack during last week’s opening ceremony.

While the majority of businesses will not find themselves singled out in such blatant fashion, they should still prepare for the possibility of a barrage of spam emails and other attempts designed to lure their employees into clicking on links or downloading files that could infect their companies’ machines and overall networks.

And that will only get worse before it gets better: As the Winter Games move closer to their grand finale, this potentially damaging email traffic will only increase during the final rounds of popular events and the coverage of the closing ceremonies.

That’s why business leaders should pay attention to the fact that, whether they like it or not, many employees are getting their updates and video highlights at work, which is why organizations are seeing their network traffic soar.

During the Summer Olympics, in Rio in 2016, the network broadcasting them — NBC — provided over 4,000 hours of streamed content. Amid all the resulting traffic, according to a survey by WAN-optimizer Riverbed Technologies, 69 percent of organizations polled reported at least one network issue caused by employee access to Games content.

Related: How These 10 Companies Are Powering the Winter Olympics

This surge in network activity and monitoring volume provides an effective screen for malicious actors, who can hide their activity amid the noise, the change in traffic flows, system-usage anomalies and, frankly, chaos. Network monitoring can be expected to be flooded. And that will mean that individual

events will be far less visible, maybe even lost, in the static, while end-users are bombarded with opportunities to view content that may or may not be authentic.

What you can do to protect your network.

To minimize the likelihood of experiencing an unplanned Olympic “downhill event” in your own security management program, here are five recommendations for dealing with this upsurge during the games:

Partition corporate and BYOD traffic. While many employees attempt to access Olympic coverage at work, most do so from their personal devices. Where possible, it’s always a good idea to create one network for approved corporate traffic and a separate, second one for employee/guest device connectivity.

In this way, you might be able to use the Olympics as a catalyst to create that second, less-trusted network that you’ve always wanted, restricting potentially untrusted traffic to a second, partitioned network.

Inform your employee users that network activity is going to be monitored even more closely than usual. Let them know that there are increases in traffic and traffic types expected during the Olympics, and that the organization is going to step up monitoring in order to avoid unexpected network congestion and down time.

If you can, set some limits or add some restrictions for employee visits to these streaming sites, and to the links they are allowed to visit. For the period of the Olympics, some additional network filtering may be critical to encourage users not to click on links from untrusted sources. They may not hold back because of fear of infection, but they will likely resist the temptation if they think this activity

is being closely monitored.

Educate your users about the risks of social engineering**.** Whether it is inbound emails from what look like national team-related groups, or short-links posted in comments sections of active articles and newsgroups, your users should recognize that smart attackers are using the passion and intensity of Olympics enthusiasts to get them to make mistakes.

Instruct employees how to examine hyperlinks before clicking on them, and show them how to scrutinize URLs to ensure the sites they are visiting are authentic and secure.

Increase your *outbound* network traffic scrutiny. It's very common for organizations to encounter a spike in inbound traffic as users begin to stream games, updates and communications about their favorite teams and events. While continuing your internal and inbound monitoring is important, it's also important to add some additional checks for unusual *outbound* behaviors.

This action will provide a more tractable means of detecting possible internal corruptions and breaches, without your having to sort through that spiky influx of media and data.

Overall, enjoy the Olympics. Root for your favorite athletes (Go, Team U.S.A.!) But also use the Olympics as a catalyst for getting more proactive and strategic about your company's security. From an IT perspective, a positive aspect of the Games is that the challenges they present occupy a strictly defined window of time. You know exactly when the risk period is going to start and how long it's going to last.

And that kind of predictability is a rare thing in cybersecurity. In general, damaging events are far more likely to occur when you least expect them, and mitigation can sometimes stretch on far longer than you'd originally planned. So, as you step back and bolster your network to handle

additional threats and traffic these next two weeks of the Olympics, take the opportunity to consider more strategic improvements that can keep your organization more secure the whole year ‘round.

Related: 10 Jaw-Droppingly Awesome and Motivational Tweets From Olympic Figure Skater Adam Rippon

The Olympics happen every two years, and their impact on infrastructure and security shouldn’t surprise anyone. Plan ahead. And get your monitoring, back-up, endpoint security and disaster recovery in line. With your security ensured, you should be able to celebrate at the end, no matter who is on the medals awards platform.

https://www.entrepreneur.com/article/309097

Falla nei processori, 7 consigli per contrastare le vulnerabilità Spectre e Meltdown

Spectre e **Meltdown** sono i nomi in codice che sono stati dati a diversi ceppi di un nuova classe di attacchi informatici, individuati nel gennaio 2018, che mirano la vulnerabilità della maggior parte dei chip di computer prodotti negli ultimi 20 anni.

Attraverso uno studio condotto dall’azienda americana **Gartner Inc,** multinazionale operante nella consulenza strategica, ricerca e analisi nel campo dell’Information Technology, i

leader della sicurezza e della gestione del rischio devono adottare un approccio pragmatico e basato sul rischio per le minacce in corso poste da questa nuova classe di vulnerabilità.

"*Il rischio è reale, ma con un piano di bonifica chiaro e pragmatico basato sul rischio, i responsabili della sicurezza e della gestione del rischio possono fornire ai leader aziendali la certezza che il rischio marginale per l'azienda è gestibile e viene affrontato*" –ha affermato **Neil MacDonald**, vicepresidente, di **Gartner**.

Ma prima andiamo con ordine, spieghiamo cosa intendiamo quando parliamo di Meltdown e Spectre.

Meltdown

È la falla che interessa computer desktop, portatili e sistemi cloud che utilizzano diverse generazioni di processori **Intel**, prodotti a partire dal 1995 (sembra facciano eccezione le versioni Itanium e Atom, ma solo se prodotte prima del 2013). Per ora i ricercatori hanno la certezza che la falla riguardi Intel, mentre sono ancora in corso verifiche per accertarsi se siano coinvolti anche processori di altre marche e con architetture diverse come ARM e AMD.

Spectre

I ricercatori stimano che "praticamente tutti i sistemi" siano affetti da Spectre, quindi: computer desktop, portatili, server cloud e smartphone. Il problema riguarda i processori Intel, **AMD** e **ARM**. L'estensione della falla sembra quindi essere molto maggiore e per gli esperti di sicurezza le prospettive non sono incoraggianti, considerato che una

soluzione software per questo problema richiede un approccio articolato, quindi più tempo.

L’azienda ha identificato sette passaggi che i responsabili della sicurezza possono attualmente adottare per ridurre i rischi:

1. **Riconosci il rischio, ma non farti prendere dal panico**

I moderni sistemi operativi (OS) e gli hypervisor dipendono da modelli di autorizzazione strutturati e stratificati per garantire l’isolamento e la separazione della sicurezza. Poiché questa implementazione di progettazione sfruttabile è sull’hardware, sotto il sistema operativo e l’hypervisor, tutti i livelli software sopra sono interessati e vulnerabili. Tuttavia, la memoria può essere solo letta, ma non modificata. Lo sfruttamento del difetto richiede che il codice non sicuro sia introdotto ed eseguito sul sistema di destinazione, il che dovrebbe essere estremamente difficile su un server o un’appliance ben gestiti come una rete o un’appliance di archiviazione. C’è anche un vantaggio nel non ricorrere alla “patch di panico”. Le patch iniziali creavano conflitti con alcune offerte antivirus e bloccavano i computer **Windows**.

2. **Fai un inventario dettagliato**

Quasi tutti i moderni sistemi IT saranno interessati in una certa misura. Dal momento che Y2K ha una vulnerabilità interessata, molti sistemi (desktop, dispositivi mobili, server, macchine virtuali, appliance di rete e di archiviazione, tecnologia operativa e dispositivi di Internet of Things) hanno richiesto un piano di azione pianificato e deliberato per gli interventi di riparazione. Il punto di partenza per i responsabili della sicurezza deve essere un inventario dei sistemi interessati. In alcuni casi, la decisione appropriata per il rischio sarà quella di non applicare la patch. Per ciascun sistema, è necessario un

database dettagliato o un foglio di calcolo per tenere traccia del dispositivo o del carico di lavoro, della versione del suo microprocessore, della versione del firmware e del sistema operativo.

3. **Sviluppare un piano di rimedio prioritario**

Le vulnerabilità non sono direttamente sfruttabili da remoto. Un attacco di successo richiede che l'attaccante esegua il codice sul sistema. Pertanto, il controllo dell'applicazione e la whitelist su tutti i sistemi riducono notevolmente il rischio di esecuzione di codice sconosciuta. Tuttavia, l'infrastruttura condivisa come infrastruttura di servizio è particolarmente vulnerabile fino a quando i provider di cloud non aggiornano il loro firmware e il livello hypervisor sottostante (che i principali provider hanno fatto).

4. **Dare priorità agli sforzi di rimedio**

Quando si escogita una strategia di correzione, si consiglia di suddividere la strategia in fasi prioritarie, poiché il rischio, le implicazioni sulle prestazioni e i potenziali aggiornamenti hardware richiesti variano notevolmente tra i casi d'uso. Inizia con i sistemi che rappresentano il maggior rischio – computer, virtual desktop infrastructure **(VDI)**, smartphone e server rivolti all'esterno.

5. **Riconoscere che a volte la decisione appropriata e basata sul rischio non deve essere applicata**

I responsabili della sicurezza devono essere preparati per scenari in cui la decisione appropriata potrà essere quella di non applicare le patch. In alcuni casi, ciò sarà dovuto alla mancanza di patch sui sistemi più vecchi. In altri casi, l'impatto sulla performance non viene compensato dalla riduzione del rischio, quindi le patch non verranno applicate. Anche per alcuni server ben gestiti, è possibile decidere di rinunciare alle patch per proteggere le prestazioni fino a quando le patch future avranno impatti accettabili. Tuttavia,

per i carichi di lavoro del server, quando le caratteristiche delle prestazioni lo consentono, si consiglia di aggiornare patch e firmware.

6. **Non inserire codici sconosciuti nei dispositivi**

Per i sistemi che non sono riparati o solo parzialmente riparati, più controlli attenuanti possono ridurre il rischio. Il problema più importante da affrontare è limitare la possibilità di inserire un codice sconosciuto o non attendibile sul dispositivo. Riducendo questo, i rischi sono significativamente ridotti, poiché gli attacchi richiedono l'esecuzione di codice locale.

7. **Pianificare ulteriori sforzi di riduzione del rischio nei prossimi anni**

Spectre e Meltdown rappresentano una nuova classe di vulnerabilità, e questo è solo l'inizio. *"In definitiva, l'eliminazione completa dell'implementazione sfruttabile richiederà un nuovo hardware non ancora disponibile e non previsto per 12 a 24 mesi, motivo per cui l'inventario dei sistemi fungerà da roadmap fondamentale per i futuri sforzi di riduzione del rischio*", ha affermato MacDonald. "Se *questi carichi di lavoro sono fisici, virtuali, cloud o pubblici ciò dovrebbe diventare una pratica standard e una priorità per tutti i leader della sicurezza e della gestione dei rischi nel 2018. "*

Falla nei processori, 7 consigli per contrastare le vulnerabilità Spectre e Meltdown