R.it | Sicurezza

Anonymous 'buca' governo e ministeri: "Abbiamo i vostri dati personali"

Un nuovo leak ha per oggetto contratti, stipendi, carte d'identità e indirizzi email di personale degli Interni, della Difesa, della Marina e della Presidenza del Consiglio. Il nuovo colpo alla cybersicurezza assestato dal gruppo di hacker anonimi

di ARTURO DI CORINTO

UNA miniera di dati, riservati e personali. Di poliziotti, militari, marinai stellati del Bel Paese. Così si presenta il leak appena diffuso in Rete da Anonymous: "Cittadini, siamo lieti di annunciarvi, per il diritto della democrazia e della dignità dei popoli, che siamo in possesso di una lista di dati personali relativi al ministero dell'Interno, al ministero della Difesa, alla Marina Militare nonché di Palazzo Chigi e Parlamento Europeo."

Dati riservati e molto personali, che includono patenti di guida, carte d'identità, dichiarazione dei redditi, numeri di telefono. Ma anche ordini di servizio, note e contratti riferiti a personale e attività di militari e poliziotti, con tanto di stipendio e curriculum. C'è anche l'indicazione delle frequenze da usare per comunicare nei viaggi all'estero del presidente **Paolo Gentiloni** e poi le attività della Digos durante le manifestazioni, per arrivare fino a targhe di auto e assicurazioni di servizio.

·IL MESSAGGIO IN RETE

La rivendicazione di Anonymous è piuttosto minacciosa: "Governo, corruttore di democrazia, la rivoluzione passa anche qui, inarrestabile, il cui ideale conosce ora i vostri nomi, i vostri contatti telefonici, le vostre residenze. Possediamo anche fotocopie dei vostri documenti personali, di quelli dei vostri parenti ed amici, contratti di lavoro, contratti d'affitto, buste paghe e molto altro." e continua criticando lo scarso livello di sicurezza dei militari stessi: "Per l'ennesima volta lo Stato italiano tradisce ed imbarazza i valori dei nostri militari che hanno giurato di difenderlo. Ma difendere chi? Difendere i propri cittadini

o un governo che imbarazza le stesse forze di difesa?"

·CYBERSICUREZZA A RISCHIO
La notizia del leak, pubblicata su un blog di Anonymous e rimbalzata su Twitter via YourAnonRevolt, lascia di stucco, perché offre molte ipotesi sullo stato dell'arte della sicurezza informatica del Sistema Italia. Proprio oggi che a Roma si tiene il 360 cybersecurity Summit dedicato alla sicurezza delle nostre aziende.

Secondo **Pierluigi Paganini**, consulente del Governo e membro dell'Agenzia europea per la sicurezza informatica, "I dati forse non sono così importanti, ma ci obbligano a chiederci quale sia l'effettivo livello di consapevolezza dell'importanza di proteggerli e con essi le persone a cui si riferiscono".

·"LA DEMOCRAZIA MUORE"
Il comunicato di Anonymous finisce con una citazione da *La Repubblica* di Platone, il filosofo greco: "Ecco, secondo me, come nascono le dittature. Esse hanno due madri. Una è l'oligarchia quando degenera, per le sue lotte interne, in satrapia. L'altra e' la democrazia quando, per sete di liberta' e per l'inettitudine dei suoi capi, precipita nella corruzione e nella paralisi. Allora la gente si separa da coloro cui fa la colpa di averla condotta a tale disastro e si prepara a rinnegarla prima coi sarcasmi, poi con la violenza che della dittatura è pronuba e levatrice. Così la democrazia muore: per abuso di se stessa. E prima che nel sangue, nel ridicolo."

·I PRECEDENTI
Non è la prima volta che Anonymous si manifesta in queste forme. Anzi, a dire il vero gli Anonymous italiani sembravano scomparsi dopo i dissidi interni fra quelli che avevano contribuito ad alcune eclatanti operazioni di sabotaggio nei confronti dell'Expo a Milano, dell'Agenzia del Farmaco, dei siti degli Esteri e della Polizia di Stato. All'epoca avevano bloccato la biglietteria di Expo, bloccato il sito del Family Day e cambiato i connotati dell'Aifa con un'operazione di defacement.

·DIETRO LA MASCHERA
In particolare sembravano ridotti al silenzio dopo l'arresto di alcuni attivisti considerati dagli inquirenti i portavoce dell'organizzazione. Un'organizzazione che però nessuno nell'underground riconosce, visto che chiunque può indossare la maschera di Anonymous e che chiunque può
partecipare alle sue azioni dimostrative, le AnonOps, senza rispondere ad alcun capo.
Adesso, quello che sembrava un grattacapo in meno per la cybersecurity italiana è tornato alla ribalta sotto il cappello di Anonymous.

WIRED.IT

Anonymous va a spasso per i siti ministeriali e preleva dati sensibili

Il collettivo di hacker ha violato i server di diversi ministeri italiani e del parlamento europeo e annuncia di avere fatto incetta di dati sensibili

"Cittadini, siamo lieti di annunciarvi, per il diritto della democrazia e della dignità dei popoli, che siamo in possesso di una lista di dati personali relativi al ministero dell'Interno, al ministero della Difesa, alla Marina Militare nonché di Palazzo Chigi e Parlamento Europeo"

Inizia con queste parole il comunicato con cui Anonymous Italia annuncia di avere fatto razzia di **dati sensibili** tra i quali ordini di servizio, attività militari, numeri di targhe delle automobili di servizio, carte di identità, numeri di telefono, contratti di affitto, stipendi, dichiarazioni dei redditi ed indirizzi email.
Tutto ciò mentre a Roma si svolge il Cyber Security 360 Summit, evento durante il quale è stato a più riprese sostenuto che, senza adeguate risorse, la cybersecurity è un'attività orfana e al cui margine è stato evidenziato che durante i primi sei mesi del 2017 i cyberattacchi sono cresciuti dell'8,35% su scala mondiale.
Anonymous enfatizza il leak in onore della democrazia, ridando ai cittadini la possibilità di sapere ciò che il governo **non rende pubblico** ma neppure tutela a dovere.

Tra i file prelevati, circa 17 megabyte in tutto, ci sono anche scambi di email tra funzionari del governo e altri della polizia che riguardano il viaggio a Bologna del premier Gentiloni previsto per il 15 novembre.

Anonymous: “Sottratte informazioni riservate italiane”. C’è anche scambio di mail su visita Gentiloni a Bologna domani

"Cittadini - scrivono gli hacker sul loro blog- siamo lieti di annunciarvi, per il diritto della democrazia e della dignità dei popoli, che siamo in possesso di una lista di dati personali". La notizia del leak arriva proprio nel giorno in cui a roma si tiene il 360 Cybersecurity Summit, dedicato proprio alla sicurezza in rete

Anonymous ha colpito ancora. Questa volta nel mirino del gruppo **hacker** sono finite alcune informazioni riservate dell‘**Italia** e del **Parlamento Europeo**. Centinaia di mail, numeri di telefoni, ordinanze di servizio delle questure ma anche buste paga e fotocopie di documenti di appartenenti a forze di polizia e forze armate sono state pubblicate sul loro **blog**. E tra questi, anche uno scambio di mail tra funzionari di palazzo Chigi e le forze di polizia sulla visita del **Presidente del Consiglio Paolo Gentiloni**domani a **Bologna**.

Anonymous ha annunciato il furto di queste informazioni riservate con un post sul suo blog, dove si legge: “Cittadini – scrivono gli hacker – siamo lieti di annunciarvi, per il **diritto della democrazia** e della dignità dei popoli, che siamo in possesso di una lista di dati personali relativi al **Ministero dell’Interno,** al **Ministero della Difesa,** alla **Marina Militare** nonché di **Palazzo Chigi** e**Parlamento Europeo**“. “Governo **corruttore** di democrazia – prosegue il post – la rivoluzione passa anche qui, inarrestabile, il cui ideale conosce ora i vostri nomi, i vostri contatti telefonici, le vostre residenze. Possediamo anche fotocopie dei vostri documenti personali, di quelli dei vostri parenti ed amici, contratti di lavoro, contratti d’affitto, buste paghe e molto altro. Per l’ennesima volta lo Stato Italiano t**radisce ed imbarazza** i valori dei nostri militari che hanno giurato di difenderlo. Ma difendere chi? Difendere i propri cittadini o un governo che imbarazza le stesse forze di difesa?”.

La notizia del **leak** è stata diffusa dagli stessi hacker sul loro profilo *Twitter*, YourAnonRevolt:

La notizia è arrivata nello stesso giorno in cui a Roma si tiene il **360 Cybersecurity Summit**, dedicato proprio alla sicurezza in rete. Tra i documenti scaricabili dalla rete c’è, ad esempio, un’ordinanza della Questura di Roma relativa a diverse manifestazioni con data 10 novembre; uno scambio di **mail** tra funzionari di palazzo Chigi e membri della **sicurezza**, con tutti i nomi di chi oggi si sarebbe occupato dei sopralluoghi in vista dell’arrivo domani del premier Gentiloni. Ci sono poi le frequenze radio chieste e concesse all’Italia per le comunicazioni di sicurezza in occasione della visita del presidente del **Consiglio a Bruxelles** lo scorso ottobre, un documento del ‘Centro unico stipendiale esercito’ con le disposizioni relative agli stipendi dei **militari** e i **numeri di cellulare** di personale del ministero dell’Interno in missione all’estero. E, ancora, dati personali e foto di agenti e militari: curricula, dichiarazioni dei redditi, fotocopie di passaporti e carte d’identità, buste paga e contratti d’affitto. Dati privati e molto riservati, che ora sono scaricabili dal loro

blog. Per introdurre il comunicato, Anonymous ha scelto una citazione presa da ‘La Repubblica’ di **Platone**: “Ecco, secondo me, come nascono le dittature. Esse hanno due madri. Una è l’oligarchia quando degenera, per le sue lotte interne, in satrapia. L’altra è la **democrazia** quando, per sete di libertà e per l’inettitudine dei suoi capi, precipita nella **corruzione** e nella paralisi. Allora la gente si separa da coloro cui fa la colpa di averla condotta a tale disastro e si prepara a rinnegarla prima coi sarcasmi, poi con la violenza che della dittatura è pronuba e levatrice. Così la democrazia muore: per abuso di se stessa. E prima che nel sangue, nel ridicolo.”

NOTIZIE RADIOCOR - FINANZA

ECONOMIA E FINANZA: GLI AVVENIMENTI DI MARTEDI' 14 NOVEMBRE

ECONOMIA - Milano: "Salone del risparmio sostenibile", con la presenza di Anasf, Efpa e Forum per la finanza sostenibile

Palazzo delle Stelline

- Milano: conferenza stampa di presentazione del 'Progetto Giovani' edito da Rizzoli Lizard. Ore 11,00. presso l'Istituto Nazionale dei Tumori, via Venezian, 1

- Milano: presentazione del nuovo orario invernale di Trenitalia. Ore 15,00. Partecipano: Tiziano Onesti, presidente Trenitalia, e Orazio Iacono, a.d. e d.g

Trenitalia. Sala Reale, Stazione di Milano Centrale

- Milano: il presidente della Repubblica, Sergio Mattarella, in visita alla Fondazione Giangiacomo Feltrinelli. Ore 17,00

- Milano: incontro stampa Nctm per la presentazione di "Are We Fit To Compete?", progetto volto alla promozione dello sport in ambito lavorativo. Ore 18,30. Via Agnello, 12

- Rozzano (Mi): alla presenza del presidente della Repubblica, Sergio Mattarella, inaugurazione del nuovo Campus Humanitas University in occasione della cerimonia di apertura dell'Anno Accademico. Ore 10,30. Partecipano, fra gli altri, Giuseppe Sala, sindaco di Milano; Maria Elena Boschi, sottosegretario Presidenza del Consiglio dei Ministri; Gianfelice Rocca, presidente HU; Carlo Calenda, ministro dello Sviluppo economico. Presso Centro Congressi Humanitas, via Manzoni, 113

- Genova: Orientamenti 2017 'Formazione duale, Apprendistato e Alternanza Scuola-Lavoro'. Ore 10,30

Partecipa, tra gli altri, Giovanni Brugnoli, Vice Presidente di Confindustria per il Capitale Umano

Magazzini del Cotone, Porto Antico

- Milano Marittima (Ra): cerimonia di consegna dei riconoscimenti di Excelsa - Confindustria Romagna Award

Ore 17,00. Via Jelenia Gora, 12

- Roma: Cyber Security 360 Summit, evento organizzato da Gruppo Digital360. Ore 9,30. Centro Congressi Roma Eventi, piazza di Spagna

- Roma: "L'Italia a sistema con Alis e Confalis" assemblea generale 2017. Ore 10,30. Partecipano, tra gli altri, Guido Grimaldi, presidente Alis; Antonio Gentile, sottosegretario di Stato ministero dello Sviluppo economico; Gabriele Toccafondi, sottosegretario di Stato ministero dell'Istruzione; Barbara Degani, sottosegretario di Stato ministero dell'Ambiente; Mario Mattioli, presidente Confitarma; Bernardo Mattarella, a.d. Banca del Mezzogiorno; Roberto Nardella, presidente Confimea

Auditorium Parco della Musica, via Pietro De Coubertin, 30

- Roma: aggiornamento congiunturale "L'economia del Lazio"

Ore 12,00. Banca d'Italia, via XX Settembre, 97

- Francoforte: il presidente Bce, Mario Draghi, partecipa al panel "At the heart of policy: challenges and opportunities of central bank communication" con Janet Yellen, presidente Fed; Mark Carney, governatore Bank of England; Haruhiko Kuroda, governatore Bank of Japan . Ore 11,00. Presso sede Bce.

Red-

affaritaliani.it

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

14 novembre 2017- 14:08

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil. È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia. "Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia", ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. "Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli. Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno

un'offensiva grave nell’ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%). “Se il 2016 è stato l’annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione e` concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli."Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressivita` degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati”, ha spiegato. In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil. “Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi”.

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

14/11/2017 14:08

Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia.

"Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia", ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica.

"Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli.

Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%).

"Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli.

"Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati", ha spiegato.

In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil.

"Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi".

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

DATI

Pubblicato il: 14/11/2017 14:08

Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia.

"Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia", ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica.

"Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli.

Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%).

“Se il 2016 è stato l’annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli.

"Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati”, ha spiegato.

In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil.

“Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi”.

TAG: Gruppo Digital360, cybersecurity, Ict, imprese

Potrebbe interessarti

Commenti

Per scrivere un commento è necessario registrarsi ed accedere: ACCEDI oppure REGISTRATI

In Evidenza


A Campli l'inaugurazione dei cantieri Open Fiber

Gestione delle risorse, tecnologie e strumenti alla conferenza Fire


“Esperienze a confronto 2017” sul trattamento dell’insufficienza cardiaca


Talent Garden


“Ipotiroidismo nell’anziano”

Pavia, pronta per la Small Valley?


Assemblea Nazionale Manageritalia


Ippodromo San Siro da record, raddoppiati accessi nella stagione


Il Gruppo Bracco apre la settimana della cultura d’impresa di Confindustria


Nuova risonanza magnetica 'hi tech' alla clinica Villalba di Bologna

ArezzoWeb

Digital360: “Strategia cybersecurity sia accompagnata da adeguate risorse”

Roma, 14 nov. (Labitalia) – Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell’8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione ‘militare’ e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l’Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all’1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

È quanto è emerso dal Cyber Security 360 Summit, l’evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell’università sulla situazione della cyber sicurezza in Italia.

“Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall’Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell’architettura cyber in Italia”, ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l’Associazione italiana per la sicurezza informatica.

“Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati”, ha proseguito Faggioli.

Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle

organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%).

"Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli.

"Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati", ha spiegato.

In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security – circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 – appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil.

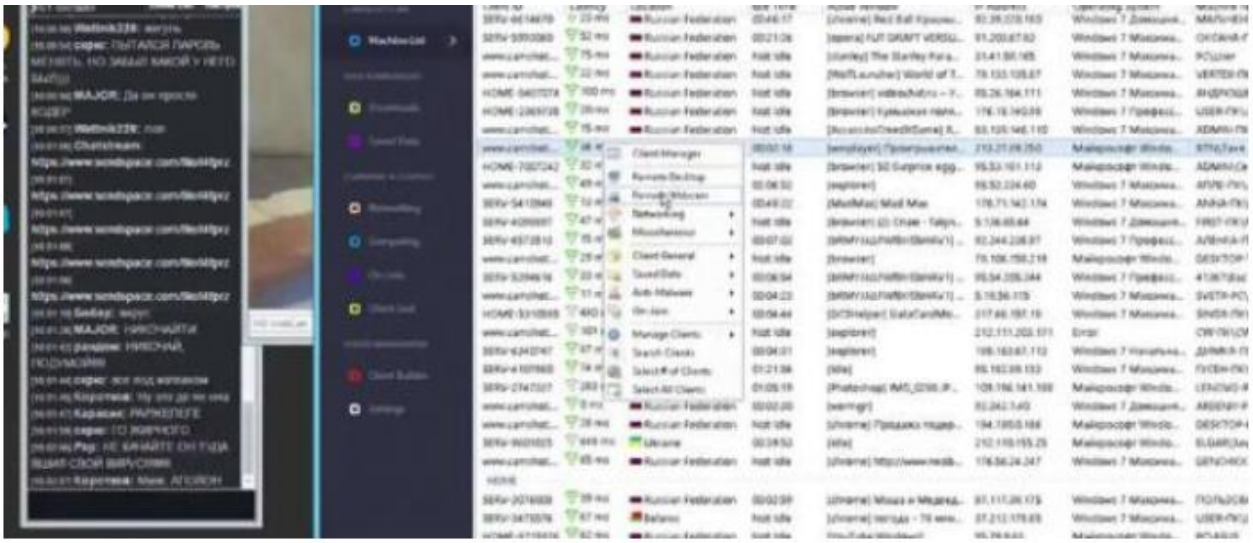
"Nello scenario attuale – ha concluso il Ceo di P4I – Partners4Innovation – è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi".

blastingnews

Sicurezza: violati i dati personali di migliaia di dipendenti dello Stato

Un gruppo di hacker anonimi sarebbe entrato in possesso dei dati personali di dipendenti di Interni, Difesa, Marina e Presidenza del Consiglio

Daniele Cimarelli | Esperto di Tasse | SEGUI
Curata da **Irene Canziani** *Pubblicato il: 14 novembre 2017*



Anonymous viola i dati di migliaia di dipendenti dello Stato

Anonymous, la rete di hacker internazionali, ha appena diffuso sulla Rete un leak con i dati personali **e riservati** di migliaia di dipendenti dello Stato italiano, per la stragrande maggioranza appartenenti a poliziotti, militari e appartenenti alla Marina Militare. Tra questi dati ci sarebbero carte di identità, contratti di ogni tipo, buste paga e indirizzi mail, ma anche numeri di telefono e dichiarazioni dei redditi. Anonymous avrebbe rilasciato anche un messaggio su internet dal tono beffardo in cui ironizza sulla libertà dei popoli e il loro diritto alla democrazia. Non solo ma tra i dati sottratti vi sarebbero anche quelli relativi **alle frequenze radio** da utilizzare quando il Premier, **Paolo Gentiloni,** è impegnato in missioni all'estero.

Il messaggio diffuso sulla Rete

Come dicevamo, Anonymous ha annunciato in un messaggio, particolarmente allarmante, di conoscere diverse informazioni sensibili tra cui numeri di telefono, indirizzi di residenza, fotocopie dei documenti di identità personali. Ma anche i contatti e i documenti di persone legate ai diretti interessati, come parenti ed amici non direttamente implicati nelle attività lavorative dei primi. Inoltre, il messaggio **evidenzia l'incapacità dello Stato** italiano nel proteggere e tutelare le informazioni sensibili di coloro che hanno giurato di difenderlo. E per evidenziare ancora di più la figuraccia fatta dal nostro Paese a livello di **#sicurezza informatica** fa una lunga citazione de *La Repubblica* di **Platone** dove si evidenzia che la democrazia, quando è intrisa di corruzione degenera, prima che nella violenza, nel ridicolo.

La Sicurezza informatica in Italia

L'attacco hacker coincide stranamente con il **360° Summit sulla cybersicurezza** che si svolge proprio oggi a Roma. Anche perché induce a sollevare importanti interrogativi sullo stato della sicurezza informatica in Italia. Come, infatti, ha fatto notare **Pierluigi Paganini,** Consulente del **#Governo** e membro dell'Agenzia europea per la sicurezza informatica, forse i dati non sono poi così importanti come vuol far credere Anonymous ma, certamente, obbligano a riflettere sulla capacità e sul grado di consapevolezza circa la necessità di protezione di tali dati.

La rinascita di Anonymous

Dopo l'arresto di alcuni attivisti che, si pensava, fossero i capi dell'organizzazione, almeno qui in Italia, sembrava che gli hacker fossero stati ridotti al silenzio. Il problema è che chiunque può indossare una maschera e partecipare alle azioni di Anonymous, le **AnonOps**, senza dover rendere conto a nessuno, tantomemo ad una struttura gerarchica sovraordinata. Secondo **Michele Colajanni,** direttore della Cyber Academy e membro del Laboratorio Nazionale di Cybersecurity del Cini, occorre rendersi conto che siamo tutti in prima linea di fronte ai cybercriminali ed è necessario informare quanto più è possibile le persone e formarle alla cybersicurezza, sopratutto se ricoprono incarichi delicati come i militari e le forze di polizia. **#esercito**

CataniaOggi

Digital360: “Strategia cybersecurity sia accompagnata da adeguate risorse”

Da **Adnkronos** - 14 novembre 2017 - 15:37

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil. È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia. ?Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia?, ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. ?Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati?, ha proseguito Faggioli. Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto

al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%). ?Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione e? concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli. "Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressivita? degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati?, ha spiegato. In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil. ?Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi?.

il giornale delle Partite Iva

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

ildenaro.it

Digital360: “Strategia cybersecurity sia accompagnata da adeguate risorse”

Da **ildenaro.it**
-
14 novembre 2017

Roma, 14 nov. (Labitalia) – Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell’8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione ‘militare’ e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l’Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all’1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

È quanto è emerso dal Cyber Security 360 Summit, l’evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell’università sulla situazione della cyber sicurezza in Italia.

“Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall’Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell’architettura cyber in Italia”, ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l’Associazione italiana per la sicurezza informatica.

“Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare

a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli.

Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%).

"Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli.

"Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati", ha spiegato.

In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security – circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 – appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil.

"Nello scenario attuale – ha concluso il Ceo di P4I – Partners4Innovation – è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi".

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse'

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil.

IL SANNIO QUOTIDIANO
Fondatore Luca COLASANTO
IL PRIMO QUOTIDIANO DI BENEVENTO

ADNK IP ADNK News Lavoro ADNKRONOS

Digital360: “Strategia cybersecurity sia accompagnata da adeguate risorse”

14 novembre 2017 Robot Adnkronos

Roma, 14 nov. (Labitalia) – Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell’8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione ‘militare’ e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l’Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all’1,5% della spesa Ict complessiva, appena lo 0,05% Pil.
È quanto è emerso dal Cyber Security 360 Summit, l’evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell’università sulla situazione della cyber sicurezza in Italia.
“Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall’Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell’architettura cyber in Italia”, ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l’Associazione italiana per la sicurezza informatica.
“Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati”, ha proseguito Faggioli.
Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un’offensiva grave nell’ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%).
“Se il 2016 è stato l’annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo”, ha avvertito Gabriele Faggioli.
“Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l’aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati”, ha spiegato.
In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell’ultimo anno sono saliti all’onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security – circa 1 miliardo di euro secondo la stima dell’Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 – appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil.
“Nello scenario attuale – ha concluso il Ceo di P4I – Partners4Innovation – è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l’1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un’adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi”.

OGGI in Edicola


IL SANNIO QUOTIDIANO
IL PRIMO QUOTIDIANO DI BENEVENTO
Palazzo Mosti • Refezione ancora ferma, la Giunta intanto dà via libera alla nuova gara d’appalto
Mensa, altro giro di corsa
Corsa contro il tempo per far partire il servizio, entro due settimane si punta a chiudere con la procedura negoziata
BENEVENTO
Vertenza casa: ancora tensioni, poi disgelo
L’amministrazione rivedrà delibera sugli alloggi Erp
IN CITTÀ
Vigili urbani Arriva il visore notturno
CALCIO
De Zerbi, tentazione tridente per battere il Sassuolo
In casa emiliana intanto mancherà Berardi
IERI A CAUTANO IL TAGLIO DEL NASTRO
Dopo fango e proteste, la valle vitulanese ritrova ponte Asciello
ALL’INTERNO
ESTERI
ITALIA
CAMPANIA
SANNIO
CERRETO SANNITA
Ala sinistra del Consiglio Cambiano gli equilibri
IRPINIA
MOLISE
VALLE CAUDINA
Montesarchio, Damiano firma il patto con la Boschi

← Shakira sta male: stop al tour in Europa Almaviva, da Ue 3,3 milioni per lavoratori licenziati →

INNOVATION Post
Nuove tecnologie e industria digitale

Sicurezza informatica, boom di attacchi. Ma la spesa per difendersi è ancora bassa

14 novembre 2017 Luca Zorloni

Ormai a ogni giro di boa il bilancio è sempre più allarmante. Gli attacchi informatici continuano a crescere. E nei primi sei mesi dell'anno sono aumentati dell'8,35% rispetto allo stesso periodo del 2016 e sono diventati sempre più gravi. La risposta dell'Italia è stata quella di adottare un programma di cybersecurity nazionale. "Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro Strategico Nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia" ha detto Gabriele Faggioli, amministratore delegato di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. Faggioli riconosce "un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber". "Alle parole però ora devono seguire i fatti e soprattutto gli investimenti", aggiunge: "È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati".


Gabriele Faggioli

La diagnosi

Il rapporto Clusit 2017 stima che da gennaio a giugno del 2017 siano avvenuti a livello globale 571 attacchi di dominio pubblico, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili. È il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via phishing e social engineering (+85%). Di fronte a questa minaccia le imprese italiane spendono per la sicurezza informatica poco meno di 1 miliardo di euro, pari all'1,5% della spesa ICT complessiva, appena lo 0,05% del prodotto interno lordo.

L'analisi

"Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo – avverte Faggioli –. Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati".

ItaliaOggi
IO ONLINE
Quotidiano economico, giuridico e politico

Economia, finanza e politica, gli appuntamenti della settimana

Questi gli appuntamenti economici, finanziari e politici più rilevanti della settimana:

Martedì 14 novembre

Milano 10h30 Iren presenta il Piano Industriale del Gruppo e i risultati dei 9 mesi del 2017. Presso Palazzo Mezzanotte, Piazza degli Affari 6

Cda Astaldi, Agatos, B&C, Cucinelli, Cairo, Cattolica Ass., Cembre, Class E., Cia, Conafi P., Enervit, Eukedos, El En, Fullsix, Ima, Isagro, It Way, Landi R., Marr, Mondo Tv, Nice, Prelios, Reply, Sabaf, Saes G., Ferragamo, Servizi I., Tamburi, Tecnoinvestimenti, Vittoria Ass.

Roma 09h30 ALIS (Associazione Logistica dell'Intermodalita' Sostenibile) Assemblea generale. Presso l'Auditorium Parco della Musica di Roma, Sala Santa Cecilia, Via Pietro De Coubertin 30

Milano 09h00 Hays Open Day. In Corso Italia 13 apre le sue porte a giovani e brillanti professionisti selezionati che potranno sperimentare il lavoro del recruiter e scoprire come si svolge la giornata tipo di un consulente Hays.

Rozzano (Mi) 09h30 Inaugurazione del Campus Humanitas in occasione della cerimonia di apertura dell'Anno Accademico 2017/2018 con Giuseppe Sala, Roberto Maroni e Maria Elena Boschi, Carlo Calenda. Presso il Centro Congressi Humanitas, via Manzoni 113

Roma 09h30 XII Edizione del Forum Meridiano Sanita' 2017 - 'La sanita' di oggi, la salute di domani'. Tra i relatori confermati Pierpaolo Baretta (Sottosegretario, Ministero Economia e Finanze); Stefano Bonaccini (Presidente, Conferenza Stato-Regioni e Governatore Emilia Romagna), Flori Degrassi (Presidente ANDOS); Antonio Gaudioso (Segretario Nazionale, Cittadinanzattiva); Domenico Mantoan (d.g Salute, Regione Veneto); Mario Melazzini (d.g di AIFA); Walter Ricciardi (Presidente, Istituto Superiore di Sanita'); Andrea Urbani (d.g, Programmazione Sanitaria, Ministero della Salute); Stefano Vella (Presidente, AIFA); Sergio Venturi (Assessore alla Salute, Regione Emilia Romagna). E' previsto l'intervento del Ministro della Salute Beatrice Lorenzin. Palazzo Rospigliosi, Via XXIV Maggio 43

Roma 09h30 'Cyber Security 360 Summit. La nuova cybersecurity nazionale alla prova dei fatti'. Tra i presenti Alberto Tripi, Delegato per la Cybersecurity, Confindustria; Corrado Giustozzi, Esperto di sicurezza cibernetica di Agid per il Cert della Pubblica amministrazione; Marcello Manca, VP, Gov & Industry Affairs,

Europe UL; Paolo Prinetto, Presidente Cini; Vincenza Bruno Bossio, Membro dell'Intergruppo Parlamentare Innovazione, Camera dei Deputati; Alessandra Camporota, Responsabile Innovazione Ministero; Roberta Lotti, Membro del Comitato di Governo del CERT MEFAntonio; Samaritani, Direttore, Agenzia per l'Italia Digitale; Mario Morcone, Capo di Gabinetto del Ministero dell'Interno. Centro Congressi Roma Eventi, Piazza di Spagna

Campli 09h30 Inaugurazione dei cantieri Open Fiber. Partecipa il Presidente del Consiglio dei Ministri, Paolo Gentiloni.
Piazza Vittorio Emanuele II

Milano 09h45 2nd Annual Investors' Conference on Italian & European NPLS. Organizzato da Information Management Network (IMN) con Giovanni Sabatini, d.g di Abi. Hotel Principe di Savoia, Piazza della Repubblica, 17

Roma 10h00 Save the Children e Treccani presentano l'8° edizione dell'Atlante dell'Infanzia a rischio, quest'anno dedicato al mondo della scuola. Interverranno all'evento, tra gli altri Massimo Bray, d.g dell'Istituto della Enciclopedia Italiana; Valerio Neri, d.g di Save the Children; Giorgio Alleva, Presidente Istat; Marco Rossi-Doria, in rappresentanza del Ministero dell'Istruzione; Raffaela Milano, Direttore Programmi Italia-Europa di Save the Children; Giulio Cederna, curatore dell'Atlante; Andrea Gavosto, Direttore Fondazione Agnelli. Presso la Sala Igea di Palazzo Mattei di Paganica, Piazza dell'Enciclopedia Italiana 4.

Roma 10h30 Games Industry Day. Presso l'Acquario Romano, piazza Manfredo Fanti 47

Milano 10h30 Presso la sede di Foro Buonaparte 10, l'Area Studi Mediobanca presenta alle agenzie di stampa l'indagine 2017 sulle 390 multinazionali piu' grandi del mondo, approfondendo le societa' del settore Software & Web.

Roma 11h00 Provincia di Rieti ed Edison, conferenza stampa Edilmag, start up marchigianam, con Marco Margheri, direttore Affari istituzionali e Crs di Edison (Rieti, sala consiliare della Provincia, via Salaria 3)

Roma 12h00 Aggiornamento congiunturale su 'L'economia del Lazio' Banca d'Italia, in Via XX Settembre, 97/E

Roma 12h00 Camera - Sala Mappamondo - Audizione dell'amministratore delegato di Poste Italiane SpA, Matteo Del Fante, sulle prospettive di sviluppo del gruppo nonche' sugli eventuali programmi di rimodulazione della rete degli uffici postali, anche alla luce delle disposizioni relative ai servizi postali nei piccoli comuni (Commissioni ambiente e lavori pubblici).

Milano 15h00 Conferenza stampa di presentazione del nuovo orario invernale di Trenitalia. Parteciperanno Tiziano Onesti, Presidente di Trenitalia, e Orazio Iacono, a.d e d.g di Trenitalia. Presso la Sala Reale della Stazione di Milano Centrale

Orvieto 17h00 Conferenza Stampa di presentazione del progetto di estensione del Vetrya Corporate Campus. Presso Auditorium del Vetrya Corporate, Via dell'Innovazione 1

Roma 17h00 Appuntamento nell'ambito del progetto 'Human-machine: new policies for the future of work', intervengono Giuliano Poletti e Marco Leonardi (sala Zuccari, palazzo Giustiniani)

Milano 18h00 Evento 'Milano. La citta' che sale' presso Milano Contract District in via Melloni 3. Presente Pierfrancesco Maran, assessore all'urbanistica del capoluogo lombardo.

Milano 18h30 Presentazione del progetto 'Are we fit to compete?'. Presso lo Studio Legale Nctm in via Agnello 12

Mercoledì 15 novembre

Cda Dada, Panaraiagroup

Siena 17h30 Assemblea Confindustria Toscana Sud 2017. Tra i presenti Vincenzo Boccia, presidente di Confindustria. Presso Auditorium Monte dei Paschi di Siena, viale G. Mazzini 23

Roma 09h00 SELTA Challenge 2017. Le Infrastrutture Critiche per lo Sviluppo (The Westin Excelsior Via Vittorio Veneto, 125). Con Riccardo Nencini (Viceministro delle Infrastrutture e dei Trasporti), Paola De Micheli (Sottosegretario alla Presidenza del Consiglio), Mirella Liuzzi (Movimento 5 Stelle), Guido Pier Paolo Bortoni (Presidente Autorita' dell'Energia), Stefano Liotta (Resp. Ingegneria e Innovazione ACEA), Sandro Moretti (Telecom Data Division Alperia), Corrado Giustozzi (Head of Cyber Team SELTA); Franco Bassanini Presidente Open Fiber, Deborah Bergamini (Vice presidente Commissione Trasporti e Tlc della Camera, Forza Italia), Sergio Boccadutri (Responsabile Innovazione PD), Antonio Nicita (Commissario AgCom), Luisa Franchina (AIIC-Associazione Italiana Infrastrutture Critiche), Vittorio Rosato (Resp. Infrastrutture Critiche ENEA), Alberto Tripi (Resp. Cybersecurity Confindustria).

Roma 09h00 Congresso Nazionale Confprofessioni 'Il professionista 4.0. Tema dell'edizione 2017, l'evoluzione delle competenze professionali tra normativa e mercato'. Intervengono il sottosegretario al ministero dell'Economia, Pier Paolo Baretta; il sottosegretario al ministero della Giustizia, Federica Chiavaroli; il presidente della commissione Lavoro della Camera, Cesare Damiano; il presidente della Cassa Dottori Commercialisti, Walter Anedda; il vicepresidente della commissione Lavoro del Senato, Nunzia Catalfo; Maurizio Bernardo, presidente della commissione Finanze della Camera; Cinzia Bonfrisco, commissione Finanze del Senato; Guido Guidesi, commissione Bilancio della Camera; Walter Rizzetto, vicepresidente della commissione Lavoro della Camera; Simona Vicari, commissione Bilancio del Senato; Guido Scorza del team per la trasformazione digitale della Presidenza del Consiglio dei Ministri; Ernesto Somma, capo di Gabinetto del ministro per lo Sviluppo Economico; Cosimo Accoto del MIT (Massachussets Institute of Technology); il d.g del Ceplis, Theodoros Koutroubas; Annamaria Canofani dell'Agenzia per la coesione territoriale della Presidenza del Consiglio; Daniela Labonia del dipartimento Politiche di coesione; Michele Baldi, consigliere della Regione Lazio; il presidente di Confprofessioni, Gaetano Stella. Presso l'Auditorium Antonianum, viale Manzoni 1

Milano 09h30 Presentazione 23° Rapporto Responsible Care. Paolo Lamberti, Presidente Federchimica; Massimo De Felice, Presidente INAIL; Mauro Parolini, Assessore allo Sviluppo Economico Regione Lombardia; Paolo Pirani, Segretario Generale UILTEC-UIL; Raffaello Vignali, Segretario Ufficio di Presidenza Camera dei Deputati; Cosimo Franco, Presidente Programma Responsible Care. Conclude Diana Bracco, Presidente e a.d di Bracco SpA. Presso Auditorium Federchimica, Via Giovanni da Procida 11

Milano 09h30 Belt and Road to the Chinese Market. Tra i presenti Massimiliano Guzzini, Vice President iGuzzini; Fabiana Scavolini, Direzione Commerciale e Marketing Scavolini; Umberto Simonelli, General Counsel e Segretario del CdA Brembo. Centro Congressi Fondazione Cariplo, Via Romagnosi 8

Roma 09h30 Assemblea di Palazzo Madama avvia l'esame del ddl n. 2942, di conversione in legge del decreto-legge in materia finanziaria.

Milano 10h00 Comitato Esecutivo Abi. Via Olona 2

Milano 11h00 Banca d'Italia presenta il rapporto 'L'economia della Lombardia - Aggiornamento congiunturale'. Presso la Sede della Banca, via Cordusio 5.

Roma 11h00 Automobile Club Roma, Fondazione Filippo Caracciolo di ACI e Direzione Compartimentale Area Centro Sud dell'Automobile Club d'Italia presentano i risultati dell'indagine 'Cinture allacciate e telefono in tasca: il caso Roma' sui comportamenti pericolosi piu' frequenti per la sicurezza stradale. Intervengono Giuseppina Fusco, Presidente Automobile Club Roma e Fondazione Filippo Caracciolo; Linda Meleo, Assessora alla Citta' in Movimento di Roma Capitale; Michele Civita, Assessore Politiche del territorio, Mobilita' della Regione Lazio. Grand Hotel Palace, Via Vittorio Veneto 70

Milano 11h30 Mediaset (Canale 5) presenta alla stampa 'The Wall', il nuovo game show condotto da Gerry Scotti. Presenti Gerry Scotti, Giancarlo Scheri, Direttore Canale 5; Paolo Bassetti, Presidente ed a.d di EndemolShine Italy. Presso Pala20, Studio 'The Wall', via Privata Deruta

Milano 17h00 A dieci anni dalla scomparsa di Vincenzo Maranghi lo ricordano Pellegrino Capaldo, Gianni Francini, Giorgio La Malfa, Fabrizio Palenzona. Presso Mediobanca, sala Assemblee, via Filodrammatici 3

Milano 17h45 L'Economia del futuro. Tra i presenti Valerio Camerano, a.d di A2A; Stefano Goglio, d.g per l'Italia Nespresso; Giorgio Guagliolo, Presidente Conai; Ivan Scalfarotto, Sottosegretario Ministero dello Sviluppo Economico; Sergio Solero, a.d di BMW Italia. Presso la Triennale di Milano, Salone d'Onore

Giovedì 16 novembre

Milano 09h00 Conferenza 'Financing Energy Renovation of buildings in Italy, Croazia and Slovenia' a cura della Commissione Europea, in collaborazione con il Ministero dello Sviluppo Economico, l'ENEA, l'Associazione Bancaria Italiana e l'UN Environmental Finance Initiative. c/o Centro Congressi Abi, Via Olona 2

Milano 09h00 Convegno di presentazione dei risultati della Ricerca dell'Osservatorio Innovazione Digitale nel Retail. Aula Magna Carassa Dadda, edificio BL.28, via Lambruschini 4b, campus Bovisa

Milano 09h00 Pambianco e Deutsche Bank invitano la stampa al 22° Fashion & Luxury Summit 'Il futuro della moda italiana.
Quali strategie per crescere nel mercato italiano e internazionale'. Tra i presenti raffaele Jerusalmi, Ceo di Borsa Italiana; Flavio valeri, Chief Country Officer Italy Deutcshe Bank; David Pambianco, Ceo Pambianco Strategie di Impresa; Andrea Guerra, Presidente esecutivo Eataly; Giovanni Zoppas, vice presidente esecutivo di Marcolin Group. Modera Enrico Mentana.
Palazzo Mezzanotte, Piazza degli Affari 6

Milano 09h30 Presentazione della ricerca 'I servizi immobiliari in Italia e in Europa', a cura di Scenari Immobiliari e Innovation Real Estate/Yard con Alessandro Pasquarelli, a.d di Innovation Real Estate/Yard e Mario Breglia, Presidente Scenari Immobiliari. Moderatore Andrea Cabrini di CLASS CNBC. Presso l'Hotel Principe di Savoia (Piazza della Repubblica, 17)

Roma 10h00 Confederazione dello Sport presenta il convegno 'Sport work Sport, lavoro futuro'. Piazza G.G. Belli 2

Roma 10h00 Presentazione del volume 'La nuova responsabilita' sanitaria e la sua assicurazione', interviene Maria Bianca Farina, presidente Ania (tempi di Adriano, piazza di Pietra)

Milano 11h00 Conferenza stampa 'La poverta' minorile: Milano presenta la controffensiva'. Presenti Giuseppe Guzzetti, Presidente Fondazione Cariplo; Paolo Morerio, Presidente Fondazione Vismara; Carlo Messina, Consigliere Delegato e Ceo di Intesa Sanpaolo; Giovanni Gorno Tempestini, Presidente Fondazione Fiera Milano; Pierfrancesco Majorino, Assessore Politiche Sociali, Salute e Diritti del Comune di Milano. Presso la Sala Tiepolo, Fondazione Cariplo, via Manin 23

Roma 14h00 Audizione Abi - Indagine impatto tecnologia con Giovanni Sabatini, d.g di Abi. Camera dei Deputati, Commissione Finanze

Roma 17h00 'La nuova via della seta cinese. Opportunita' per il sistema Italia. Tra i presenti Riccardo Monti, Presidente di Italferr; Edward Chen, Ceo Huawei Italia. Conclusioni di Ivan Scalfarotto, sottosegretario Ministero dello sviluppo economico. Presso NCTM Studio legale, Sala delle Conferenze, Via delle Quattro Fontane 161

Venerdì 17 novembre

Roma Tavolo su Roma Calenda Raggi

Pero (Mi) 09h30 Al via il Forum delle eccellenze, il piu' grande evento formativo in Italia dedicato ai temi del management e della leadership. Presso Atahotel Expo Fiera di Milano, via Keplero 12. Termina domani

Milano 11h30 Presentazione della seconda ricerca dell'Osservatorio Birra 'Famiglie e Birra. La spina dorsale dei consumi fuori casa in Italia'. Tra i presenti Soren Hagh, a.d di Heineken Italia; Alfredo Pratolongo, presidente Fondazione Birra Moretti; Alessandro Marangoni, a.d di Althesys. Presso Palazzo Bovara, Sala Aquile, corso Venezia 51

Milano 11h30 Conferenza stampa 'Le ragioni giuridiche e scientifiche contro l'obbligo vaccinale. Informazione, reazioni avverse, Costituzione'. Presso Palazzo Giurenconsulti, piazza Mercati 2

Roma 12h00 'Fare impresa al Sud', interviene Vincenzo Boccia (Festival 'Economia come', auditorium Parco

della Musica, teatro studio Borgna)

Milano 16h00 Bookcity Milano 2017 per parlare di politica internazionale attraverso 18 incontri, con oltre 50 relatori italiani e internazionali e il coinvolgimento di 16 case editrici. Palazzo Clerici, via Clerici 5

Roma 16h00 'La rinascita dei territori', interviene Graziano Delrio (Festival 'Economia Come', auditorium Parco della Musica, teatro studio Borgna)

Roma 18h00 'Le banche: termometro della ripresa', interviene Carlo Messina (Festival 'Economia Come', auditorium Parco della musica, teatro studio Borgna)

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell’8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil. È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia. “Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall’Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia”, ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. “Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati”, ha proseguito Faggioli. Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad

oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell’ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%). “Se il 2016 è stato l’annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli."Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati”, ha spiegato. In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil. “Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi”.

Sassari Notizie

DATI

Digital360: "Strategia cybersecurity sia accompagnata da adeguate risorse"

14/11/2017 14:08

Roma, 14 nov. (Labitalia) - Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil. È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia. "Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia", ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. "Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli. Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%). "Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli."Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati", ha spiegato. In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security - circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 - appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil. "Nello scenario attuale - ha concluso il Ceo di P4I - Partners4Innovation - è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi".

SICILIAINFORMAZIONI.COM
Looking Far, Looking Deep

Cybersecurity: Digital360, strategia sia accompagnata da adeguate risorse

Il primo semestre 2017 è stato il peggiore di sempre per gli attacchi informatici, che sono cresciuti dell'8,35% a livello globale e che risultano sempre più dannosi. Ormai vengono compiuti con precisione 'militare' e strategie diverse a seconda del settore, e nessuna organizzazione può dirsi completamente immune. Di fronte a minacce crescenti, l'Italia si è finalmente dotata di una strategia per la cybersecurity nazionale, che ora affronta la prova dei fatti, ma che per essere realmente efficace deve essere accompagnata da adeguate risorse economiche. Intanto, le imprese investono ancora troppo poco in sicurezza informatica, poco meno di 1 miliardo di euro, pari all'1,5% della spesa Ict complessiva, appena lo 0,05% Pil. È quanto è emerso dal Cyber Security 360 Summit, l'evento organizzato oggi a Roma dal Gruppo Digital360, che ha messo a confronto rappresentanti delle istituzioni, delle imprese e dell'università sulla situazione della cyber sicurezza in Italia. "Il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, adottato dall'Italia secondo gli indirizzi individuati dal Quadro strategico nazionale, ha un obiettivo ambizioso: stimolare un ulteriore sviluppo dell'architettura cyber in Italia", ha detto Gabriele Faggioli, Ceo di P4I-Partners4Innovation, società di advisory e coaching del Gruppo Digital360, e presidente del Clusit, l'Associazione italiana per la sicurezza informatica. "Un fatto positivo: protezione cibernetica e sicurezza informatica nazionali devono essere un

processo che coinvolge tutti gli attori interessati a vario titolo alla tematica cyber. Alle parole però ora devono seguire i fatti e soprattutto gli investimenti. È importante vedere quali risorse saranno messe in campo per poter trasformare piani e linee guida in interventi reali a tutti i livelli. A fronte di un sicuro aumento degli attacchi, bisogna puntare a conseguire nei prossimi anni una diminuzione di quelli riusciti e dei danni arrecati", ha proseguito Faggioli. Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi. Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware, +86% rispetto al secondo semestre 2016, ma crescono anche gli attacchi via Phishing e Social Engineering (+85%). "Se il 2016 è stato l'annus horribilis della sicurezza cyber, nel 2017 la situazione è persino peggiorata: oggi in Italia, come nel mondo, qualsiasi organizzazione è concretamente a rischio di un attacco informatico significativo", ha avvertito Gabriele Faggioli. "Preoccupa la crescita delle minacce verso gli smartphone, un oggetto ormai posseduto da tutti spesso senza adeguati sistemi di protezione, e in generale la crescente esposizione degli utenti a social, cloud o Internet of Things, senza le necessarie misure di sicurezza. Mentre è in crescita l'aggressività degli attaccanti e sul mercato nero si diffondono strumenti di attacco sempre più sofisticati", ha spiegato. In Italia, per quanto il numero di attacchi gravi di dominio pubblico sia basso rispetto al totale, nell'ultimo anno sono saliti all'onore delle cronache alcuni casi eccellenti. Ma gli investimenti in Ict Security – circa 1 miliardo di euro secondo la stima dell'Osservatorio Information Security & Privacy del Politecnico di Milano nel 2016 – appaiono insufficienti se rapportati al valore complessivo del mercato di beni e servizi Ict, pari a 66 miliardi di euro, e al totale del Pil. "Nello scenario attuale – ha concluso il Ceo di P4I – Partners4Innovation – è importante che tutti gli attori siano adeguatamente sensibilizzati al tema della sicurezza informatica. Le aziende devono fare la loro parte, con adeguati investimenti: una spesa per Information Security pari ad appena l'1,5% della spesa Ict complessiva, circa lo 0,05% del Pil, è davvero troppo poco. È importante però che si diffonda nella popolazione un'adeguata cultura della sicurezza, perché a volte bastano semplici accorgimenti per scongiurare gli attacchi".

GIORNALE 24 NEWS .IT

Anonymous: rubati dati istituzioni italiane ed europee

PUBBLICATO DA ETTORE SPOSARO 15 NOVEMBRE 2017

“Cittadini, siamo lieti di annunciarvi, per il diritto della democrazia e della dignità dei popoli”, così inizia il **leak di Anonymous**, “che siamo in possesso di una lista di dati personali relativi al ministero dell’Interno, al ministero della Difesa, alla Marina Militare nonché di Palazzo Chigi e Parlamento Europeo.”

Gli anonimi mascherati hanno sottratto centinaia di file riguardati **dati personali**, per lo più appartenenti a forze dell’ordine: dichiarazione dei redditi, buste paga, patenti, numeri di telefono, curriculum, attività della Digos e targhe delle vetture di servizio.

L’hacking ha riguardato anche informazioni sulla visita di oggi del premier **Paolo Gentiloni** a Bologna, in occasione dell’inaugurazione del parco agroalimentare Fico di Eataly World. Il furto riguarderebbe scambi di mail tra Palazzo Chigi e la polizia incaricata del sopralluogo precedente.

Gli Anonymous hanno dichiarato sul loro blog di essere riusciti a sottrarre le informazioni sensibili a ministeri, istituzioni nazionali e dell’UE, corpi dello Stato “per il diritto della democrazia e della dignità dei popoli”. Dichiarazioni che lasciano molti interrogativi sulla **sicurezza informatica** del Sistema Italia, che sembra fare acqua da tutte le parti, e paradossalmente proprio nel giorno in cui a Roma si è tenuto il 360 cybersecurity Summit dedicato proprio a questo tema.

La Polizia Postale ha però diffuso un comunicato secondo cui “al momento non sono state evidenziate ulteriori compromissioni di sistemi informatici istituzionali”: si tratterebbe, secondo quanto dichiarato dal Corpo, di un attacco alle caselle di

posta elettronica personali di un dipendente del Ministero della Difesa e di un poliziotto.

È tuttavia tornato alla ribalta il gruppo Anonymous italiano, dopo un lungo periodo di silenzio dopo l'arresto di alcuni attivisti; ricordiamo infatti che gli ultimi attacchi si erano avuti durante il periodo dell'Expo di Milano, quando gli hacker avevano bloccato la biglietteria, e nei confronti del sito dedicato al Family Day, chiuso anch'esso.