CYBERSECURITY - PIANETTA (ANCI PIEMONTE): "IMPEGNO SU UN TEMA CHE DEVE RAPPRESENTARE INCENTIVO A INNOVAZIONE"

[04-04-2017]

Il 2016 è stato l'anno peggiore di sempre in termini di cybersecurity: 1.050 gli incidenti noti classificati come gravi a livello globale, con impatto significativo per le vittime in termini di danno economico, reputazione e diffusione di dati sensibili. Notevole l'incremento degli attacchi gravi compiuti per finalità di Cybercrime (+9,8%), mentre crescono a tre cifre quelli riferibili ad attività di Cyber Warfare, la "guerra delle informazioni" (+117%). In termini assoluti, Cybercrime e Cyber Warfare fanno registrare il numero di attacchi più elevato degli ultimi sei anni.
Questi i dati illustrati oggi a Roma durante il convegno "Cybersecurity: il lato oscuro del digitale" organizzato dal Csi Piemonte e Clusit (Associazione italiana per la sicurezza informatica), con il patrocinio di Anci Piemonte. È un dato di fatto che le Pubbliche amministrazioni, stiano invece sempre più diventando bersaglio di attacchi cibernetici, sempre più articolati ed evoluti. Da qui l'idea del Csi Piemonte di organizzare un incontro per promuovere una collaborazione forte tra organizzazioni pubbliche e private. Per il Csi il tema della Digital Security è di straordinaria importanza: nel 2016 sono state sostenute ondate di tentativi di attacchi, con picchi che in alcune occasioni hanno anche superato la soglia dei 150.000 al giorno verso i servizi web per la Pa, contrastati efficacemente grazie a sistemi tecnologici di protezione e azioni sinergiche di collaborazione con gli enti.
"Eppure - spiega Michele Pianetta, vice presidente di Anci Piemonte con delega all'innovazione, intervenuto al convegno del Csi - gli studi dicono che il tema della cybersecurity non viene purtroppo considerato centrale dalla Pubblica Amministrazione; per questa ragione, ci stiamo impegnando affinché le cose cambino e dibattiti come questo contribuiscono a fare informazione su un tema che non deve rappresentare un ostacolo, bensì un incentivo all'innovazione".
Ma quali sono le tecniche di attacco più diffuse a livello globale? Phishing e social engineering (+ 1166%), ovvero attacchi mirati a "colpire la mente" delle vittime, inducendole a fare passi falsi che poi rendono possibile l'attacco informatico vero e proprio. Ma anche il "malware" comune - tra cui vi sono i cosiddetti "ransomware" – non più solo per compiere attacchi di piccola entità, ma anche contro bersagli importanti e con impatti significativi. In aumento anche gli attacchi compiuti con DDoS (+13%) e l'utilizzo di vulnerabilità "0-day". A livello globale la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") rappresenta il 56% del totale: questo dato è uno dei più allarmanti, secondo gli esperti del Clusit, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui e bassi costi. Se il rischio cyber quindi non può essere annullato, le armi per combatterlo non sono solo tecnologiche: il primo passo è la consapevolezza delle persone, che devono adottare comportamenti adeguati in materia di sicurezza informatica. (com/fdm)

anci.it Redazione ASSOCIAZIONE NAZIONALE COMUNI ITALIANI
ANCI - Associazione Nazionale Comuni Italiani
Contatti: Tel. 06680091 - Fax 0668009202
Gestione tecnica a cura di ancitel La rete dei Comuni Italiani

Versione grafica Cambia
Quaderni ANCI Manuali tecnici per gli amministratori
ANCI MULTIMEDIA FOTO VIDEO
SERVIZI ANCI
CONVEGNI E SEMINARI
ASSEMBLEE ANCI
ANCI RIVISTA
GAZZETTA UFFICIALE
LAVORI PARLAMENTARI
DOSSIER E RICERCHE
CONVENZIONI
PROTOCOLLI D'INTESA
SITI TEMATICI
Piccoli Comuni
Unioni di Comuni
Consigli Comunali
Richiedenti Asilo e Rifugiati
Permessi di soggiorno
Anticontraffazione
Prima Infanzia
Osservatorio Smart City
Patrimonio immobiliare
Festa dei vicini
Protezione Civile
Retribuzioni apicali Anci
Opendata Anci
STATISTICHE ACCESSI
RASSEGNA STAMPA
ACCESSO HELP DESK SPRAR
TERREMOTO CENTRO ITALIA
QUOTE ASSOCIATIVE 2017

CYBER SECURITY Martedì 4 aprile 2017 - 13:16

Cyber attacchi, Csi Piemonte: in Italia rischio sottostimato

I dati illustrati in un evento organizzato a Roma con Clusit

Roma, 4 apr. (askanews) – Il 2016 è stato l'anno peggiore di sempre in termini di cyber security: 1.050 gli incidenti noti classificati come gravi a livello globale, con impatto significativo per le vittime in termini di danno economico, reputazione e diffusione di dati sensibili. Notevole l'incremento degli attacchi gravi compiuti per finalità di cybercrime (+9,8%), mentre crescono a tre cifre quelli riferibili ad attività di Cyber Warfare, la 'guerra delle informazioni' (+117%). In termini assoluti Cybercrime e Cyber Warfare fanno registrare il numero di attacchi più elevato degli ultimi 6 anni. Questi sono alcuni dei dati illustrati oggi a Roma durante il convegno 'Cybersecurity: il lato oscuro del digitale' organizzato dal Csi Piemonte e Clusit, l'Associazione Italiana per la Sicurezza Informatica che ogni anno fornisce un rapporto sul quadro della situazione globale della sicurezza informatica.

Per gli organizzatori del convegno, "la vulnerabilità dei sistemi informatici è oggi riconosciuta a livello globale. Cittadini, aziende e governi subiscono attacchi sempre più frequenti e difficili da contrastare. E questo inasprimento vale anche e soprattutto per la Pubblica Amministrazione". Ciò "è dovuto ad un fenomeno", si legge nel rapporto Clusit 2017, "relativamente recente, di mutamento della prospettiva nel riguardo della appetibilità delle PA da parte di organizzazioni o anche singoli individui portatori di interessi illeciti. È un dato di fatto", spiega una nota, "che le Pubbliche Amministrazioni, stiano invece sempre più diventando bersaglio di attacchi cibernetici, sempre più articolati ed evoluti".

"Il CSI Piemonte ha organizzato questo incontro – ha sottolineato Riccardo Rossotto, presidente del Csi Piemonte – per promuovere una collaborazione forte tra organizzazioni pubbliche e private, in linea con i provvedimenti del Governo a livello nazionale, e contribuire alla salvaguardia dei nostri dati. Nel nostro Paese il tema è ancora sottostimato. Permane

una forma di ‘altruismo’ legata ad una lettura miope e pericolosa del rischio: ho letto che succede ma non a me… agli altri. Bisogna combattere questo tipo di approccio con una politica di formazione e prevenzione che aiuti tutti i comparti imprenditoriali e professionali a dare il giusto peso ad una minaccia gravissima che incombe sulla nostra sicurezza pubblica e privata. Per il Csi il tema della Digital Security è da tempo pervasivo rispetto alle attività che esso svolge per i suoi 129 Enti Consorziati piemontesi, nella protezione quotidiana dei servizi affidati. Anche per il Consorzio il 2016 è stato un anno impegnativo sotto questo profilo: sono state sostenute ondate di tentativi di attacchi, con picchi che in alcune occasioni hanno anche superato la soglia dei 150mila al giorno verso i servizi web per la PA, contrastati efficacemente grazie a sistemi tecnologici di protezione e azioni sinergiche di collaborazione con gli enti”.

Ma quali sono le tecniche di attacco più diffuse a llivello globale? Phishing e social engineering (+ 1166%), ovvero attacchi mirati a ‘colpire la mente’ delle vittime, inducendole a fare passi falsi che poi rendono possibile l’attacco informatico vero e proprio. Ma anche il “Malware” comune – tra cui vi sono i cosiddetti “Ransomware” – non più solo per compiere attacchi di piccola entità, ma anche contro bersagli importanti e con impatti significativi. In aumento anche gli attacchi compiuti con DDoS (+13%) e l’utilizzo di vulnerabilità “0-day”. A livello globale la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, phishing, malware “semplice”) rappresenta il 56% del totale: questo dato è uno dei più allarmanti, secondo gli esperti del Clusit, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui e bassi costi.

“Il 2016 è stato l’anno peggiore in termini di attacchi – ha dichiarato Gabriele Faggioli, presidente di Clusit – e questo paradossalmente ha comportato un innalzamento di attenzione sul tema. L’augurio è che questa attenzione unita alle normative che arriveranno nel 2018 permetta di affrontare il tema in termini maturi”.

COR.COM
IL QUOTIDIANO ON LINE DELL'ECONOMIA DIGITALE E DELL'INNOVAZIONE

Giovedì 06 Aprile 2017
Direttore Responsabile: Gildo Campesato
Condirettore: Mila Fiordalisi

I L R E P O R T

Cybersecurity, esplode la guerra delle info: "warfare" nuova frontiera degli hacker

Secondo il report Clusit-Csi Piemonte questo tipo di attività malevole sono cresciute del 117%. Cybercrime a +9,8%. Gabriele Faggioli: "Mai registrati finora tanti attacchi. Bisogna affrontare il tema in termini maturi"

Il 2016 è stato l'anno nero della cybersecurity, quello in cui si è registrato il più alto numero di attacchi su scala globale. Basti pensare che sono stati **1.050 gli incidenti noti classificati come gravi**, che hanno avuto un impatto significativo per le vittime in termini di danno economico, reputazione e diffusione di dati sensibili. E se da una parte è stata notevole la crescita degli attacchi gravi compiuti per finalità di **Cybercrime (+9,8%)**, salta agli occhi il fatto che quelli riferibili ad attività di **Cyber Warfare,** la "guerra delle informazioni", sono cresciuti a tre cifre, segnando un **+117%**. I dati sono stati illustrati Da **Csi Piemonte** e **Clusit** (l'associazione italiana per la sicurezza informatica che ogni anno fornisce il quadro della situazione globale della sicurezza informatica) durante il convegno **"Cybersecurity: il lato oscuro del digitale**".

"Il 2016 è stato l'anno peggiore in termini di attacchi - afferma **Gabriele Faggioli**, **Presidente di Clusit** - e questo paradossalmente ha comportato un innalzamento di attenzione sul tema. L'augurio è che questa attenzione unita alle normative che arriveranno nel 2018 permetta di affrontare il tema in termini maturi".

"Il CSI Piemonte ha organizzato questo incontro - ha sottolinea **Riccardo Rossotto**, **Presidente del CSI Piemonte** - per promuovere una collaborazione forte tra organizzazioni pubbliche e private, in linea con i provvedimenti del Governo a livello nazionale, e contribuire alla salvaguardia dei nostri dati. Nel nostro Paese il tema è ancora sottostimato. Permane una forma di 'altruismo' legata a una lettura miope e pericolosa del rischio: 'ho letto che succede ma non a me...agli altri'. Bisogna combattere questo tipo di approccio con una politica di formazione e prevenzione che aiuti tutti i comparti imprenditoriali e professionali a dare il giusto peso ad una minaccia gravissima che incombe sulla nostra sicurezza pubblica e privata. Per il **Csi** il tema della **Digital Security** è da tempo pervasivo rispetto alle attività che esso svolge per i suoi 129 Enti Consorziati piemontesi, nella protezione quotidiana dei servizi affidati. Anche per il Consorzio il 2016 è stato un

anno impegnativo sotto questo profilo: sono state sostenute ondate di tentativi di attacchi, con picchi che in alcune occasioni hanno anche superato la soglia dei 150.000 al giorno verso i servizi web per la PA, contrastati efficacemente grazie a sistemi tecnologici di protezione e azioni sinergiche di collaborazione con gli enti".

Ma quali sono le tecniche di attacco più diffuse a livello globale? **Phishing e social engineering** (+ 1166%), ovvero attacchi mirati a "colpire la mente" delle vittime, inducendole a fare passi falsi che poi rendono possibile l'attacco informatico vero e proprio. Ma anche il "**Malware**" comune - tra cui vi sono i cosiddetti "**Ransomware**" – non più solo per compiere attacchi di piccola entità, ma anche contro bersagli importanti e con impatti significativi.

In aumento anche gli attacchi compiuti con DDoS (+13%) e l'utilizzo di vulnerabilità "0-day". A livello globale **la somma delle tecniche di attacco più banali** (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") **rappresenta il 56% del totale**: questo dato è uno dei più allarmanti, secondo gli esperti del **Clusit**, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui e bassi costi.

Se il rischio cyber quindi non può essere annullato, le armi per combatterlo non sono solo tecnologiche: il primo passo è la consapevolezza delle persone, che devono adottare comportamenti adeguati per seguire le policy aziendali. "La sicurezza informatica è un problema di tutti, e come tutti i problemi deve essere affrontato al di là degli aspetti tecnici e degli specifici adempimenti normativi, lavorando molto sugli aspetti formativi, in modo da favorire una mentalità diffusa di attenzione per le problematiche di sicurezza ICT" conclude **Giulio Lughi, Presidente CTS del CSI Piemonte.** La questione non è più se si verrà attaccati, ma quando, e in quel momento occorrerà farsi trovare pronti.

04 Aprile 2017

TAG: Csi Piemonte, Clusit, Cybersecurity, Cyber warfare, Cybercrime, Giulio Longhi, Riccardo Rossotto, Gabriele Faggioli

ARTICOLI CORRELATI

L'AL

Csi-Piemonte, mancano all'appello 8 milioni. Torino corre ai ripari

LA SPERIME

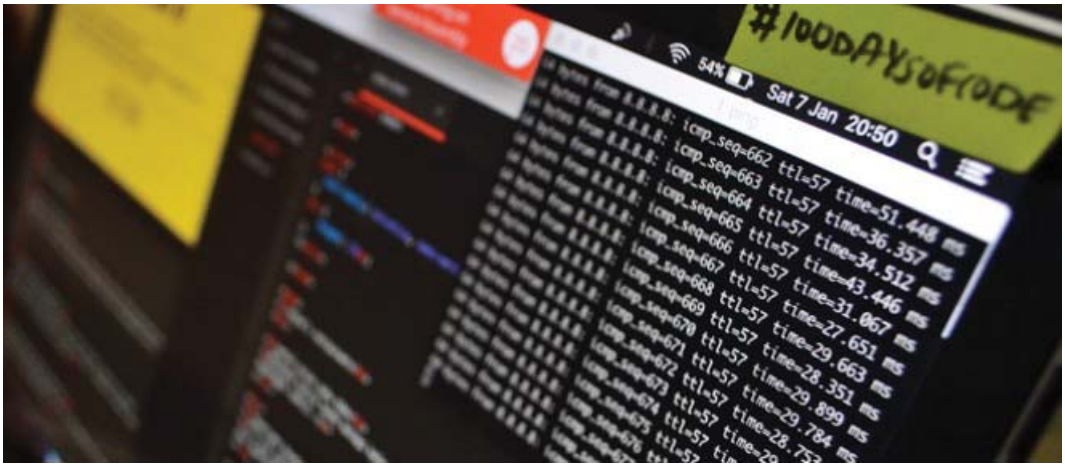
Buste paga online, dal Garante Privacy ok alla biometria

LO STUD

PA nuovo bersaglio degli hacker, in aumento gli attacchi-spia

LA RICE

Piemonte: cresce il cloud, ma le Pmi sono ancora "pigre"



NEWS

CYBERSECURITY: IL LATO OSCURO DEL DIGITALE

A firma di Antonio Lioy, Politecnico di Torino, Angelo Saccà, Università di Torino e Francesca Bosco, Unicri

"Il 2016 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce *cyber* e del relativo impatto". Questa frase, ritrovata su diversi quotidiani, sintetizza in poche parole lo stato dell'arte sulla sicurezza informatica emergente dagli ultimi dati del rapporto Clusit. Termini come Ransonware, DDOS, Phishing, 0-day fino a qualche anno fa relegati alle competenze di una ristretta cerchia di esperti, rappresentano oramai problematiche quotidiane che coinvolgono tutti i cittadini, siano essi professionisti, imprenditori o dipendenti di aziende private e pubbliche, o semplici studenti.

"La sicurezza informatica è divenuta un problema di tutti, e come tutti i problemi" – riprendendo un'intervista al **Prof. Giulio Lughi, Presidente del Comitato Tecnico Scientifico del CSI Piemonte** – "deve essere affrontato al di là degli aspetti tecnici e degli specifici adempimenti normativi lavorando molto sugli aspetti formativi, in modo da favorire una mentalità diffusa di attenzione per le problematiche di sicurezza ICT". Non basta definire processi e tecnologie, sono decisive la "cultura" della sicurezza informatica e la "consapevolezza" del rischio e delle modalità per affrontarlo, in modo tale da formare un senso critico più oggettivo per valutare comportamenti, tecnologie e situazioni in un mondo che cambia sempre più velocemente

È proprio dal Piemonte che partono forti segnali rivolti al governo nazionale di voler partecipare come parte attiva nella protezione dei dati dei cittadini attraverso un'attività importante di sensibilizzazione e cultura al fine di maturare una maggior consapevolezza e condivisione su questi temi. **Per il CSI Piemonte il tema della Digital Security è da tempo pervasivo rispetto alle attività che svolge per i suoi 125 Enti Consorziati piemontesi, nella protezione quotidiana dei servizi affidati.**

Anche il **Politecnico di Torino** è impegnato su questo tema. Recentemente ha rinnovato accordi di collaborazione con il Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri e con la CONSOB, anche su aspetti di cybersecurity". Il Politecnico inoltre è stato Coordinatore del progetto europeo SECURED, che ha introdotto un cambiamento sostanziale nel modo di concepire la sicurezza informatica, proponendo un unico elemento in grado di proteggere contemporaneamente diversi dispositivi informatici, anche in mobilità. Il progetto prosegue in un nuovo progetto europeo del programma H2020, denominato SHIELD.

L'**Università di Torino** invece opera in un contesto che sul piano culturale prevede apertura, partecipazione, condivisione fra l'altro in contesti disciplinari molto eterogenei, tipico delle università "generaliste". Ciò che in azienda potrebbe essere considerato un comportamento sospetto in Ateneo potrebbe essere attività di ricerca scientifica in corso. La consapevolezza dei rischi e se vogliamo anche la prevenzione in materia di sicurezza informatica passa anche dalla capacità di tracciare ed identificare gli accessi ai servizi. L'Università di Torino ha ormai da diversi anni effettuato importanti investimenti, non solo tecnici ma anche sotto il profilo di gestione ed organizzativo, sul tema dell'*Identita Digitale.* Dal processo di "rilascio dell'identità digitale", alla gestione dei servizi che

ormai in modo massiccio ne implementano i criteri di autenticazione ed autorizzazione. Ha implementato soluzione di Identità digitale federate (IDEM), basate sul mutuo riconoscimento degli utenti da parte degli enti che aderiscono alla federazione; presupposto di un approccio di responsabilità distribuita ma secondo standard e logiche di inclusione. Un approccio sul digitale che richiama nel contesto "fisico" le sfide ancora irrisolte (i confini, la circolazione di persone e beni, il riconoscimento delle identità, l'accesso ai servizi). L'identità digitale come antidoto rispetto ad alcuni rischi dell'anonimato apre ulteriori sfide, la privacy. La ricerca non del migliore equilibrio ma del nuovo equilibrio che ogni nuova tecnologia impone in alternativa all'obsolescenza (tecnica ed in alcune circostanze anche gestionale) è il contesto in cui si sviluppano molte azioni di Cybersecurity dell'Università di Torino. L'implementazione del sistema pubblico di identità digitale (SPID) pongono l'ateneo sulla frontiera dell'innovazione con gli stimoli di una community universitaria molto dinamica e vivace anche rispetto alle soluzioni per l'accesso ai servizi online.

A Torino ha anche sede **l'Istituto Interregionale delle Nazioni Unite per la Ricerca sul Crimine e la Giustizia (UNICRI**) che si occupa da anni dei rischi associati alle nuove tecnologie e in particolare del loro uso improprio per fini criminali e terroristici. L'UNICRI nel corso degli anni ha svolto un costante lavoro di monitoraggio dell'evoluzione di tali rischi e collaborato con organizzazioni regionali e internazionali per lo sviluppo di azioni di contrasto e prevenzione. Il lavoro dell'Istituto si è inizialmente focalizzato sui crimini informatici per giungere a un più ampio programma sulla sicurezza informatica che coinvolge attori privati e pubblici. Attualmente il programma si è esteso a tutte le minacce collegate alla sicurezza informatica (con particolare attenzione ai rischi per le infrastrutture critiche e per la supply chain), e si è altresì concentrato sulle possibilità che le tecnologie (ad esempio big data analytics) offrono ai paesi per il miglioramento della sicurezza.

Il governo nazionale ha certamente intrapreso a partire dal 2013 alcune valide iniziative per rafforzare le difese cyber, dal "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*", al "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*" e le organizzazioni nazionali come AgID, che istituzionalmente hanno un ruolo di primo piano nella gestione della sicurezza informatica della pubblica amministrazione italiana, hanno profuso notevoli energie ed effettuato significativi investimenti per innalzare il livello di sicurezza cibernetica della PA e, di riflesso, dell'intera nazione. E l'attuazione del Piano Triennale porterà probabilmente ulteriori azioni di miglioramento della sicurezza.

Tuttavia è oramai consapevolezza diffusa e certa che il rischio della criminalità informatica "*questo lato oscuro del digitale*", non possa essere annullato, ma purtroppo solo contrastato e mitigato, con molteplici e continue energie investite, con la collaborazione di tutti gli attori.

CIS-Sapienza ed il Laboratorio Nazionale di Cyber Security, in collaborazione con diverse organizzazioni pubbliche e private, hanno realizzato un *Framework Nazionale per la Cyber Security* con lo scopo di offrire alle organizzazioni un approccio omogeneo per affrontare la cyber security, al fine di ridurre il rischio legato alla minaccia cyber.

E il **workshop *Cybersecurity: il lato oscuro del digitale* promosso dal Comitato Tecnico Scientifico del CSI Piemonte in collaborazione con il CLUSIT**, **che si terrà a Roma il prossimo 4 aprile**, vuole proprio essere un'occasione, attraverso le testimonianze e le indicazioni di importanti rappresentanti del mondo politico, accademico, governative e aziende esperte del settore per delineare un quadro di prospettive strategiche locali e nazionali atte a fronteggiare efficacemente il crescente livello delle minacce informatiche.

Programma e iscrizioni su: https://roma_cts2017.eventbrite.it/

CSI Piemonte | Cybersecurity | identità digitale

ALTRE NEWS

6 APRILE 2017 – GIORNATA INTERNAZIONALE ONU DELLO SPORT PER LO SVILUPPO E PER LA PACE

Si è svolta oggi alle 10.30 a Roma, nella prestigiosa sede della SIOI a Palazzetto Venezia, la Celebrazione della Giornata Internazionale delle Nazioni Unite dello Sport per lo Sviluppo e per la Pace.

SEMINARIO SUI MECCANISMI DI MONITORAGGIO E DENUNCIA DEI CRIMINI E DISCORSI D'ODIO ONLINE – LA APP DEL PROGETTO EMORE

Monitorare e combattere i discorsi d'odio online in un'ottica di sinergia: questo è il tema dell'iniziativa che si terrà il 29 marzo 2017 a Roma alle ore 16, presso la

Roma | 04-04-2017

Cyber security

Cyber attacchi, Csi Piemonte: in Italia rischio sottostimato

I dati illustrati in un evento organizzato a Roma con Clusit

Roma, 4 apr. (askanews) - Il 2016 è stato l'anno peggiore di sempre in termini di cyber security: 1.050 gli incidenti noti classificati come gravi a livello globale, con impatto significativo per le vittime in termini di danno economico, reputazione e diffusione di dati sensibili. Notevole l'incremento degli attacchi gravi compiuti per finalità di cybercrime (+9,8%), mentre crescono a tre cifre quelli riferibili ad attività di Cyber Warfare, la 'guerra delle informazioni' (+117%). In termini assoluti Cybercrime e Cyber Warfare fanno registrare il numero di attacchi più elevato degli ultimi 6 anni. Questi sono alcuni dei dati illustrati oggi a Roma durante il convegno 'Cybersecurity: il lato oscuro del digitale' organizzato dal Csi Piemonte e Clusit, l'Associazione Italiana per la Sicurezza Informatica che ogni anno fornisce un rapporto sul quadro della situazione globale della sicurezza informatica.
Per gli organizzatori del convegno, "la vulnerabilità dei sistemi informatici è oggi riconosciuta a livello globale. Cittadini, aziende e governi subiscono attacchi sempre più frequenti e difficili da contrastare. E questo inasprimento vale anche e soprattutto per la Pubblica Amministrazione". Ciò "è dovuto ad un fenomeno", si legge nel rapporto Clusit 2017, "relativamente recente, di mutamento della prospettiva nel riguardo della appetibilità delle PA da parte di organizzazioni o anche singoli individui portatori di interessi illeciti. È un dato di fatto", spiega una nota, "che le Pubbliche Amministrazioni, stiano invece sempre più diventando bersaglio di attacchi cibernetici, sempre più articolati ed evoluti".
"Il CSI Piemonte ha organizzato questo incontro - ha sottolineato Riccardo Rossotto, presidente del Csi Piemonte - per promuovere una collaborazione forte tra organizzazioni pubbliche e private, in linea con i provvedimenti del Governo a livello nazionale, e contribuire alla salvaguardia dei nostri dati. Nel nostro Paese il tema è ancora sottostimato. Permane una forma di 'altruismo' legata ad una lettura miope e pericolosa del rischio: ho letto che succede ma non a me... agli altri. Bisogna combattere questo tipo di approccio con una politica di formazione e prevenzione che aiuti tutti i comparti imprenditoriali e professionali a dare il giusto peso ad una minaccia gravissima che incombe sulla nostra sicurezza pubblica e privata. Per il Csi il tema della Digital Security è da tempo pervasivo rispetto alle attività che esso svolge per i suoi 129 Enti Consorziati piemontesi, nella protezione quotidiana dei servizi affidati. Anche per il Consorzio il 2016 è stato un anno impegnativo sotto questo profilo: sono state sostenute ondate di tentativi di attacchi, con picchi che in alcune occasioni hanno anche superato la soglia dei 150mila al giorno verso i servizi web per la PA, contrastati efficacemente grazie a sistemi tecnologici di protezione e azioni sinergiche di collaborazione con gli enti".
Ma quali sono le tecniche di attacco più diffuse a llivello globale? Phishing e social engineering (+ 1166%), ovvero attacchi mirati a 'colpire la mente' delle vittime, inducendole a fare passi falsi che poi rendono possibile l'attacco informatico vero e proprio. Ma anche il "Malware" comune - tra cui vi sono i cosiddetti "Ransomware" - non più solo per compiere attacchi di piccola entità, ma anche contro bersagli importanti e con impatti significativi. In aumento anche gli attacchi compiuti con DDoS (+13%) e l'utilizzo di vulnerabilità "0-day". A livello globale la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, phishing, malware "semplice") rappresenta il 56% del totale: questo dato è uno dei più allarmanti, secondo gli esperti del Clusit, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui e bassi costi.

"Il 2016 è stato l'anno peggiore in termini di attacchi - ha dichiarato Gabriele Faggioli, presidente di Clusit - e questo paradossalmente ha comportato un innalzamento di attenzione sul tema. L'augurio è che questa attenzione unita alle normative che arriveranno nel 2018 permetta di affrontare il tema in termini maturi".

askanews

ULTIM'ORA

16:30 L.elettorale,Renzi al Pd:...

16:30 Fmi, da scenari bassa crescita...