CLUSIT:
“Prepararsi all’impatto”.
Cyber crimine in crescita del 30% nei primi sei mesi del 2015.

Presentata oggi al Security Summit di Verona l’ottava edizione del Rapporto CLUSIT: incremento a tre cifre degli attacchi alle infrastrutture critiche, al settore Automotive, GDO, Telecomunicazioni e Informazione-Entertainment.

Tra le cause, l’industrializzazione degli attacchi e la loro automazione, a fronte di una mancata gestione del rischio, secondo gli esperti dell’Associazione Italiana per la Sicurezza Informatica.

Ottobre è il mese europeo dedicato alla sicurezza informatica (European Cyber Security Month -ECSM), campagna UE volta a promuovere la consapevolezza dei rischi informatici

#securitysummit #rapportoclusit #CyberSecMonth

Milano, 1° ottobre 2015 – Da “rischio teorico” a “certezza nel medio-breve termine”: vulnerabilità ormai endemiche a livello globale espongono oggi in maniera crescente cittadini, aziende, istituzioni e governi agli attacchi, più velocemente della capacità complessiva di attivare una protezione.

Questa la premessa alla presentazione dell’ottava edizione del Rapporto CLUSIT sulla sicurezza informatica in Italia, avvenuta questa mattina nel corso della tappa di Verona del Security Summit, il più importante convegno italiano dedicato alla sicurezza delle informazioni delle reti e dei sistemi informatici.

Il Rapporto – che fornisce **il quadro più aggiornato ed esaustivo della situazione globale della sicurezza informatica,** grazie alla collaborazione di oltre cento professionisti impegnati in aziende private e pubbliche e docenti universitari che mettono a fattor comune le proprie competenze – contiene in questa edizione per la prima volta contributi inediti della Polizia Postale e delle Comunicazioni e del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza. I dati rilevati evidenziano **l’inarrestabile incremento del cyber crimine nei primi sei mesi del 2015.**
Come già nel 2014, si tratta della **prima causa di attacchi gravi a livello globale**: al cyber crimine, vanno ricondotti, infatti, **il 66% degli incidenti informatici** dichiarati nella prima metà di quest’anno (+ 6% dal dicembre 2014; questo valore era pari al 36% nel 2011).

Nei primi sei mesi del 2015 gli attacchi gravi con finalità dimostrative tipici dell’**Hacktivism** sono invece diminuiti di oltre 15 punti percentuali rispetto al picco del 2013. Dal 2014 rimangono invece sostanzialmente stabili le **attività di spionaggio**. L’**Information Warfare** – la guerra delle informazioni – segna quest’anno una tendenza al calo (probabilmente per mancanza di informazioni pubbliche in merito).

CHI SUBISCE?
Sono le "**infrastrutture critiche**" tuttavia a registrare la crescita percentuale maggiore degli attacchi gravi negli ultimi sei mesi, passando da 2 attacchi nella seconda metà del 2014 a 20 da gennaio a giugno 2015: si tratta di un **incremento del 900%**, pur rappresentando questo settore solo il 4% tra quelli che subiscono attacchi.

Crescita a tre cifre anche per quanto riguarda **Automotive (+400%)**, **Grande Distribuzione (+ 400%), Telecomunicazioni (+ 125%),** e la categoria "**informazione ed entertainment**": siti e testate online, piattaforme di gaming e di blogging **(+ 179%**).

Da evidenziare – sempre nei primi sei mesi del 2015 - il raddoppio degli attacchi informatici subito dalle realtà operanti nella **sanità**, che segna un **incremento dell'81%**.

Per la prima volta, inoltre, i **servizi online e cloud** (principali sistemi di Webmail, Social Network, siti di e-Commerce e piattaforme Cloud) mostrano quest'anno una crescita degli incidenti di oltre il 50%, a dimostrazione di quanto ormai gli attacchi gravi siano mirati contro tutte le tipologie di servizi erogati via Internet.

Nella nuova edizione del Rapporto CLUSIT viene evidenziata anche l'inarrestabile industrializzazione delle minacce e la completa automazione degli attacchi. Secondo gli esperti dell'Associazione Italiana per la Sicurezza Informatica la parola d'ordine è "**prepararsi all'impatto**", gestendo il rischio nell'ambito di una regia istituzionale forte.

"*Lo scenario attuale si è venuto a delineare a causa di vulnerabilità endemiche, non gestite a livello globale per troppo tempo, tanto da divenire oggi in grado di mettere realmente a rischio tutto ciò che è informatizzato*", dichiara Andrea Zapparoli Manzoni, membro del Consiglio Direttivo CLUSIT.
"*Si aggiunge la crescente capacità organizzativa dei criminali hi-tech che, indipendentemente dalla loro natura e dai loro scopi, hanno a disposizione strumenti sempre più sofisticati e relativamente economici, oltre che facilmente reperibili e completamente automatizzabili, ovvero in grado di colpire milioni di sistemi in poche ore. Questo consente loro di cambiare tattiche e strategie in tempo reale e di operare senza interruzione da qualsiasi punto del pianeta*", conclude Zapparoli Manzoni.

La ragione principale per cui gli attaccanti hanno la meglio è, infatti, economica: per ogni dollaro investito dagli attaccanti nello sviluppo di nuovo malware, o nella ricombinazione di malware esistente per nuovi scopi, il costo sopportato dai difensori è attualmente di milioni di dollari.

"*Se consideriamo tutti i sistemi costantemente connessi in Rete, come per esempio router casalinghi, telecamere di sicurezza, stampanti, vending machines, smart tv, giochi per bambini e riflettiamo sul fatto che tutti questi miliardi di sistemi difficilmente riceveranno patch per la vulnerabilità, possiamo comprendere quanto sia davvero grave il problema*", afferma ancora Zapparoli Manzoni.

COME DIFENDERSI?
Gli esperti del CLUSIT delineano quale unica possibilità per fronteggiare le minacce l'adozione di una logica multidisciplinare di **Cyber Resilience**, che fa convergere compliance e cyber security, governance e risk management, cyber intelligence e crisis management, attività di prevenzione e di reazione rapida, fino alla cooperazione tra pubblico e privato e, più in generale, di condivisione delle informazioni.
Cyber Resilience, di fatto, significa comprendere le proprie vulnerabilità e criticità per predisporre un modello di rischio "cyber" accurato e costantemente aggiornato, che consenta di stimare le perdite potenziali al fine di determinare correttamente gli investimenti necessari in sicurezza. L'Italia è in prima linea, come tanti paesi europei: dinamiche di **Cyber Resilience sono state per esempio inserite** nell'ambito del Quadro Strategico Nazionale[1].

"*Un livello soddisfacente di sicurezza informatica si raggiunge solo nel momento in cui tutti coloro che sono in qualche modo connessi in Rete e coesistono nel cyberspazio sono ragionevolmente sicuri*", chiosa Zapparoli Manzoni.

LE TENDENZE PER IL FUTURO
La crescente collaborazione tra gruppi cyber criminali e gruppi terroristici o paramilitari porta gli esperti del CLUSIT ad evidenziare un possibile incremento delle logiche estorsive Ci si attende inoltre che le organizzazioni terroristiche (tra cui l'IS) utilizzino sempre più frequentemente le piattaforme di **Social Networking** come veri e propri campi di battaglia nei confronti dei governi.
Gli stessi Social Network continueranno - come per altro già ampiamente documentato lo scorso anno – ad essere facili vettori di attacco per la diffusione di malware e per le frodi basate su social engineering e potrebbero essere direttamente attaccate. Gli utenti sono potenzialmente oggetto una vera e propria "guerra psicologica" e di "gestione delle emozioni" su larga scala.

I **sistemi POS**, secondo il CLUSIT , presentano una fragilità intrinseca. Contribuiscono a renderli dei facili bersagli la difficoltà oggettiva nel sostituirli rapidamente e la facilità con la quale i criminali possono monetizzare questo genere di attacchi. Con la diffusione di malware sviluppato ad-hoc acquistabile per pochi dollari da criminali comuni, subiranno nel medio-breve termine attacchi anche singoli ristoranti, bar, benzinai, negozi etc. Le banche dovranno fare fronte ad una quantità maggiore di frodi e al crescente scontento degli utenti finali.

A causa del rapido e sviluppo – a cui non è fino ad oggi corrisposta l'adeguata adozione di misure di sicurezza - l'**Internet of Things**, insieme ai device "smart" connessi in Rete, ai sistemi wearable ai sensori per la domotica, agli elettrodomestici intelligenti, alle automobili, si rivela un bersaglio immediato.

La definitiva affermazione dei **device mobili** (smartphone e tablets) sui PC tradizionali implica già oggi un aumento sostanziale di attacchi verso questo genere di strumenti. Cresce l'attenzione da parte di agenzie governative, spie mercenarie e criminali nei confronti di piattaforme quali iOS e Windows Phone, le più difficili da compromettere. In conseguenza di ciò, produttori di device mobili, sviluppatori di applicazioni e tutti gli utenti dovranno rivedere le proprie strategie ed i propri investimenti in materia di mobile, ponendo l'accento sulla sicurezza e non più solo sugli aspetti marketing o di business.

1 http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

Secondo il trend di crescente collaborazione tra gruppi cyber criminali e gruppi terroristici o paramilitari già evidenziato, gli esperti del CLUSIT delineano inoltre una tipologia di attacco economico-politico, che colpirà non solo utenti finali ed aziende, ma anche la **PA ed i sistemi industriali**, incluse – come già visto - le **Infrastrutture Critiche**. In questo ambito, continueranno a diffondersi ransomware di grande successo - quali Cryptolocker – che agiscono secondo una logica estorsiva.

A fronte dell'incremento dei rischi "cyber" evidenziato, gli esperti del CLUSIT prevedono nei prossimi mesi la diffusione della domanda di **strumenti assicurativi** da parte delle imprese, per le quali sarà sempre più critico operare attraverso la Rete e gli strumenti informatici adottando misure correttive adeguate.
La domanda – come si legge nel Rapporto CLUSIT – "sarà parzialmente frustrata dalla scarsità di offerta, e soprattutto dall'impossibilità di assicurare organizzazioni spesso prive delle più elementari misure di sicurezza (in particolare PMI e studi professionali) per mancanza di requisiti. Si diffonderanno comunque per prime quelle polizze che offrono qualche forma di tutela legale per le vittime, e con maggiore lentezza quelle che prevedono un risarcimento dei danni subiti".

Per ulteriori informazioni su Security Summit e sul Rapporto Clusit: www.securitysummit.it
E' possibile richiedere copia digitale del Rapporto CLUSIT 2015 a questo link: https://www.securitysummit.it/generale/rapporto-clusit/

Security Summit è organizzato da:
CLUSIT - i cui soci rappresentano oltre 500 aziende e organizzazioni - è la principale associazione italiana nel campo della sicurezza informatica. Il CLUSIT collabora, a livello nazionale, con diversi Ministeri, Authority e Istituzioni, con la Polizia Postale e con altri organismi di controllo. Inoltre, svolge un'intensa attività di supporto e di scambio con le Confederazioni Industriali, con numerose Università e Centri di Ricerca e con Associazioni Professionali e dei Consumatori.
In ambito internazionale, CLUSIT partecipa a svariate iniziative in collaborazione con i CERT, i CLUSI, la Commissione Europea, ITU (International Telecommunication Union), UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale) e sostiene attivamente le attività di ENISA (European Union Agency for Network and Information Security). Ulteriori informazioni sulle attività del CLUSIT sono disponibili sul sito www.clusit.it

Astrea, Agenzia di Comunicazione e Marketing, specializzata nell'organizzazione di eventi b2b. Con sede operativa a Milano, Astrea mette le competenze dei propri professionisti a disposizione delle organizzazioni per sviluppare soluzioni creative ed innovative volte a incrementare visibilità e ad acquisire autorevolezza sui mercati di riferimento.