Clusit: rischi cyber sottostimati, istituzioni e sanità nel mirino.

Si chiude a Roma Security Summit. Gli esperti Clusit: oltre un'organizzazione su due ha subìto un attacco nell'ultimo anno. Ma se ne accorge solo dopo 146 giorni.

#SecuritySummit #RapportoClusit

Milano, 8 giugno 2017 – 146 giorni, ovvero quasi cinque mesi di "vuoto", in cui aziende, enti, istituzioni, e i loro dati, dopo aver subito un attacco, sono potenzialmente alla mercé dei cyber-criminali. E' questa la situazione media nel 2016 in organizzazioni di ogni tipologia, grandi e piccole, di ogni settore.

Lo evidenziano gli esperti Clusit - l'Associazione per la Sicurezza Informatica in Italia - che nel corso della due giorni romana di Security Summit, svoltasi presso l'Auditorium della Tecnica con un pubblico di circa 600 persone, si sono confrontati con i rappresentanti di istituzioni, imprese e del mondo accademico partendo dai dati del Rapporto Clusit 2017. Obiettivo, accrescere la consapevolezza dei rischi cyber e renderla sempre più parte della quotidianità dei cittadini.

A fronte dell'impressionante escalation di attacchi informatici degli ultimi mesi e della previsione che "*qualsiasi organizzazione (…) ha la ragionevole certezza di subire un attacco informatico di entità significativa entro i prossimi 12 mesi, mentre la metà ne ha subito almeno uno nell'ultimo anno*"[1], è evidente la situazione di "allarme rosso" a livello globale per quanto riguarda il **Cybercrime**.

Sono in inesorabile crescita truffe ed estorsioni nei confronti di privati, aziende ed organizzazioni. In particolare, il rischio cyber appare sempre più elevato nei settori della **Sanità** (che nel 2016 ha subito un incremento degli attacchi del 102% rispetto all'anno precedente), delle **Banche** (+64%), delle **Infrastrutture Critiche** (+15%), che risultano particolarmente vulnerabili e quindi appetibili ai criminali, data la mole di dati gestiti e l'elevata possibilità di creare gravi disservizi, se non di mettere completamente in ginocchio servizi fondamentali per i cittadini. E' questo uno degli obiettivi anche dei sempre più frequenti **State Sponsored Attacks**.

Gli stessi cittadini diventano sempre più bersagli primari: gli esperti Clusit denunciano infatti anche l'incremento di attività di propaganda su web, **PsyOps** - la cosiddetta "guerra psicologica" volta a influenzare opinioni e comportamento - e **alterazione di massa della percezione** (alt-truth), supportate da cyber attacchi.

Il **Phishing**, che adesca le proprie vittime via email, instant messaging e social network, rimarrà il principale vettore di attacco anche nei prossimi mesi. "*Lo abbiamo visto con il recente Wannacry: un ransomware non sofisticato, che si è diffuso rapidamente in tutto il mondo*", afferma Andrea Zapparoli Manzoni, tra gli autori del Rapporto Clusit. "*Siamo in una fase molto delicata, in cui protocolli e architetture sono inadeguate per una superficie di attacco cresciuta in maniera esponenziale, soprattutto con l'Internet of Things e l'Industry 4.0. La messa a punto di un nuovo modello di investimenti in materia di sicurezza ICT, in cui normative, strumenti, consapevolezza e formazione siano gli elementi fondanti, è improrogabile*", conclude Andrea Zapparoli Manzoni.

[1] Rapporto Clusit 2017

Proprio l'aspetto normativo è stato oggetto di approfondito dibattito nel corso della tappa romana di Security Summit: il **GDPR** (General Data Protection Regulation - Regolamento Europeo 2016/679), che entrerà in vigore nel maggio 2018, prevede infatti la comunicazione obbligatoria entro 72 ore al Garante della Privacy di un eventuale "data breach", ovvero della "violazione della sicurezza che porta alla distruzione, alla perdita, all'alterazione accidentale o illegale, alla divulgazione non autorizzata o all'accesso a dati personali trasmessi, memorizzati o altrimenti trattati".

"*Diventa critico, a questo punto, per tutte le organizzazioni dotarsi di sistemi di monitoraggio e prevenzione. A rischio c'è la sopravvivenza*", conferma Andrea Zapparoli Manzoni.

Solo in Italia, è stato calcolato un **costo**, relativo al 2014, pari a **13 miliardi di euro** per l'**interruzione dei sistemi a seguito di attacco cyber**. La perdita di informazioni ha causato danni per 8,4 miliardi di euro; 7,4 miliardi di euro sono stati invece i costi derivati da danni di immagine e alla reputazione e per il recupero dei dati[2].

Security Summit ha il patrocinio della Commissione Europea e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazione e della rete. La tappa romana di Security Summit si è svolta con il patrocinio di Unindustria.

Security Summit continua nel 2017 dopo Milano, Treviso e Roma, con la tappa di **Verona, il prossimo 4 ottobre**. Ulteriori informazioni sono disponibili sul sito securitysummit.it.

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. www.astrea.pro

Per ulteriori informazioni alla stampa si prega di contattare l'Ufficio Stampa Security Summit:
Daniela Sarti
Tel. 335 459432
email: press@securitysummit.it

2 Criminalità Informatica e Rischi per L'economia e le Imprese a Livello Italiano ed Europeo, UNICRI (Dati Italia 2014)