e7
Il settimanale di quotidiano energia

4 OTTOBRE 2017

dossier

DA OTTOBRE TUTTI ATTENTI ALLA SICUREZZA INFORMATICA

Da **OTTOBRE** tutti attenti alla **SICUREZZA INFORMATICA**

Antonio Jr Ruggiero

4 ottobre ’17 - La sicurezza cyber nel luogo di lavoro. Governance, privacy e data protection. Sicurezza cyber in tutte le case. Le competenze della sicurezza cyber. Sono questi i temi che animeranno le quattro settimane dell’European Cyber Security Month (ECSM, 1° - 31 ottobre), che avrà come focus generale il Regolamento europeo sulla protezione dei dati.

L’iniziativa, promossa dalla Commissione UE e organizzata da ENISA (Agenzia dell’Unione europea per la sicurezza delle reti e dell’informazione), è giunta alla sua quinta edizione. Lo scopo è sensibilizzare società, imprese e istituzioni su un problema che sta diventando sempre più di attualità in tutto il mondo. Basti pensare che il 2016 è stato definito “Annus Horribilis” della sicurezza cyber, visto che si è chiuso con incrementi a tre e quattro cifre dei crimini in rete rispetto al 2015: dalla guerra delle informazioni (+117%) a phishing e social engineering (+1.166%).

“Sappiamo che il cybercrime non è più solo un problema informatico ma riguarda tutta la sfera sociale, culturale e perfino emotiva di ogni singolo individuo”, spiega in una nota **Paolo Giudice, Segretario Generale dell’Associazione nazionale sicurezza informatica (Clusit)**, che promuove in Italia la ECSM in collaborazione con l’ISCOM. “Quando parliamo di sicurezza cyber parliamo di una responsabilità condivisa. Per questo mettiamo in campo tutte le nostre risorse, la conoscenza e le esperienze positive, fino ai possibili collegamenti con istituzioni nazionali ed europee, con il supporto di oltre 200 docenti ed esperti che hanno fino ad ora aderito alla campagna ECSM 2017, per accrescere a tutti i livelli la cultura della sicurezza informatica nel nostro Paese”.

Sono circa 50 gli eventi che si alterneranno in Italia nell’ambito del mese europeo della sicurezza informatica (al momento secondo Paese per adesioni) e tra i molti partner nazionali dell’iniziativa ci sono anche le testate editoriali di Gruppo Italia Energia: Quotidiano Energia, e7 e CH4 - la rivista italiana del gas. In particolare, l’appuntamento ufficiale di avvio della manifestazione nel nostro Paese è per oggi, con l’organizzazione a Verona del Security Summit.

“Nel 2017, grazie all’eco mediatica ottenuta da attacchi su scala globale quali WannaCry, l’aumento dei rischi e dei danni provocati dalla crescente insicurezza informatica è diventato mainstream”, secondo **Andrea Zapparoli Manzoni, Membro del Comitato Direttivo Clusit**. “Purtroppo - si legge in un comunicato - le risorse dedicate alla sicurezza da parte di produttori, integratori e utenti finali sono ancora inadeguate rispetto alle minacce attuali. Questo favorisce enormemente gli attaccanti”.

Proprio per aumentare la consapevolezza, nel corso dell’evento di Verona sarà presentato l’aggiornamento dei dati contenuti nel report Clusit 2017 sulla sicurezza ICT. “I dati emersi dall’analisi di centinaia di attacchi gravi del primo semestre 2017 sono emblematici”, prosegue Zapparoli Manzoni. “Siamo ormai entrati in una nuova fase, nella quale la sicurezza cibernetica rappresenta il principale abilitatore della nostra civiltà digitale. In questo scenario, senza investimenti adeguati in sicurezza, l’applicazione delle tecnologie informatiche al business e nelle vite dei singoli cittadini rischia di diventare un boomerang, generando rischi economicamente e socialmente insostenibili”.

Da gennaio a giugno di quest’anno sono stati 571 gli attacchi gravi di dominio pubblico nel mondo (ovvero atti che hanno avuto un impatto significativo per le vittime in termini di danno economico, reputazione e diffusione di dati sensibili), segnando un +8,35% rispetto al secondo semestre 2016. In questo modo il primo semestre 2017 è stato il peggiore dal 2011 e oltre il 50% delle organizzazioni nel pianeta ha subito almeno un attacco grave nell’ultimo anno.

Nel dettaglio, sono aumentati del 253% gli attacchi verso “bersagli multipli indifferenziati” condotti da un’unica forza criminale secondo una logica “industriale”. A essere utilizzati sono soprattutto Malware (+86%, di cui oltre un terzo Ransomware) e tecniche di Phishing/Social Engineering (+85%). In questo scenario l’Europa è l’unico continente dove cresce la percentuale di vittime.

Per quanto riguarda i device, invece, gli smartphone sono quelli maggiormente nel mirino con malware specifici per tutte le piattaforme.

“La rapida diffusione di smart working, che si avvale di strumenti quali mobile, cloud e social, spesso utilizzati in maniera indiscriminata mescolando profili personali e lavorativi, e dell’Internet of Things, con apparecchiature per lo più prive delle più elementari misure di sicurezza, costituiscono punti di accesso sempre più immediati verso i sistemi informativi delle organizzazioni”, scrive il Clusit nel report 2017. “Da evidenziare che ciò avviene oggi anche in contesti produttivi, quali l’Industry 4.0, e per applicazioni critiche come e-health e smartcity”. Ma perché avvengono questi attacchi? “Il cybercrime la prima ragione nei primi sei mesi dell’anno: i criminali colpiscono le loro vittime nel 75% dei casi con l’obiettivo di estorcere denaro”.

CULTURA E AZIONI CONCRETE PER LA CYBERSECURITY

A.J.R.

4 ottobre ‘17 - Qual è lo stato di salute della sicurezza informatica nel nostro Paese? Ne abbiamo discusso con **Claudio Telmon, membro del Consiglio direttivo Clusit e Consulente nel campo della sicurezza informatica**.

Quanto sono efficaci eventi come l'European Cyber Security Month?
Con l'occasione del mese della sicurezza ci sono iniziative che in alcuni casi non sarebbero state fatte o altrettanto pubblicizzate. Quindi hanno maggiore riscontro. Sono particolarmente efficaci le attività che coinvolgono contesti dove normalmente non ci si occupa della sicurezza.

Prima dell'estate è stato pubblicato in Gazzetta Ufficiale il nuovo "Piano nazionale per la protezione cibernetica e la sicurezza informatica". È un documento che va nella direzione giusta?
Non sono critico sul piano perché i principi indicati e le linee d'azione sono sicuramente validi e significativi. La mia perplessità, come spesso capita quando si parla di sicurezza, è che seguano anche azioni concrete. Se guardiamo a questo documento e alla versione precedente le differenze sono limitate. Per molti degli ambiti trattati dal piano nazionale degli anni scorsi, però, non ci sono stati grandissimi passi avanti. La perplessità, dunque, non è sul piano in sé ma sul fatto che da un documento di quel genere derivi qualcosa di sostanziale.

Cosa si dovrebbe fare di diverso?
Il passaggio verso la concretezza ha due esigenze. La prima è che alcune strutture previste o richiamate dal piano abbiano le risorse e il commitment per svolgere in maniera completa e incisiva il loro compito. Il secondo aspetto riguarda la Pubblica Amministrazione. In questo caso, al di là delle regole, serve fare in modo che le indicazioni siano rispettate. La non adeguatezza della P.A. è un tema importante. L'ultimo esempio è dato dal problema riscontrato nell'avvio dello "Spesometro" da parte dell'Agenzia delle Entrate. Il problema è stato proprio la violazione della privacy. In generale ci sono aspetti molto di base su cui la P.A. deve adeguarsi.

Sul fronte delle imprese, invece, in Italia il Governo ha puntato sul Piano Industria 4.0, che arriva fino alle PMI. Ci sono risvolti significativi di cybersecurity?
Nella prima versione del Piano il tema della sicurezza era uno di quelli su cui c'erano finanziamenti. Ogni azienda, mettendo sicurezza nei propri asset, tutela i suoi interessi. È chiaro che servirebbero finanziamenti per questo, però serve anche cultura e i manager di settore possono fare qualcosa. Quando partecipo a eventi e convegni in cui viene spiegato alle PMI i rischi della sicurezza c'è una risposta, anche se certamente la capacità successiva di intervenire è più limitata rispetto a una grande realtà, anche solo per quanto riguarda l'accesso alle competenze; per questo bisognerebbe intervenire tramite le associazioni di settore.