

Diritto alla privacy e gestione sicura dei dati personali nel sistema sanitario, tra falsi miti, realtà e complessità

Pisa, 30 novembre 2018

Cybercrime e rischi di sicurezza in ambito sanitario, la guerra continua

Giuseppe Augiero FTGM











Il gioco continuo

 "La Sicurezza Informatica è come un gioco continuo del gatto e del topo, con gli esperti di sicurezza da un lato e gli intrusi dall'altro."



Arte dell'inganno





E' un problema che ci riguarda?





Il cybercrime è fuori controllo 122 attacchi gravi ogni mese

Pagine a cura di Roxy Tomasicchio

a curva dei crimini informatici non ha ancora iniziato il suo tratto discendente. Anzi: dopo il 2016 e 2017, già etichettati come gli anni peggiori, l'anno in corso, con 730 attacchi gravi registrati e analizzati, pari a una crescita del 31% rispetto al semestre precedente, si appresta a battere il primato. Ci sono anche crimini informatici che hanno messo a segno percentuali di crescita a tre cifre, per esempio nel settore auto motive (+200%), e le tecniche, nella maggior parte dei casi, sono alla portata di tutte le tasche dei cyber criminali. È, infatti, il malware semplice, cioè un prodotto a costi decrescenti, il vettore di attacco più utilizzato (40% del totale). Lo scenario è quello delineato dalla nuova edizione del Rapporto Clusit, redatto dall'Associazione italiana per la sicurezza informatica, e presentato nel corso di Security Summit di Verona, il convegno che si propone di analizzare lo stato dell'arte della cybersecurity e di stimare le prospettive future per incrementare la cultura sui temi della sicurezza delle informazioni, delle reti e delle infrastrutture informatiche.

al 2011, anno a cui risale la prima edizione del rapporto Clusit, e del 7% rispetto al 2016. Ma più che il dato numerico, spaventa l'elemento qualitativo: oggi il fenomeno intralcia non solo la vita privata dei cittadini (vittime nel 2017 di crimini estorsivi su larghissima scala), ma anche il piano finanziario e geopolitico. Leggendo tra le cifre, emerge che il cybercrime (il cui scopo è sottrarre informazioni, denaro, o entrambi), è sempre la prima causa di attacchi gravi a livello mondiale (76% degli attacchi complessivi, in crescita del 14% rispetto al 2016). Ma sono già in corsia di sorpasso gli attacchi compiuti con finalità di Information Warfare (la cosiddetta guerra delle informazioni) con il +24% rispetto al 2016 e il cyber espionage (lo spionaggio con finalità geopolitiche o di tipo industriale, tra cui va ricompreso il furto di proprietà intellettuale), che cresce del 46%. Ad accrescere lo stato di allerta ci sono i dati sui costi, quintuplicati, per un importo complessivo di 500 miliardi di dollari nel 2017 (circa 435 miliardi di euro). E nel corso del 2017 truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati, una

assoluto più alto negli ultimi 4 anni e mezzo. In linea con i dati precedenti, nei primi sei mesi del 2018 il cybercrime è stato la causa dell'80% degli attacchi informatici a livello globale, risultando in crescita del 35% rispetto all'ultimo semestre 2017; ad aumentare maggiormente quest'anno (69% rispetto ai sei mesi precedenti) sono però le attività riferibili al cyber espionage.

Per quanto riguarda i settori, dopo l'automotive, ci sono crescite a tre cifre anche in ambito «Research/Education» (+128%) e «Hospitability»: hotel, ristoranti, residence hanno subito da gennaio a giugno 2018 il 69% di attacchi in più rispetto agli ultimi sei mesi dello scorso anno. In decisa crescita anche i crimini nei settori Sanità (+62%), Istituzioni (+52%) e Servizi online/ Cloud (+52%) e nel settore della Consulenza (+50%). In assoluto la categoria più colpita è quella identificata dagli esperti Clusit come «Multiple Targets» (18% del totale degli attacchi a livello globale), in aumento del 15% rispetto ai sei mesi precedenti, ossia quegli attacchi compiuti in parallelo dallo stesso soggetto attaccante contro numerose organizzazioni appartenenti a categorie diverse e a settori differenti. Il fenomeno evidenzia concretamente la



Cyber (in)Security

- Il 2017 era stato definito come l'anno:
 - "peggiore di sempre".
 - del trionfo dei malware.
 - dell'industrializzazione degli attacchi a livello mondiale.

· ...e il 2018?



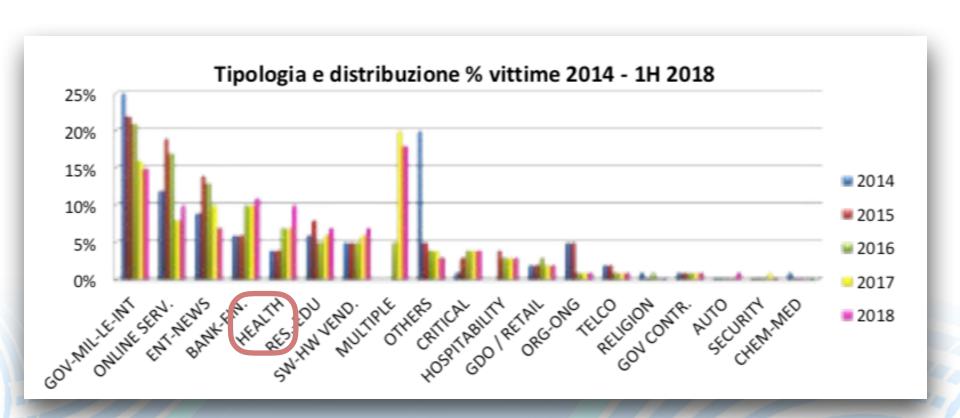
Il trend degli attacchi informatici







Sanità





Crescita degli attacchi

- Il CyberCrime è aumentato del 35% rispetto al 2017.
- 80% degli attacchi è portato a termine da gruppi criminali.
- Molte "soluzioni d'attacco" sono facilmente acquistabili nel mercato nero.
- Sono scesi in campo alcuni Stati.



Money, money ... cybercrime

 Ogni attacco informatico, il cui scopo è la sottrazione di informazioni, ha un ritorno economico per l'attaccante.



Il valore delle informazioni

• Un singolo record sottratto ha un valore di mercato di circa 148\$.

• Un "dato" sanitario sottratto ha un valore che varia tra i 700\$ e i 1000\$.

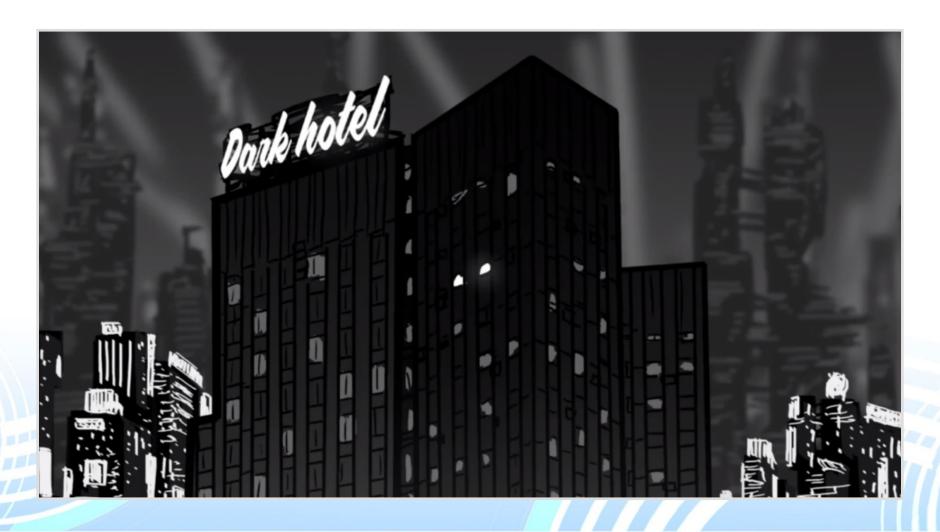


Come vengono sottratte le informazioni?





Dark Hotel





Possiamo essere la causa dei nostri databreach?





CodeMotion - 29 e 30 novembre 2018





Peer to peer

- Una azienda che gestiva una banca dati del DNA è fallita a causa dell'installazione di un software di p2p da parte di una sua segretaria.
- La segretaria aveva "condiviso" la cartella Documenti con il software di p2p.
- E' facile immaginare le conseguenze...



Ransomware

- Gli attacchi andati a buon fine sono tanti...
- Industria 4.0:
 - Un'azienda Italiana ha dovuto chiudere i battenti per 3 giorni e mandare a casa 650 persone perché i suoi sistemi erano stati infettati da un ransomware.
 - La linea di produzione era completamente ferma.



Fascicolo Sanitario Elettronico





I problemi sono finiti?





Pacs





Babbo Natale





Conclusioni

- Non basta acquistare un prodotto o pagare un consulente per risolvere i problemi di cybersecurity.
- La grande rete non è un ambiente virtuale.
- Occorre migliorare passo dopo passo in una marcia costante.
- Ci saranno nuove sfide tecnologiche e quindi occorre ... Consapevolezza!!!





Diritto alla privacy e gestione sicura dei dati personali nel sistema sanitario, tra falsi miti, realtà e complessità

Pisa, 30 novembre 2018

Cybercrime e rischi di sicurezza in ambito sanitario, la guerra continua

Giuseppe Augiero

Email: giuseppe@augiero.it

Website: www.augiero.it

Twitter: @GiuseppeAugiero









