Privacy e Cybersecurity nella sanità

Relatore: Stefania Tonutti

21 giugno 2017: ore 18.30

FP1640985001
#Sharing3FVG

Webinar realizzato da IALFVG e parte degli 80 di #Sharing3FVG, progetto cofinanziato dal Fondo Sociale Europeo nell'ambito del Programma Operativo Regionale 2014/2020

CYBERCRIMES

Ma cosa sono i CRIMINI INFORMATICI?
Una definizione semplice

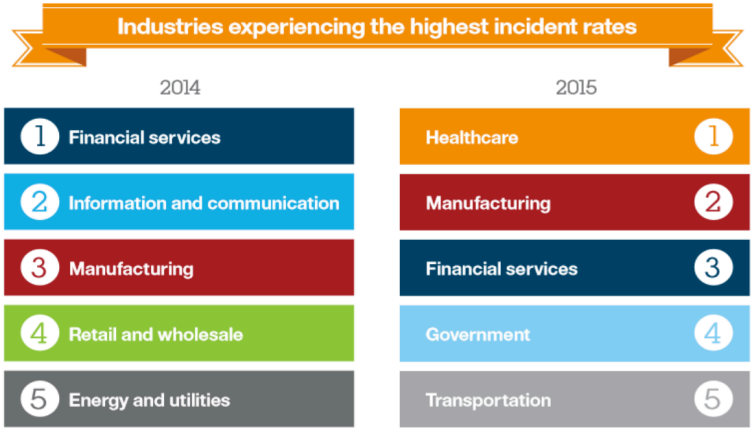
- Attività illegali che comprendono una vasta gamma di reati, dal crimine contro dati riservati alla violazione di contenuti e del diritto d'autore (Krone, 2005)
- Fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica Possono essere distinti in due macro categorie:
- 1. Crimini che hanno come obiettivo diretto, le reti digitali e i computer ad essa connessi;
- 2. Crimini facilitati dalle reti digitali e dai computer ad essa connessi.

Alcuni dati statistici

Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	↗
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑

Rapporto Clusit 2017



Ponemon Institute – 2016 Cost of Data Breach Study; IBM X-Force – 2016 Cyber Security Intelligence Index

Un tipico esempio di cyberattacco nel mondo sanitario

RAMSOMWARE

Un ransomware è un malware distribuito via email che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.

- Pagamento in Bitcoin. Vengono utilizzati servizi di pagamento accessibili solo attraverso il "Deep Web"

Attacco hacker mondiale: virus "Wannacry" chiede il riscatto, ospedali britannici in tilt. "Usato codice Nsa"

Pirateria informatica, attacco hacker in corso in tutto il mondo: chiesto "riscatto" in bitcoin

Usa, i pirati informatici bloccano cartelle cliniche e mail: l'ospedale sceglie di pagare il riscatto

Ramsomware in sanità

Perché gli ospedali?

- ✓ Utilizzo di sistemi IT legacy
- ✓ Utilizzo di dispositivi medici con sicurezza debole
- ✓ Necessità di accesso immediato alle informazioni

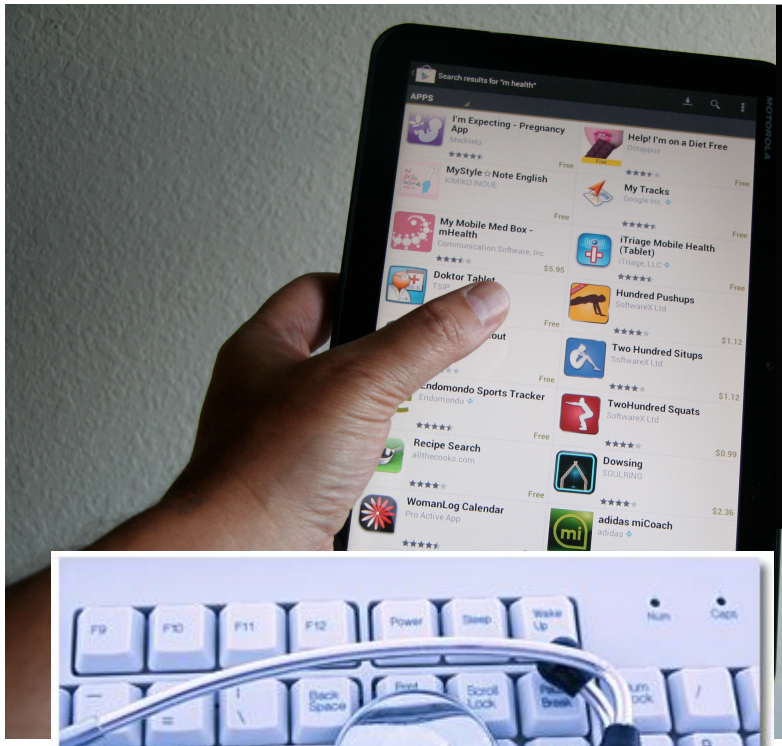
Alcune garanzie che dovrebbe mettere a disposizione la struttura

- ✓ Continuità della cura del paziente
- ✓ Sicurezza dei dati dei pazienti proteggendoli da possibili violazioni e fughe di notizie
- ✓ Supporto e manutenzione di attrezzature adeguate ed aggiornate

La maggior parte degli attacchi sono il risultato NON intenzionale di azioni dei dipendenti, ad esempio:

- ✓ **Azioni di click a link malevoli**
- ✓ **Apertura di allegati alle mail**
- ✓ **Cattivo utilizzo dei dispositivi medici**

Nel concreto.....



E quindi quali soluzioni?

Food and Drug Administration (FDA)

- ottobre 2014 ha emesso le linee guida sulla gestione della cybersecurity nei medical devices prima della loro commercializzazione (fase di "pre market")
- dicembre 2016 sono state pubblicate analoghe linee guida anche per la fase di "post-market", nell'ottica di garantire un adeguato livello di protezione dei dispositivi biomedicali lungo tutto il loro ciclo di vita, dalle fasi iniziali di sviluppo e progettazione fino al supporto post vendita

UE E GARANTE PRIVACY

- Regolamento Generale Europeo sulla Protezione dei Dati Personali (General Data Protection Regulation – GDPR)
- D.lgs. 196/2003 (Codice Privacy: verrà totalmente sostituito dal GDPR nel maggio del 2018)

"MESSA IN SICUREZZA"
cd. Risk and Security Cycle

RISK AND SECURITY CYCLE

PIANIFICAZIONE E GOVERNANCE

- Comprendere priorità e strategie aziendali
- Adeguata allocazione delle risorse

PIANIFICAZIONE DEL SISTEMA DI GESTIONE DELL'ICT SECURITY & RISK MANGEMENT

- rilevazione dello scenario attraverso una ricognizione di tutte le componenti del sistema informativo aziendale

PREDISPOSIZIONE DEL DOCUMENTO DI RELAZIONE FINALE

- complesso di interventi e misure di sicurezza fisiche, logiche, organizzative
- piano di continuità aziendale

IMPLEMENTAZIONE MISURE DI SICUREZZA

IN SANITÀ COME APPLICO TUTTO QUESTO

- necessità di interazione fra diverse figure professionali, che, in tempi diversi, ruotano "intorno al paziente" sino al suo domicilio e che possono appartenere a "legal entity" diverse
- principio di necessità e non eccedenza dei dati raccolti per uno specifico trattamento e per una specifica finalità
- rispetto dell'autodeterminazione del cittadino nella gestione dei propri dati clinici precisando che la "self determination" concerne anche la possibilità di conoscere quando e chi abbia consultato i propri dati clinici
- necessità dell'informativa sul trattamento e quindi che il cittadino sia reso dettagliatamente informato rispetto all'utilizzo che verrà effettuato dei suoi dati clinici

E POI……

GRANDI NOVITÀ

"CONSUMERIZZAZIONE" SANITARIA

Frequente nella prassi quotidiana, e difficilmente regolabile, l'utilizzo di whatsapp, dropbox e altri strumenti che facilitano la presa in carico del cittadino e la comunicazione tra cittadino ed equipe che lo sta seguendo (ad es. per la comunicazione di referti, pareri o scambio immagini sia tra clinici sia tra paziente e team di riferimento)

~~Cittadino off/on-line~~

~~Professionista off/on-line~~

ON-LINE

NUOVI CONFINI PER LE AZIENDE SANITARIE

I confini del sistema informativo di un'azienda sanitaria diventano quindi:

- ✓ permeabili: non più solo clienti interni ma utilizz-Attori (interni ed esterni) sempre "on web"
- ✓ estesi: ben oltre "le mura" aziendali, sempre più verso homecare, wearable, IoT
- ✓ disponibilità e continuità dei servizi h24
- ✓ sicurezza nella gestione/consultazione ubiquitaria dei dati
- ✓ privacy e Integrità dei dati trattati
- ✓ disponibilità dei servizi e dei dati any where e any device

LA SVOLTA: IL GDPR

Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (General Data Protection Regulation – GDPR) è entrato in vigore il 26 maggio 2016 e sarà applicato a partire dal 25 maggio 2018.

- Nuove responsabilità per titolare e responsabile (cd. "accountability")

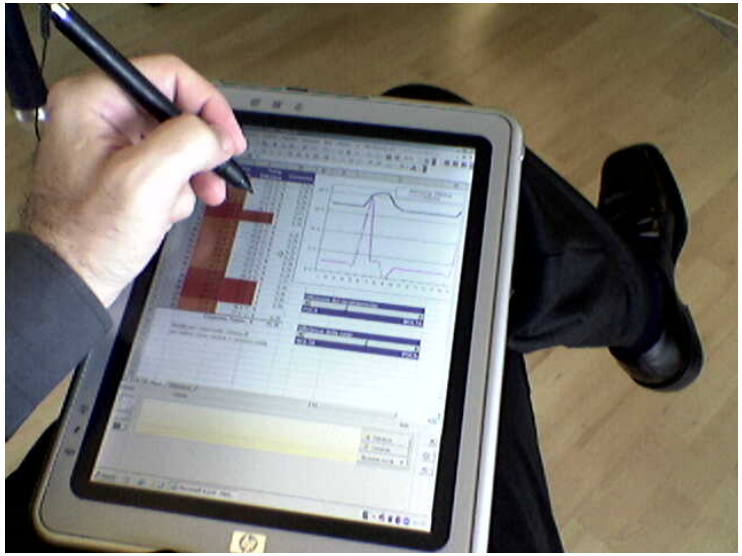
Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.** ...

ESPRESSA possibilità della DESIGNAZIONE DIRETTA DI UN RESPONSABILE DA PARTE DI ALTRO RESPONSABILE (tramite delega del titolare)

LA SVOLTA: IL GDPR

- I registri dei trattamenti



Articolo 30
Registri delle attività di trattamento

1.Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

...

2.Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

LA SVOLTA: IL GDPR

- DATA BREACH

Il GDPR richiede poi di comunicare al Garante le violazioni dei dati personali eventualmente subite entro un tempo molto stretto: 72 ore

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1.In caso di violazione dei dati personali, **il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

LA SVOLTA: IL GDPR

PRIVACY BY DESIGN e PRIVACY BY DEFAULT

- ✓ **prevenire** non correggere, cioè i problemi vanno valutati nella fase di progettazione;
- ✓ privacy come impostazione di **default**;
- ✓ privacy **incorporata** nel progetto;
- ✓ massima **funzionalità**, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- ✓ **sicurezza** durante tutto il ciclo del prodotto o servizio;
- ✓ **trasparenza**;
- ✓ **centralità** dell'utente

LA SVOLTA: IL GDPR

IL DPO

la nomina di è obbligatoria in tre casi specifici:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

COSA DEVE FARE IL DPO

- ✓ Sorvegliare l'osservanza del GDPR
- ✓ Effettuare una valutazione d'impatto
- ✓ Valutare il rischio
- ✓ Tenere il registro dei trattamenti
- ✓ Fare da tramite fra il Titolare e l'Autorità Garante
- ✓ Figura autonoma e *super partes*

IN SINTESI….

E ORA CHE FARE?

GRAZIE PER L'ATTENZIONE!

stefania.tonutti@gmail.com

www.linkedin.com/in/stefania-tonutti

@TonuttiStefania

Stefania Tonutti It and Privacy Expert Ph.D in Law and New Technologies