Sviluppo di competenze tecnico-operative nell'ambito delle tecnologie assistive e di modelli di servizio innovativi

Mod. 2- Privacy e Gestione dei rischi

Febbraio- Marzo 2022

AGENDA

- Questionario
- Discussione collettiva
- Alcuni dati di contesto
- Pausa
- Il processo di gestione del rischio privacy
- Esercitazioni e restituzione

QUESTIONARIO

Il livello di maturità della mia organizzazione in materia privacy e sicurezza

https://forms.gle/HQWWBf8J3996oXvWA

Panorama italiano ed internazionale sulla sicurezza informatica

Fonte: Rapporto CLUSIT 2021 *(Associazione italiana per la sicurezza informatica)*

Per l'Italia…

- Obiettivo: rilevare la percezione che le aziende hanno della sicurezza informatica
- 304 aziende in tutto il territorio nazionale (toscana quarta regione per affluenza con circa 40 aziende) – 52% piccole aziende (<50), 28% medie aziende (51-250), 28% grandi aziende (> 250)
- Il 76% dice di non essere stato colpito nel 2020 da attacchi informatici – **23%** dichiara di averli subiti
- I danni sono stati considerati: di grave entità (**20%**), di media entità (**40%**), di bassa entità (13%), trascurabili (26%)
- Tipologia di danni subiti: circa 38% esfiltrazione/perdita di dati; 25% danni di natura economica; 17% danni di immagine, 17% danni infrastrutturali e di perdita di tempo per il ripristino dello status quo(blocco della continuità operativa)

Panorama italiano ed internazionale sulla sicurezza informatica

Fonte: Rapporto CLUSIT 2021 *(Associazione italiana per la sicurezza informatica)*

Per l'Italia…

- Capacità di difendersi: 41% ritiene di essere perfettamente in grado di difendersi, il 17% sufficientemente capace di difendersi, il **41%** poco o per niente capace di difendersi
- Percezione circa la probabilità di essere colpiti da un attacco: **48%** lo ritiene altamente probabile, 24% sufficientemente probabile, 25% poco probabile, 3% per nulla probabile
- Grado di consapevolezza dell'organizzazione circa le conseguenze di un attacco: 19% molto alta, 22% abbastanza alta, 16% sufficiente, **30%** poca, 13% nessuna
- Formazione mirata: 54% delle organizzazioni li prevede, **46%** non li prevede
- Percezione circa la necessità di formazione mirata: **95%** molto utile, 5% non utile
- Verifiche di sicurezza in sede di procurement: **56%** non opera alcuna verifica in ordine ai requisiti di sicurezza di terze parti fornitrici; 44% controlla i requisiti di sicurezza

L’ANELLO PIU’ DEBOLE DELLA CATENA E’ IL FATTORE UMANO,
TANTO E’ VERO CHE LA TECNICA DI ATTACCO MAGGIORMENTE UTILIZZATA E’ QUELLA DEL PHISHING, CHE SFRUTTA TECNICHE DI SOCIAL ENGENEERING

Consiglio bibliografico: «*L’arte dell’inganno. I consigli dell’hacker più famoso del mondo*» di Kevin D. Mitnick

Qualche esempio

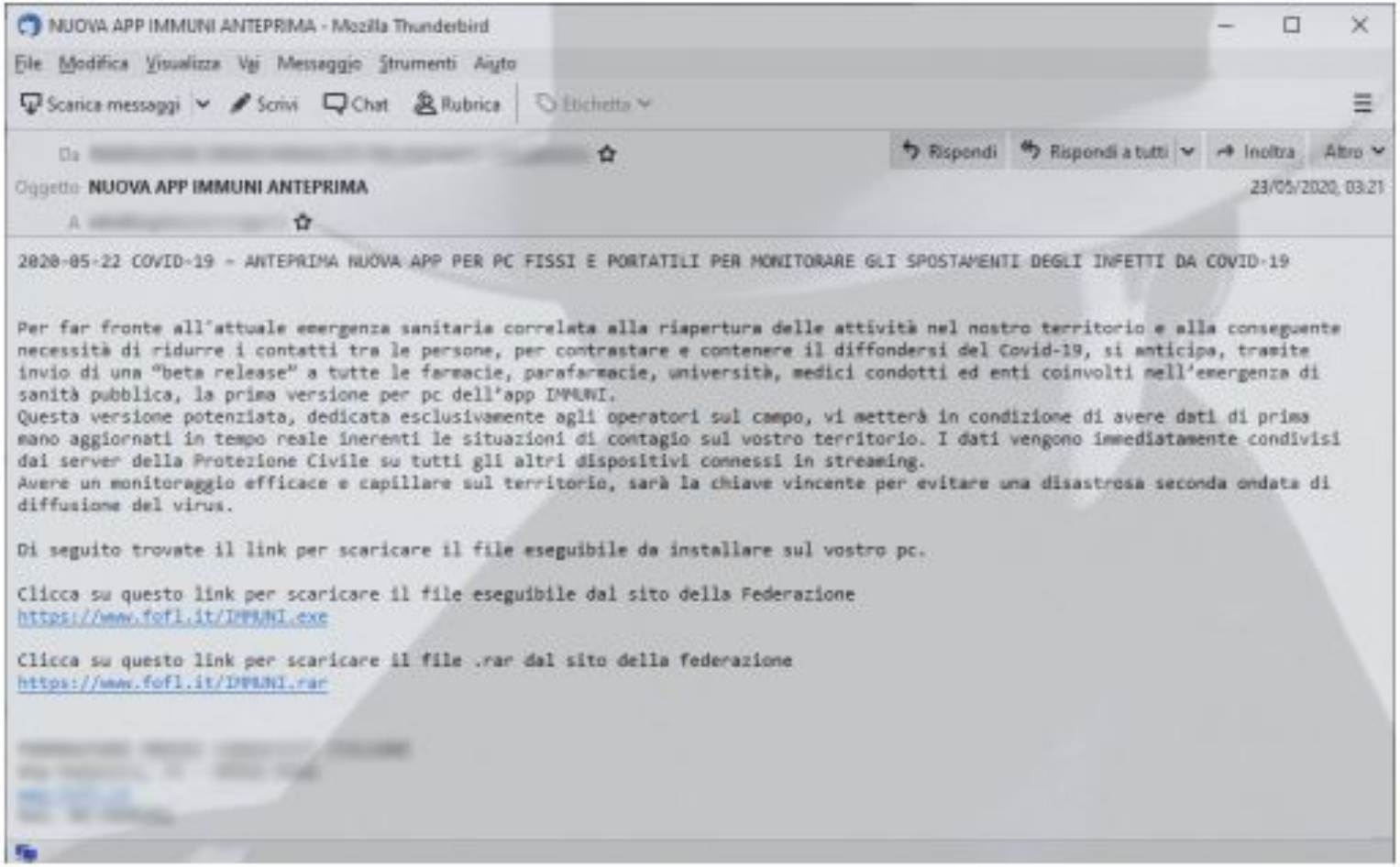
Il COVID-19 ha offerto innumerevoli nuovi spunti per campagne di phishing veicolate via email, spunti che sono stati prontamente colti e utilizzati in campagne malevole.
Ricordiamo che una campagna di phishing efficace è caratterizzata da tre elementi principali: il presentarsi come una fonte autorevole, la capacità di catturare l'attenzione della vittima, quella di instillare un senso di urgenza al fine di indurre a compiere un'azione dannosa come aprire un allegato malevolo, cliccare su un link, fornire credenziali o informazioni confidenziali. Autorevolezza, cattura dell'attenzione, senso di urgenza, call-to-action ... se ci facciamo caso parliamo esclusivamente di leve che agiscono su aspetti affatto tecnici ma legati ai comportamenti umani.
Non è difficile immaginare come un evento eccezionale come quello pandemico con tutto il suo carico emotivo, il flusso continuo di nuove informazioni, il susseguirsi di provvedimenti normativi, i cambiamenti delle modalità di lavoro e delle abitudini di vita, abbia creato un terreno molto fertile per gli autori di campagne di phishing.

FUCKUNICORN – Il ransomware italiano

Il 23 maggio 2020 è stata avviata una campagna malspam in italiano con oggetto "**NUOVA APP IMMUNI ANTEPRIMA**".
Il messaggio invitava ad installare nel proprio PC l'app IMMUNI da un link presente all'interno del messaggio, per far fronte all'attuale emergenza epidemiologica del Covid-19.
Il link in realtà scaricava il ransomware denominato **FUCKUNICORN**.

In figura la nuova immagine dello sfondo cambiata dal ransomware **FUCKUNICORN** al termine della cifratura

Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist


NUOVA APP IMMUNI ANTEPRIMA - Mozilla Thunderbird

File Modifica Visualizza Vai Messaggio Strumenti Aiuto

Scarica messaggi Scrivi Chat Rubrica Etichetta

Da [redacted]

Rispondi Rispondi a tutti Inoltra Altro

Oggetto: **NUOVA APP IMMUNI ANTEPRIMA** 23/05/2020, 03:21

A [redacted]

2020-05-22 COVID-19 - ANTEPRIMA NUOVA APP PER PC FISSI E PORTATILI PER MONITORARE GLI SPOSTAMENTI DEGLI INFETTI DA COVID-19

Per far fronte all'attuale emergenza sanitaria correlata alla riapertura delle attività nel nostro territorio e alla conseguente necessità di ridurre i contatti tra le persone, per contrastare e contenere il diffondersi del Covid-19, si anticipa, tramite invio di una "beta release" a tutte le farmacie, parafarmacie, università, medici condotti ed enti coinvolti nell'emergenza di sanità pubblica, la prima versione per pc dell'app IMMUNI.
Questa versione potenziata, dedicata esclusivamente agli operatori sul campo, vi metterà in condizione di avere dati di prima mano aggiornati in tempo reale inerenti le situazioni di contagio sul vostro territorio. I dati vengono immediatamente condivisi dai server della Protezione Civile su tutti gli altri dispositivi connessi in streaming.
Avere un monitoraggio efficace e capillare sul territorio, sarà la chiave vincente per evitare una disastrosa seconda ondata di diffusione del virus.

Di seguito trovate il link per scaricare il file eseguibile da installare sul vostro pc.

Clicca su questo link per scaricare il file eseguibile dal sito della Federazione
https://www.fofi.it/IMMUNI.exe

Clicca su questo link per scaricare il file .rar dal sito della federazione
https://www.fofi.it/IMMUNI.rar

[redacted]

Mentre il Ransomware cifra i file viene mostrata all'utente la seguente schermata di una mappa raffigurante l'infezione da Covid-19:
Il malware contiene diversi indicatori che fanno ipotizzare che la realizzazione del Ransomware sia italiana.

Il riscatto richiesto è di 300 Euro, da versare in cryptovaluta BitCoin.

"La lunga serpe sul bastone di Asceplio si è ribellata, ed una nuova era sta per sopraggiungere! Questa è la vostra possibilità per redimervi dopo anni di peccati e soprusi. Sta a voi scegliere. Entro 3 giorni il pegno pagare dovrai o il fuoco di Prometeo cancellerà, i vostri dati così come ha cancellato il potere degli Dei sugli uomini. Il pegno è di solamente 300 euros, da pagare, con i Bitcoin al seguente indirizzo: 195naAM74WpLtGHsKp9azSsXWmBCaDscxJ dopo che pagato avrai, una email mandarci dovrai. xxcte2664@protonmail.com il codice di transazione sarà la prova. Dopo il pegno pagato riceverai la soluzione per spegnere il fuoco di Prometeo. Andare dalla polizia o chiamare tecnici a niente servirà, nessun essere umano aiutarti potrà."

Contenuto del file del riscatto

PRIMA DI GESTIRE IL RISCHIO OCCORRE ESSERE CONSAPEVOLI CHE ESISTE E COMPRENDERLO

CONSAPEVOLEZZA

https://www.youtube.com/watch?v=nTWPWscGOIA

https://www.youtube.com/watch?v=OaT_chrUy2w

DIVERTIAMOCI UN PO'!!!!

Per verificare quanto la tua password è affidabile: https://password.kaspersky.com/it/

PER COMPRENDERE IL RISCHIO OCCORRE PARTIRE DALL'ALFABETIZZAZIONE

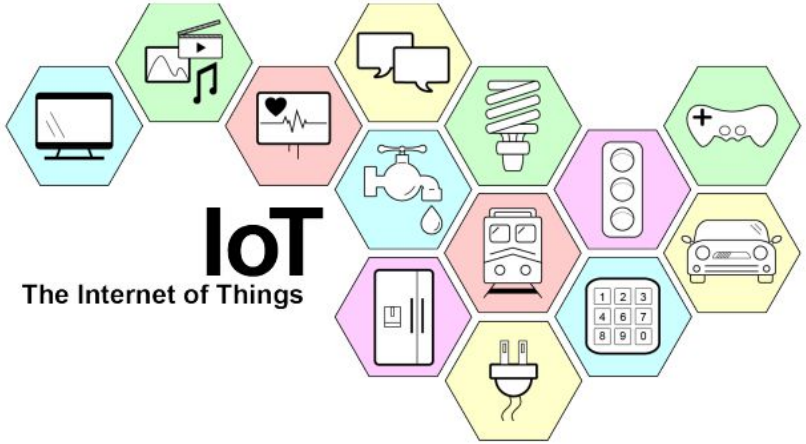
GLOSSARIO INTERATTIVO
(da affiancare al catalogo tecnologie)

Aggiungere link

1. Rischi Privacy che non dipendono dal contesto ma sono insiti nella tecnologia stessa

Per entrare meglio nel dettaglio utilizzeremo la suddivisione nelle seguenti categorie:

- ➔ **IoT (compresi wearables, sensori e Smart TV)**
- ➔ **Robotica e AI**
- ➔ **Big Data**



Definizione

E' un network di oggetti fisici o virtuali connessi in una rete che incorporano una tecnologia per intercettare dati, comunicare e/o interagire tra di loro e/o con l'ambiente circostante

(link ppt Fiorini su Lessico ICT)

Caratteristiche distintive dell'IoT :

→ capacità di interagire con il mondo fisico e digitale circostante

→ minore capacità di accedere, gestire e controllare le componenti e i sistemi del dispositivo

→ i tradizionali sistemi o le tradizionali misure di protezione per la privacy non sono applicabili o non sono efficaci su molti dispositivi IoT

NIST, *Consideration for Managing IoT Cybersecurity and Privacy Risks*, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Proprietà		**Rischi privacy**	**Principi e referenti normativi**
capacità di interagire con il mondo fisico e digitale circostante	• funzioni di *sensing* e *actuating* • interfaccia di altri apparecchi (M2M), di network e umani	• la misurazione del mondo esterno può sempre avere un margine di errore • incidere direttamente nella sfera di diritti e libertà delle persone • maggior segmentazione dei trattamenti, minor capacità di comprensione • concentrazione di grande quantità di dati con capacità di entrare capillarmente nella vita delle persone (**profilazione** e dati biometrici)	❑ **esattezza** del dato (art. 5 c. 1 lett. d) - GDPR) ❑ non essere sottoposti a decisione basata su **trattamento automatizzato** (art. 22 GDPR) ❑ **trasparenza** (art. 5 c. 1 lett. a) - GDPR) ❑ principio di **limitazione delle finalità** e **minimizzazione** (art. 5 c.1 lett.b)-c) - GDPR)
minore capacità di accedere, gestire e controllare le componenti e i sistemi del dispositivo	• "black boxes" • frammentazione delle componenti che ne determinano l'usabilità • frammentazione dei trattamenti	• oggettivizzazione dell'interessato (user-non user) • difficoltà di ricostruire in maniera chiara il data flow e quali entità sono coinvolte	❑ **liceità** del trattamento (art. 5 c.1 lett. a)- art. 6 GDPR) ❑ **integrità** , **riservatezza** (art. 5 c.1 lett. f - art. 32 GDPR) e **limitazione della conservazione** (art. 5 c.1 lett. e) ❑ identificabilità del data controller/processor
i tradizionali sistemi o le tradizionali misure di protezione per la privacy non sono applicabili o non sono efficaci su molti dispositivi IoT	• le misure di sicurezza da adottare devono essere ripensate in funzione delle suddette caratteristiche	• difficoltà legate alla funzionalità che ci si attende o ad aspetti strutturali rendono difficile incorporare misure di sicurezza	❑ **Privacy by Design** (art. 25 GDPR)

Definizione

Macchina programmabile in grado di eseguire una serie di azioni o attività complesse al pari, o addirittura meglio, di un essere umano

Caratteristiche distintive del robot :

→ assenza di vita biologica

→ supporto fisico minore (o assente? Bot)

→ autonomi o semi-autonomo, grazie alla capacità di interagire con l'ambiente circostante (interconnettività) grazie a sensori

→ adattamento del proprio comportamento e delle proprie azioni all'ambiente

→ (talvolta) capacità di autoapprendimento tramite esperienza ed interazione

***Risoluzione Parlamento UE 16/2/2017**, "Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica"*

Definizione

"Sistemi che mostrano un comportamento intelligente, analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia per raggiungere specifici obiettivi.
I sistemi basati sull' AI possono consistere solo in sw che agiscono nel mondo virtuale (assistenti vocali, sw per l'analisi delle immagini, sistemi di riconoscimento vocale o facciale, ecc..) oppure incorporare l'AI in dispositivi hardware (per es. robot avanzati, auto a guida autonoma, droni o applicazioni dell'IoT)"

dalla **Comunicazione Comm. UE (2018) 237** *"Artificial Intelligence for Europe"*

Caratteristiche distintive dell'AI:

→ **potenza e velocità di calcolo**

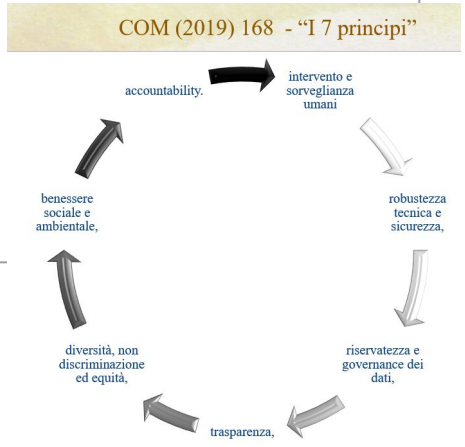
→ **capacità di prendere decisioni con elevato grado di affidabilità**

→ **riproduzione dei meccanismi di funzionamento del cervello umano**

→ **tecnologia di base: connessione delle reti neurali =** ***rete composta da nodi e in cui ogni nodo riceve segnali da altri nodi e contemporaneamente emette segnali verso altri nodi.***

→ **apprendimento automatico (ML), basato su algoritmi, ossia funzioni matematiche, che correlino un input ad un'etichetta output o classe di appartenenza**

Principali tecniche di ML		**Rischi privacy**	**Principi e referenti normativi**
Apprendimento **supervisionato** - Funzione deduttiva = ricondurre i dati non ancora noti al sistema alla regola/categoria generale nota	- Addestramento dell'algoritmo- apprendimento per errore - Fondamentale importanza di un dataset completo, con dati chiari e corretti e che non siano in nessun modo alterati - Corretta e puntuale classificazione ed etichettatura delle categorie	• Bias = interpretazione distorta delle informazioni in possesso che possa incidere sui diritti e libertà degli individui • Adeguatezza quantitativa e qualitativa del dataset di addestramento - controllo diffuso e capillare ingiustificato • Effettiva titolarità del diritto di disporre di tali dati • Scarsa chiarezza dell'ownership dei dati • Effettiva capacità dell'interessato di comprendere il trattamento a cui i propri dati sono sottoposti – intellegibilità dell'algoritmo • Difficoltà a spiegare in maniera chiara il processo di trattamento e come funziona l'algoritmo	❑ sottoposti a decisione basata su **trattamento automatizzato** (art. 22 GDPR) ❑ **Minimizzazione**: più dati ho meglio è per addestrare l'algoritmo ma questo non coincide con il principio di minimizzazione - Anonimizzazione/Pseudonimizzazione ❑ **Legittimità del trattamento** ❑ **Liceità del trattamento** ❑ **Informative complesse e scarsamente intelligibili per** soggetti con conoscenza media (Art. 13 e 14 GDPR) ❑ **Trasparenza** ❑ **Privacy by Design** ❑ **AFFIDABILITA' – Linee Guida Comm. UE per un'AI etica**
Apprendimento **non supervisionato** - Funzione induttiva = estrarre o ricavare da una serie di dati noti la regola generale non nota (fondamentale apporto dei Big Data)	- Apprendimento attraverso dati sconosciuti alla macchina, non etichettati - L'apprendimento avviene per ripetitività di fenomeni costanti o per individuazione di pattern ripetitivi o costanti nella DESCRIZIONE delle informazioni per IDENTIFICARE le CATEGORIE		



Definizione

Raccolta di dati informativi così estesa in termini di volume, velocità o varietà da richiedere tecnologie e metodi analitici specifici

(da Wikipedia)

Caratteristiche distintive dei Big Data :

→ uso di algoritmi AI

→ tendenza a collezionare «tutti i dati»

→ opacità del processo decisionale

→ riutilizzo dei dati per nuove finalità

→ uso di nuovi tipi di dati

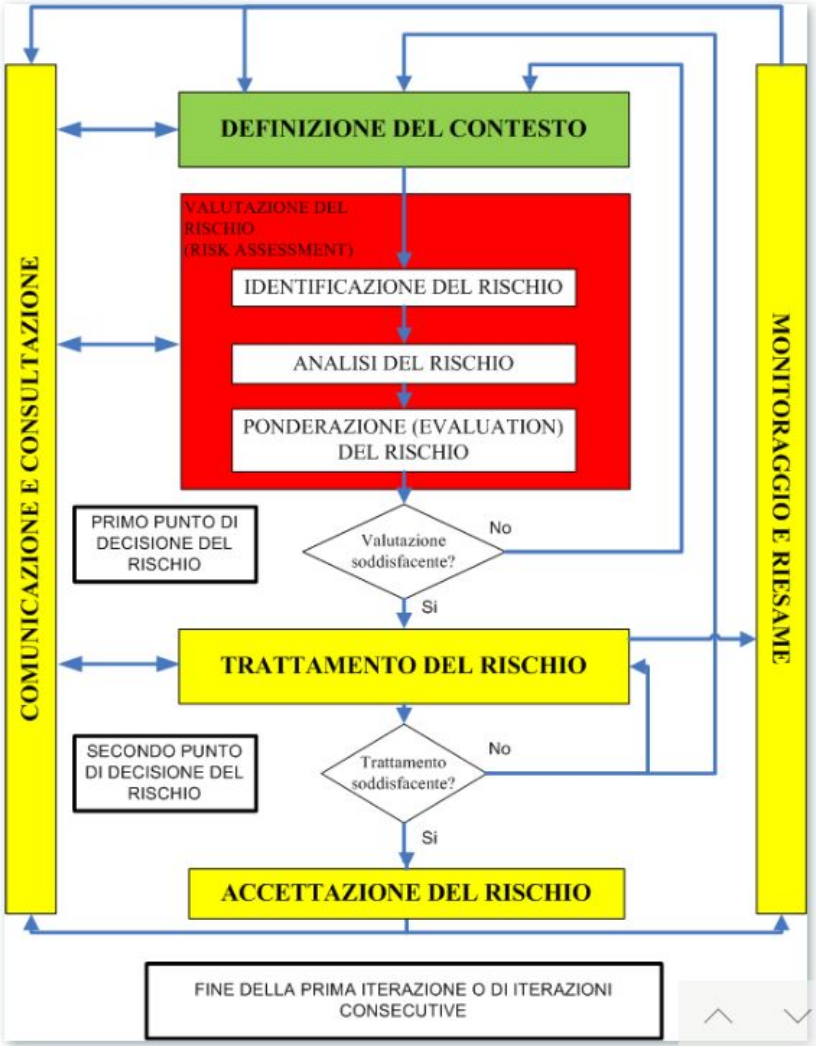
ICO, Information Commissioner's Office UK, «*Big Data, Artificial Intelligence, Machine Learning and Data Protection*»

Proprietà		Rischi privacy	Principi e referenti normativi
Uso AI (in particolare, uso di tecniche di Deep Learning (DL)) e opacità del processo decisionale	• «Black box» • Difficoltà a distinguere quando viene usata la vera tecnologia dei Big Data e quando invece si tratta di semplice possesso di una grande mole di dati	● Il livello di complessità è tale da rendere difficilissimo se non impossibile ricostruire il percorso logico svolto dalla macchina («decisioni inumane» - gap di umana comprensibilità) ● L' imprevedibilità delle inferenze e la possibilità di correlare tra loro dati potrebbe portare a far emergere connessioni capaci di risalire in maniera univoca ad un soggetto, anche se si tratta di dati anonimizzati ● L'imprevedibilità degli output può portare a non sapere con chiarezza quali siano gli effetti del trattamento	❑ trasparenza (art. 5 c. 1 lett. a) - GDPR) ❑ Vedere elenco per AI ❑ minimizzazione ❑ Limitazione delle finalità ❑ Limitazione della conservazione ❑ Liceità e legittimità del trattamento ❑ identificabilità del data controller ❑ Decisioni non esclusivamente automatizzate (art. 22 GDPR)
Uso di tutti i dati	● Anziché usare le tradizionali tecniche di analisi basate su campioni statistici più o meno rappresentativi qui si usano tutti i dati ● Dati che aumentano progressivamente	● Controllo diffuso	
Riutilizzo dei dati per nuove finalità	● I dati originariamente raccolti possono essere poi analizzati per scopi differenti o forniti ad altri soggetti per scopi differenti	● Deriva incontenibile che non consente all'interessato di disporre consapevolmente dei propri dati	
Uso di nuovi dati (dati provenienti da altre tecnologie)	● È stata proposta la distinzione tra: - Dati forniti - Dati Osservati (IoT) - Dati derivati (da altri dati con tecniche di analisi semplici) - Dati «ricostruiti» - «inferred» (con tecniche di analisi complesse e a carattere	● Vengono «rastrellati» anche online dati in modo che l'interessato ne è del tutto inconsapevole	

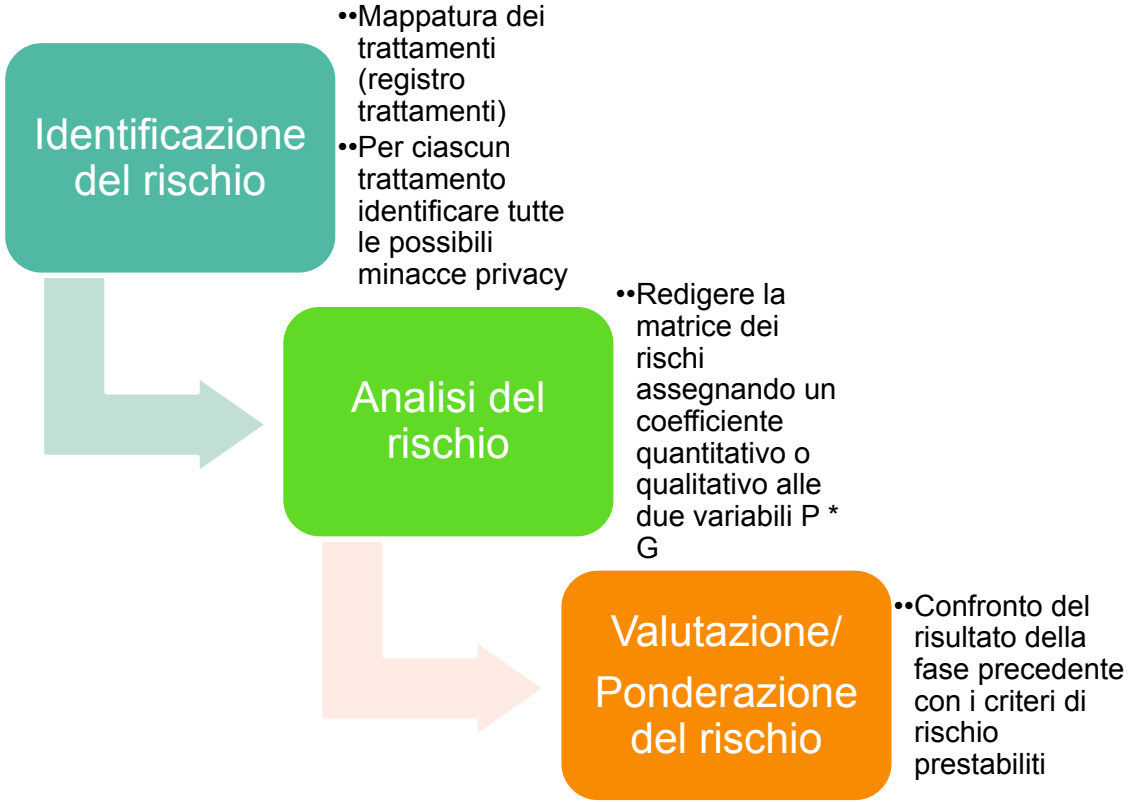
2. Rischi Privacy che dipendono dal contesto in cui le tech sono collocate e dalle modalità del loro impiego

PROCESSO DI GESTIONE DEL RISCHIO

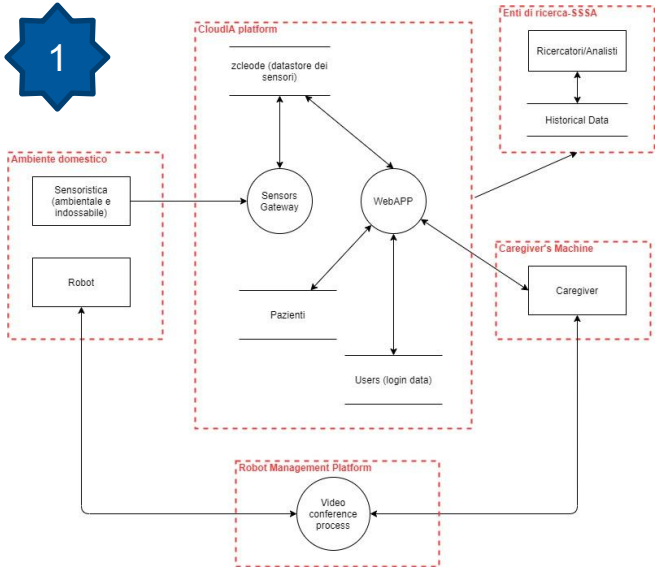
Fonte: **ISO-IEC 31000:18,** Principi e linee guida generali sulla gestione del rischio di impresa


COMUNICAZIONE E CONSULTAZIONE
DEFINIZIONE DEL CONTESTO
VALUTAZIONE DEL RISCHIO (RISK ASSESSMENT)
IDENTIFICAZIONE DEL RISCHIO
ANALISI DEL RISCHIO
PONDERAZIONE (EVALUATION) DEL RISCHIO
PRIMO PUNTO DI DECISIONE DEL RISCHIO
Valutazione soddisfacente?
No
Si
TRATTAMENTO DEL RISCHIO
SECONDO PUNTO DI DECISIONE DEL RISCHIO
Trattamento soddisfacente?
No
Si
ACCETTAZIONE DEL RISCHIO
MONITORAGGIO E RIESAME
FINE DELLA PRIMA ITERAZIONE O DI ITERAZIONI CONSECUTIVE

Parte 1- Analisi del rischio



1



DATA FLOW DIAGRAM

1

MAPPATURA DELLE MINACCE PRIVACY

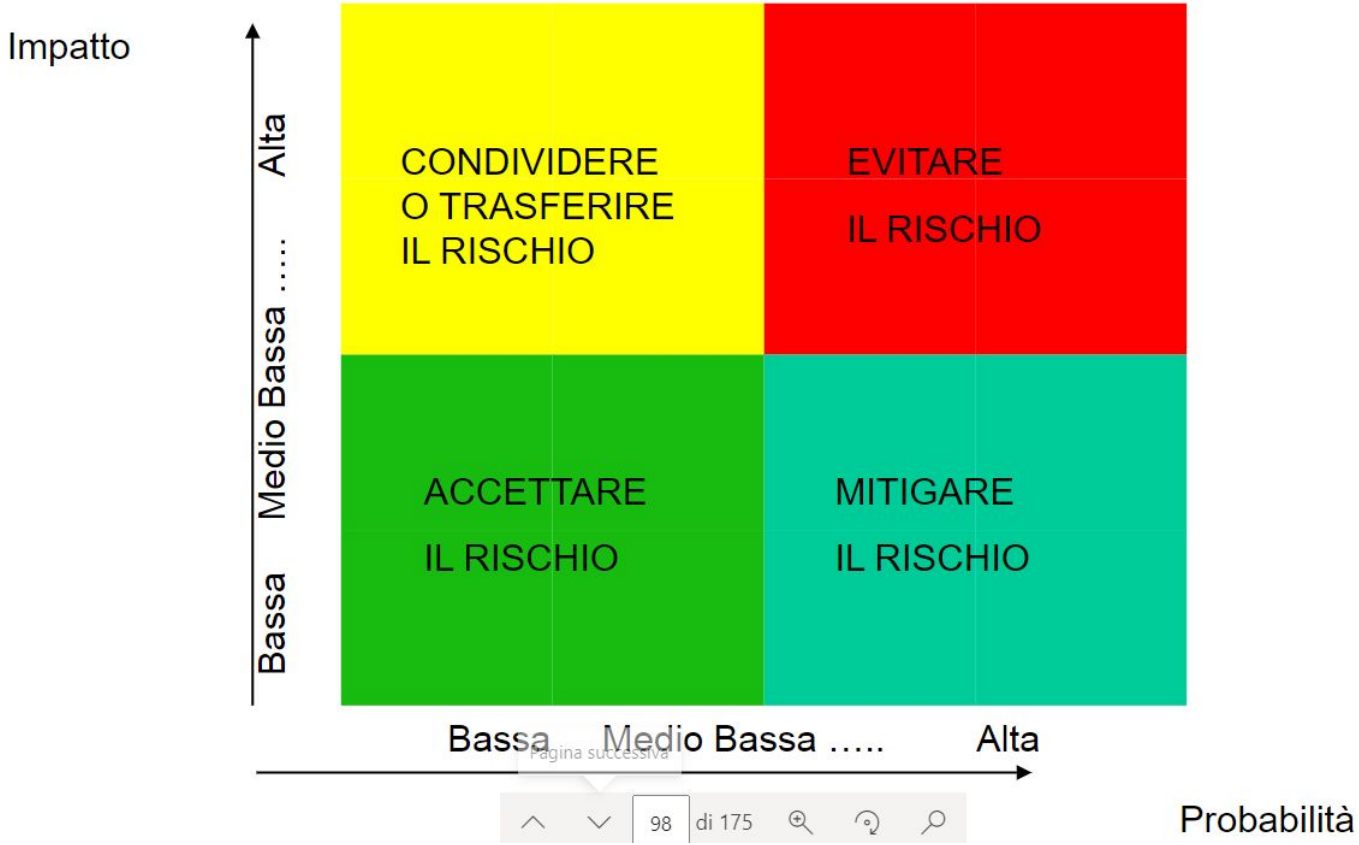
ID	LINDDUN subcategories		Minacce		
	Cod	Descrizione	Hotspot	Descrizione	Note
L5.01	L5	LINKABILITY OF SHARED DATA	Enti di ricerca	Informazioni sui pazienti potrebbero essere correlate tra loro per creare una serie di profili, anche identificativi	I dati inviati agli enti di ricerca, se non anonimizzati, potrebbero essere collegati tra loro

2

CALCOLO DEL RATING DI RISCHIO E SELEZIONE DEI RISCHI DA TRATTARE

ID	LINDDUN subcategories		Minacce			Rating		
	Cod	Descrizione	Hotspot	Descrizione	Note	Pr	Im	R
L5.01	L5	LINKABILITY OF SHARED DATA	Enti di ricerca	Informazioni sui pazienti potrebbero essere correlate tra loro per creare una serie di profili, anche identificativi	I dati inviati agli enti di ricerca, se non anonimizzati, potrebbero essere collegati tra loro	8	8	64

Parte 2- Trattamento del rischio



Pagina successiva
98 di 175

Parte 2- Riduzione del rischio attraverso l'adozione di apposite misure

ORGANIZZATIVE

MODELLO ORGANIZZATIVO PRIVACY
Referenti interni
Incaricati/autorizzati
Ads
DPO
Formazione

INFORMATIVE
Dipendenti
Sito web
Candidati
Fornitori/Consulenti
Visitatori
Videosorveglianza

CONSENSI
Marketing
Profilazione
Geolocalizzazione
Comunicazione

GESTIONE TERZE PARTI
DPA
Policy per qualificazione terze parti

GESTIONE DIRITTI INTERESSATO
Accesso, Oblio, Rettifica, Portabilità, Opposizione, Limitazione
Policy per diritti

DATA BREACH
Policy per la gestione del breach
Metodologia per la quantificazione del breach (Enisa 2013)

RISK e PRIVACY ASSESSMENT
Policy per la valutazione del rischio e dell'impatto del trattamento, necessario per determinare misure adeguate

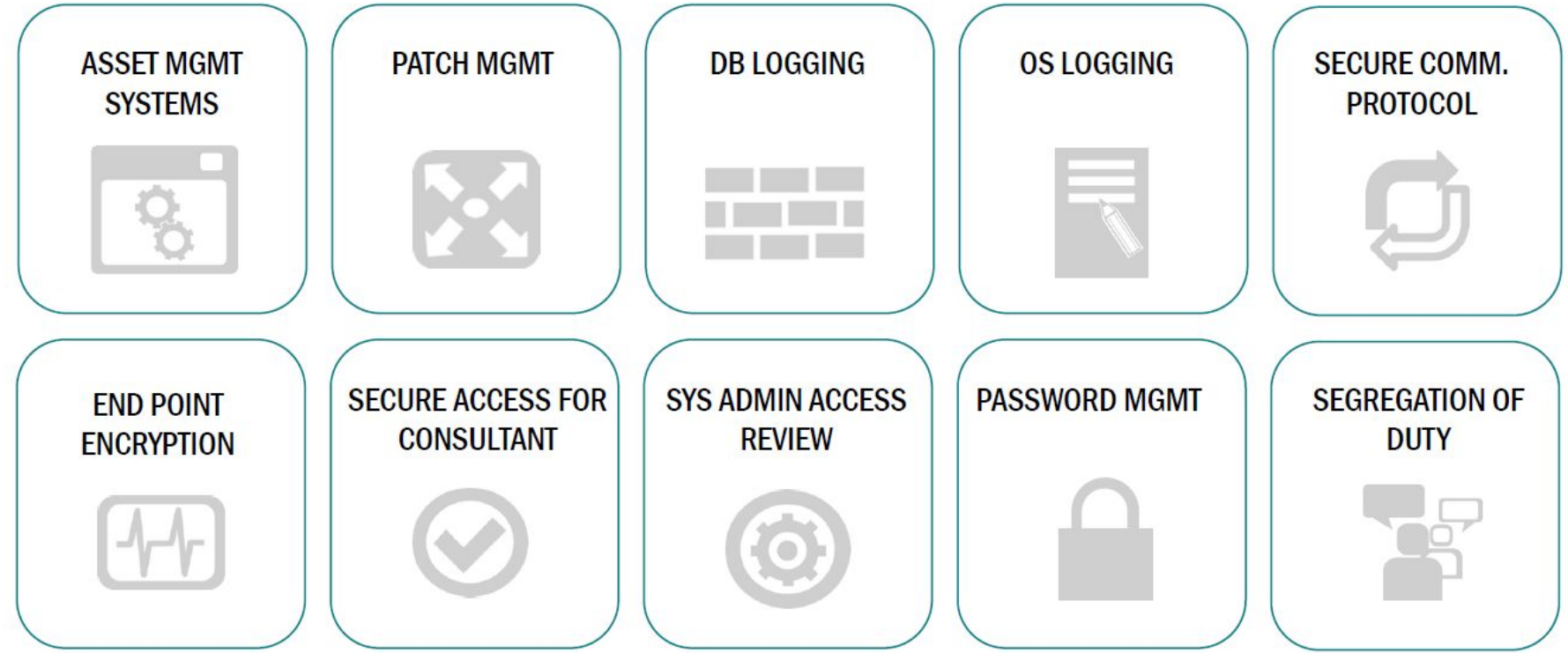
PRIVACY BY DESIGN
Policy e approccio di incorporazione della privacy a partire dalla progettazione di un processo aziendale

REGISTRI DEL TRATTAMENTO
con + 250 dipendenti
se trattamento di dati particolari (art. 9)
o rischio per libertà fondamentali (es. profilazione su larga scala)

DATA RETENTION
Policy e metodologia di data retention
Retention per dato, trattamento e sistema

Parte 2- Riduzione del rischio attraverso l'adozione di apposite misure

TECNICHE



ACCOUNTABILITY

Domande aperte

- La gestione del rischio privacy esiste già o – se così non è- come può integrarsi nei processi ordinari?
- La gestione del rischio è una funzione esistente? C'è qualche risorsa (skills personali, report già presenti) che può essere ottimizzata?
- In generale ritenete che la funzione di risk management, trasversale all'organizzazione, sia una funzione strategica anche per altri aspetti all'interno dell'organizzazione?

Cosa pensano le persone

ESERCITAZIONE

Risultato esercitazione – proposta di aggiornamento in ottica Privacy by Design del processo di erogazione di un servizio con l’uso di soluzioni tecnologiche

Da inserire

Grazie per l’attenzione!