Fondazione CRT

SOS! FCRT CYBER>> SECURITY

29 NOVEMBRE
2023
OGR TORINO

CYBERSECURITY E PRIVACY NEL TERZO SETTORE

Guida pratica per sopravvivere agli adempimenti legali ed alle sfide cyber

Avv. Luisa Di Giacomo

Presidente e founder di CyberAcademy / Data Protection Officer / Portavoce nazionale del C.N.A.C.
Componente del pool di esperti in privacy e cybersecurity presso lo European Data Protection Board

PRIMA DI TUTTO
LE PRESENTAZIONI

Laureata in giurisprudenza a pieni voti nel 2001, avvocato dal 2005, ho studiato e lavorato nel Principato di Monaco e a New York.
Mi occupo di compliance e protezione dati, nel 2016 ho conseguito il **Master come Consulente** Privacy e dal 2020 ho il titolo **Maestro per la Protezione dei Dati e Data Protection Designer** dell'Istituto Italiano per la Privacy, di cui sono diventata docente dall'anno successivo e membro del Comitato scientifico.
Dal 2022 faccio parte del pool di **consulenti esperti di Cyber Law presso lo European Data Protection Board**, e sono stata nominata **Portavoce Nazionale del CNAC, Centro Nazionale Anti Cyberbullismo.** Sono docente e autrice per Maggioli e Giuffré, coordino la sezione Cybersecurity della pagina diritto.it e sono **legal** influencer, con oltre 150.000 follower tra Instagram e TikTok.
Sono **Data Protection Officer** e consulente per la protezione e sicurezza dei Dati in numerose società nel nord Italia, Presidente e founder di ***CyberAcademy***, la Business School per la formazione dei legali del futuro.

Mi piace definirmi Cyberavvocato

A ME NON INTERESSA LA PRIVACY, TANTO NON HO NIENTE DA NASCONDERE...

PRIVACY VS PROTEZIONE DEI DATI

Il linguaggio che usiamo dà forma ai nostri pensieri. I pensieri danno forma alle nostre azioni. Privacy e protezione dei dati sono due facce della stesa medaglia

>> ACCOUNTABILITY

Approccio basato sul rischio.

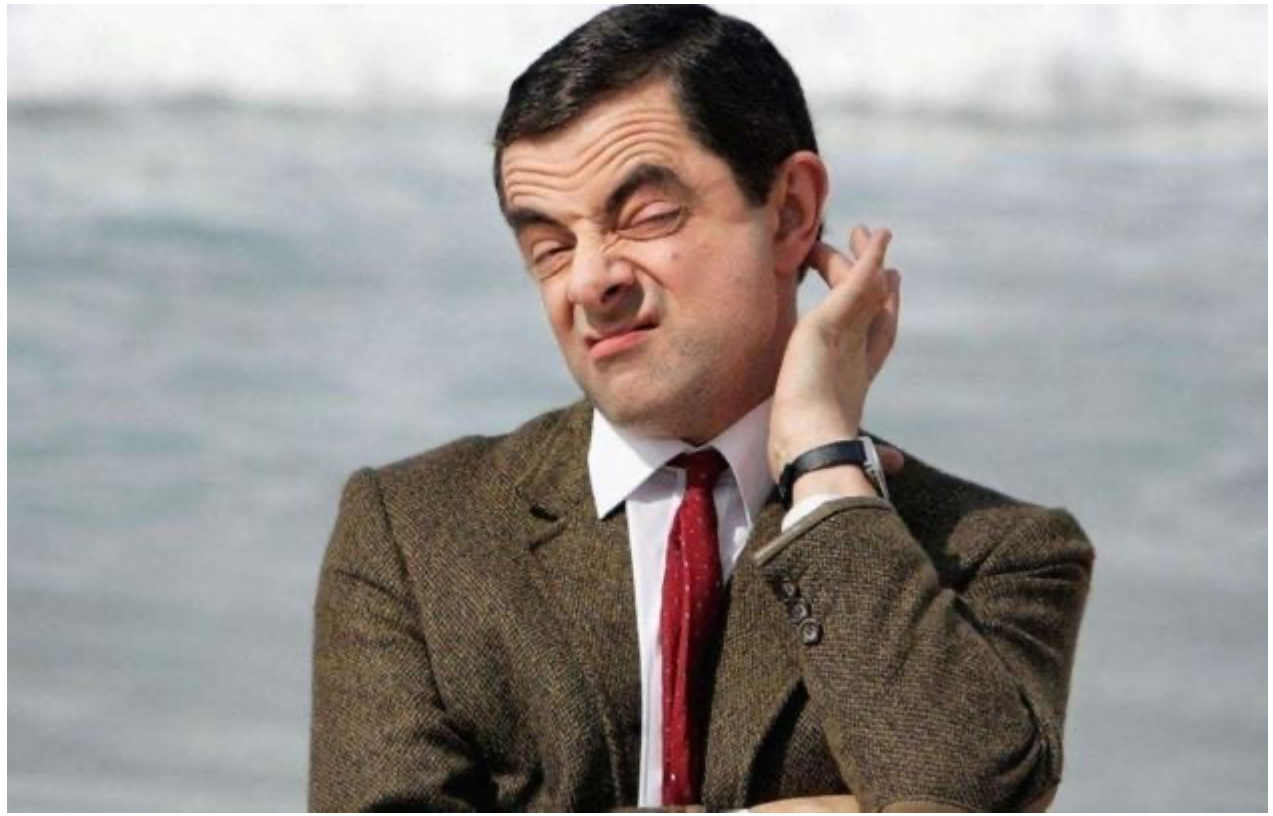
>> DATA PROTECTION BY DESIGN

Protezione dei dati fin dalla progettazione.

>> DATA PROTECTION BY DEFAULT

Protezione dei dati per impostazione predefinita.

MA...
CHE COSA SIGNIFICA
TUTTO QUESTO
IN PRATICA?



«POSSO DIRE CHE FACCIO MOLTI PIÙ DANNI IO, CON IL MIO PORTATILE, IN PIGIAMA, DAVANTI ALLA PRIMA TAZZA DI EARL GREY, DI QUANTI NE FACCIA TU IN UN ANNO SUL CAMPO»

Q a 007, Skyfall, 2012

ADEGUAMENTO:
COME E PERCHÉ FARLO?

1

SICUREZZA
INFORMATICA

2

DOCUMENTI

3

PROCEDURE

4

DANNI
ECONOMICI

5

DANNI
REPUTAZIONALI

6

BUSINESS
CONTINUITY

IL NEMICO NUMERO UNO: LA MENTALITÀ

Abbiamo sempre fatto così

SE VUOI OTTENERE RISULTATI DIVERSI

Non fare sempre le stesse cose

DA GRANDI DATA BASE

DERIVANO GRANDI RESPONSABILITÀ

I NUMERI DEL CYBERCRIME

22T USD

20T USD

10T USD

Il valore economico dei dati

Doxing: diffusione pubblica di dati online senza il consenso dell'utente e la successiva vendita dei dati tramite il dark web
Dati identificativi: costo compreso tra 40 centesimi e 8 euro. In questa categoria di dati rientrano il nome completo, il codice fiscale, la data di nascita, l'indirizzo e-mail e il numero di cellulare
Selfie con documento: (passaporto o patente) vale tra 33 e 50 euro
Scansione passaporto: tra 4 e 13 euro.
Scansione patente: tra 4 e 21 euro
Dati del contocorrente: sono venduti sul dark web a circa 1/10% del suo valore.
Account Paypal: tra 42 e 418 euro.
Dettagli carta di credito: dai 5 ai 16 euro.
Dati di accesso servizi in abbonamento: tra 40 centesimi e 7 euro.

Fonte: Kaspersky

I DIVERSI TIPI DI ATTACCO INFORMATICO (DATA BREACH)

Il **Phishing** è uno degli attacchi informatici più comuni e consiste nell'invio di comunicazioni fraudolente (email, SMS, chiamate) con l'obiettivo di ottenere informazioni sensibili (credenziali d'accesso, dati di pagamento) o di installare un malware sul dispositivo del destinatario della comunicazione ed esfiltrare dati sensibili.

Il termine **Malware** racchiude diversi tipi di software malevoli (es. Ransomware, Spyware, Virus).
Il malware sfrutta le vulnerabilità della rete per violarla attraverso un allegato malevolo a una e-mail o un link pericoloso.

Dos: Questo tipo di attacco ha come obiettivo creare un disservizio del sistema target inviando anomali flussi di traffico. Di conseguenza, il sistema attaccato non è più in grado di soddisfare le richieste legittime e garantire le funzioni operative che ne consentono il corretto funzionamento.
Distributed Denial of Service (DDoS).

ALTRI TIPI COMUNI DI ATTACCO

SQL INJECTION

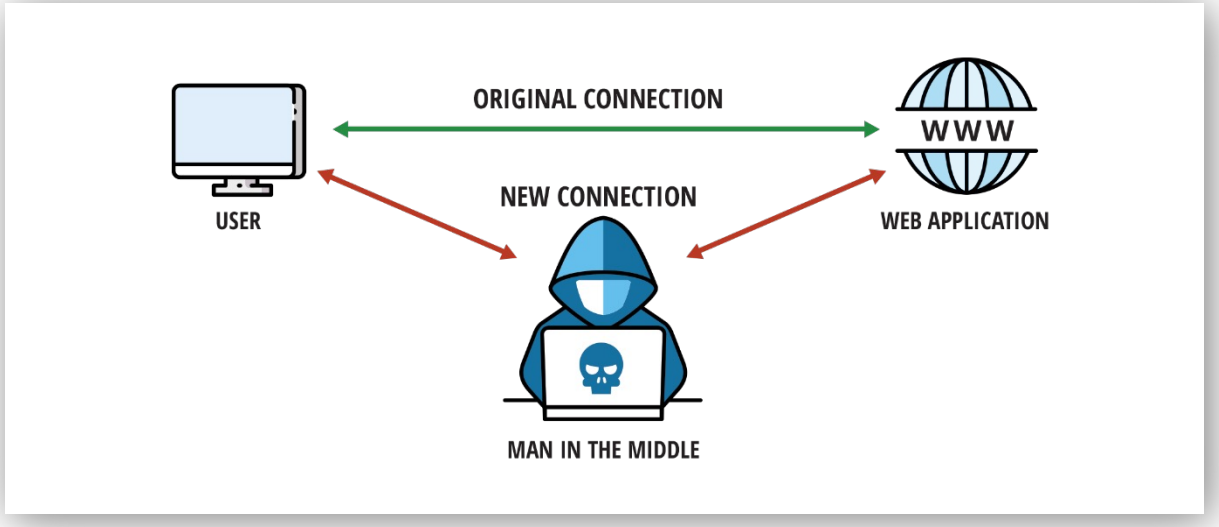
Una Structured Query Language Injection è una tecnica di injection di codice che si verifica quando l'attaccante aggiunge una porzione di codice malevolo in un server che utilizza linguaggio SQL.
L'obiettivo di questa tipologia di attacco è la pubblicazione di informazioni che dovrebbero rimanere confidenziali.

ZERO DAY

Un attacco viene definito zero-day quando si verifica non appena viene scoperta una vulnerabilità zero-day prima che sia possibile implementare patch o azioni di rimedio.
Il metodo exploit zero-day viene utilizzato dagli attaccanti per targetizzare i sistemi con vulnerabilità ancora non identificate.

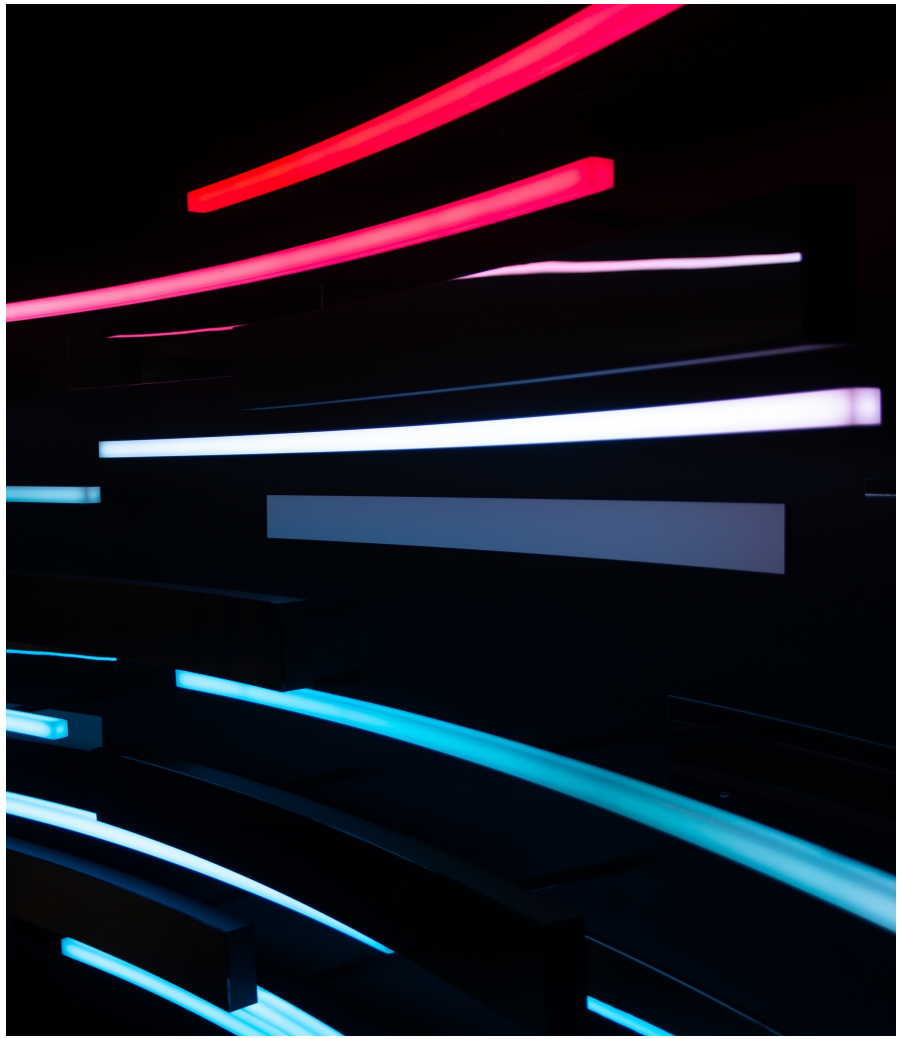
SOCIAL ENGINEERING

Manipolazione psicologica della vittima per portarla a compiere errori e ottenere informazioni sensibili.
L'attaccante inizialmente studia e osserva la vittima e le sue abitudini
Successivamente, agisce in modo da ottenere la fiducia della vittima per convincerla a condividere informazioni sensibili



ATTACCO MAN IN THE MIDDLE

Il MitM è un esempio di attacco di intercettazione in cui l'attaccante (nella maggior parte dei casi attraverso reti Wi-Fi pubbliche non sicure) si inserisce in una connessione tra due parti esfiltrando dati ed informazioni.



DATA BREACH: PERDITA DI RISERVATEZZA,CONFIDENZIALITÀ, INTEGRITÀ DEI DATI

Il rischio zero non esiste... ma ci sono molte cose che si possono fare per evitare un attacco.

Domanda frequente: ma figurati se vengono proprio ad attaccare me...

RAPPORTO CLUSIT 2022

Nel 2022 si sono registrati più attacchi cyber, oltretutto la maggior parte gravi o gravissimi, con un aumento del 21 per cento nel mondo rispetto all'anno precedente.
In Italia l'aumento è stato del 169 per cento.
2022 anno peggiore di sempre sul fronte della sicurezza informatica.

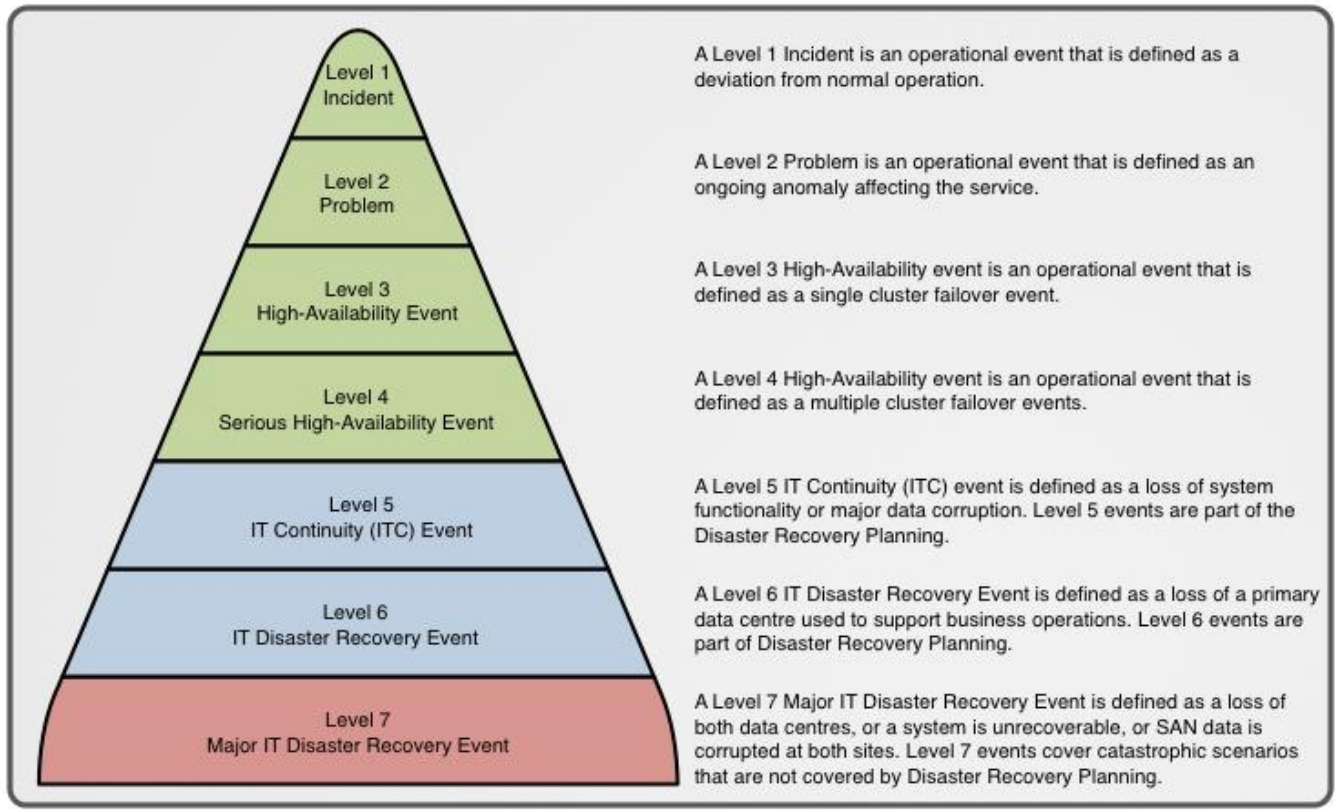
80%

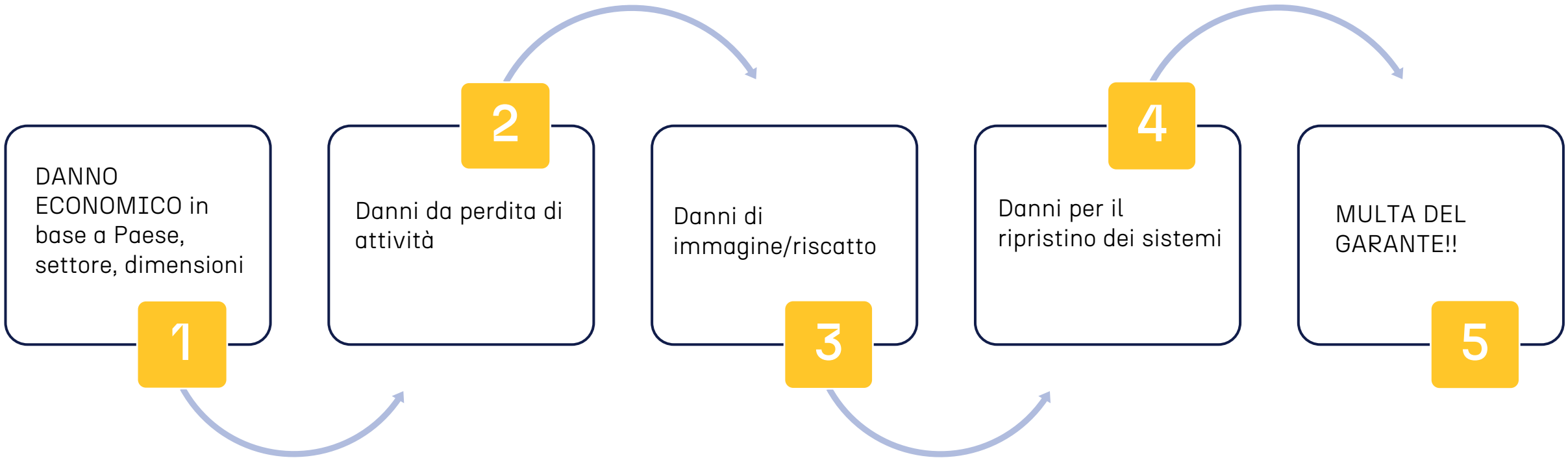
DEGLI ATTACCHI COMPLESSIVI HA
AVUTO UN IMPATTO MOLTO ELEVATO
(Severe high o critical impact)

8%

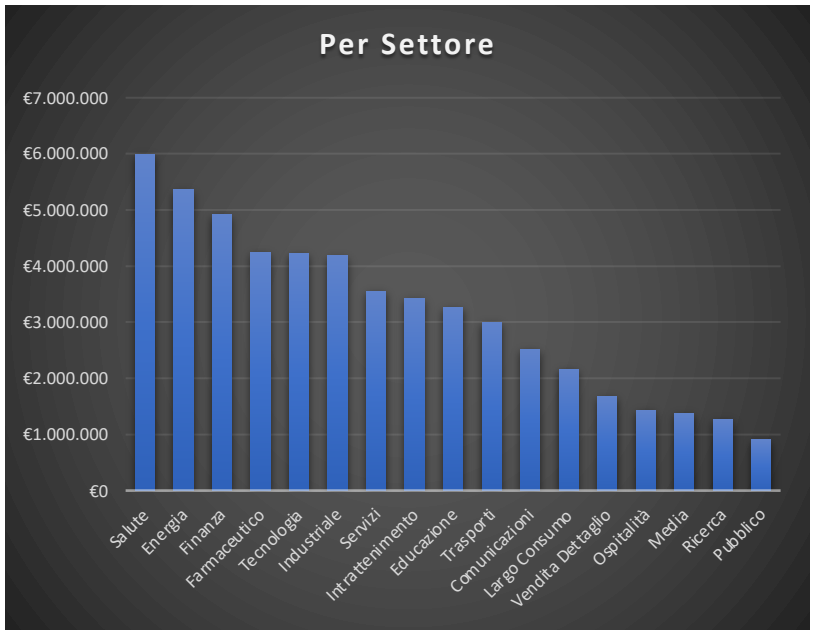
DEGLI ATTACCHI MONDIALI
AVVIENE IN ITALIA
(poco meno di 300 attacchi al mese).

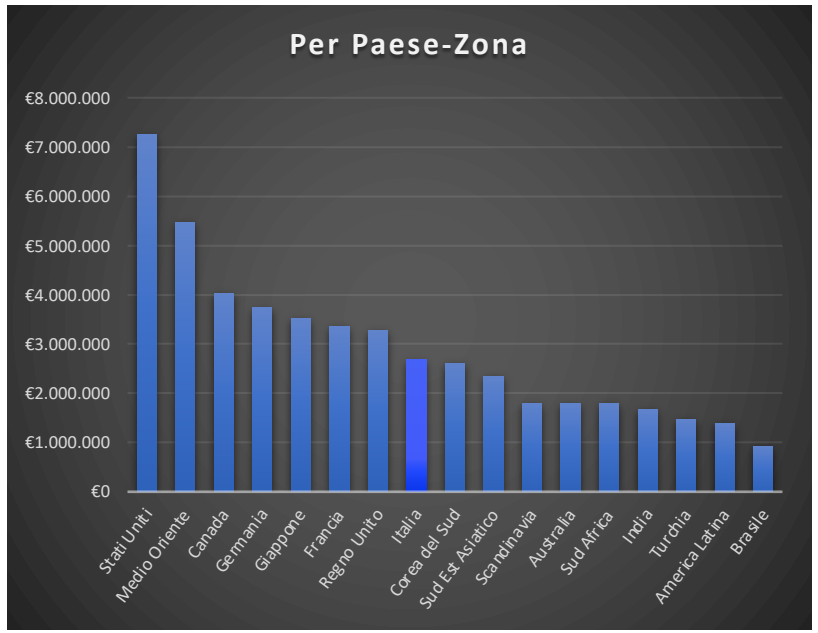
>>

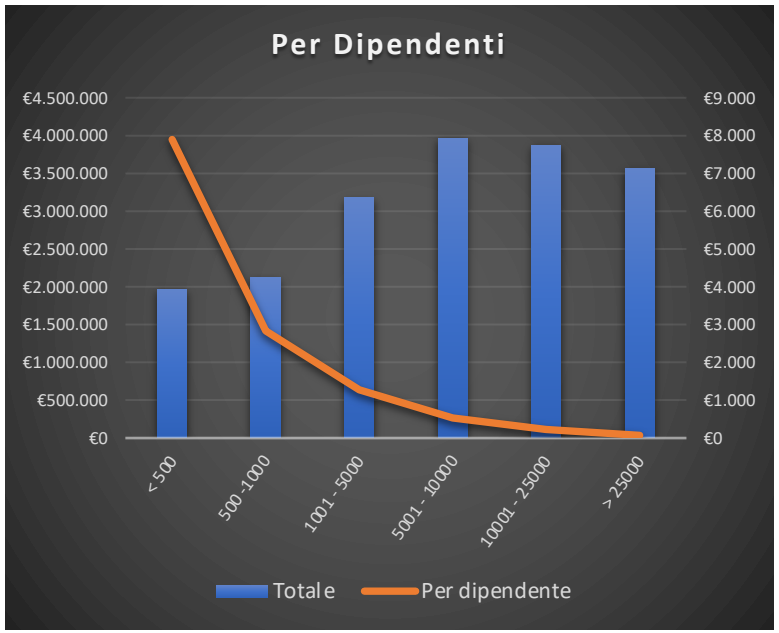

Level 1
Incident
Level 2
Problem
Level 3
High-Availability Event
Level 4
Serious High-Availability Event
Level 5
IT Continuity (ITC) Event
Level 6
IT Disaster Recovery Event
Level 7
Major IT Disaster Recovery Event
A Level 1 Incident is an operational event that is defined as a deviation from normal operation.
A Level 2 Problem is an operational event that is defined as an ongoing anomaly affecting the service.
A Level 3 High-Availability event is an operational event that is defined as a single cluster failover event.
A Level 4 High-Availability event is an operational event that is defined as a multiple cluster failover events.
A Level 5 IT Continuity (ITC) event is defined as a loss of system functionality or major data corruption. Level 5 events are part of the Disaster Recovery Planning.
A Level 6 IT Disaster Recovery Event is defined as a loss of a primary data centre used to support business operations. Level 6 events are part of Disaster Recovery Planning.
A Level 7 Major IT Disaster Recovery Event is defined as a loss of both data centres, or a system is unrecoverable, or SAN data is corrupted at both sites. Level 7 events cover catastrophic scenarios that are not covered by Disaster Recovery Planning.


DANNO ECONOMICO in base a Paese, settore, dimensioni
1
Danni da perdita di attività
2
Danni di immagine/riscatto
3
Danni per il ripristino dei sistemi
4
MULTA DEL GARANTE!!
5

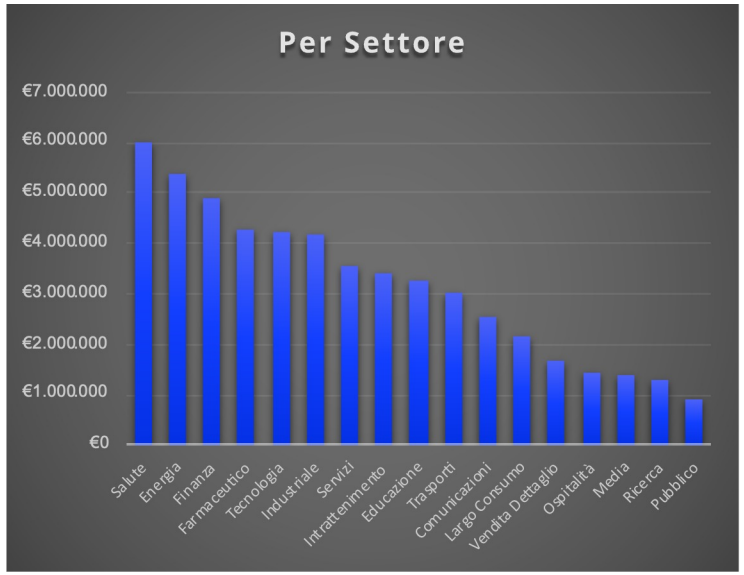
CALCOLO DEL DANNO ECONOMICO

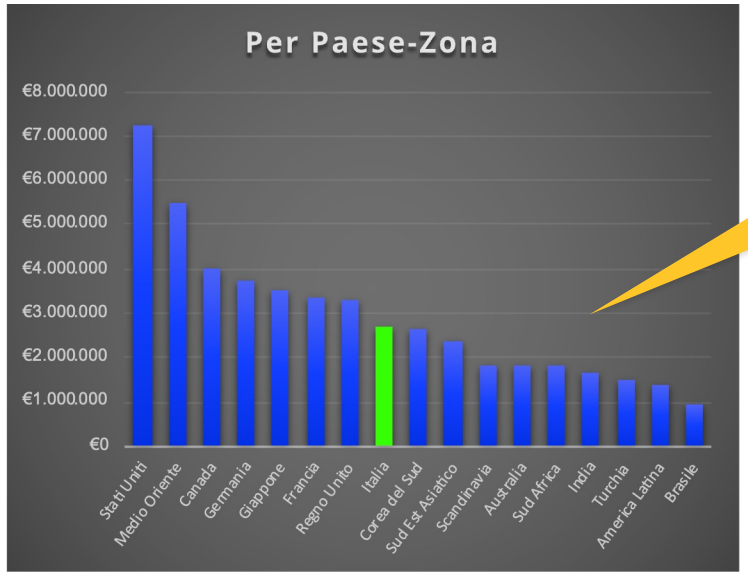




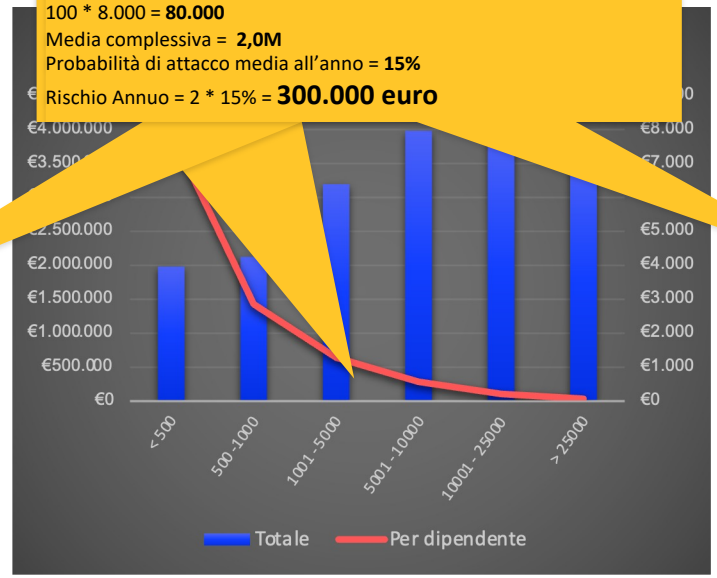


CALCOLO DEL DANNO ECONOMICO





Settore = **3,5M+**
Paese = **2,8M**
Dimensione = **1,9M+** e **8.000** per dipendente
100 * 8.000 = **80.000**
Media complessiva = **2,0M**
Probabilità di attacco media all'anno = **15%**
Rischio Annuo = 2 * 15% = **300.000 euro**



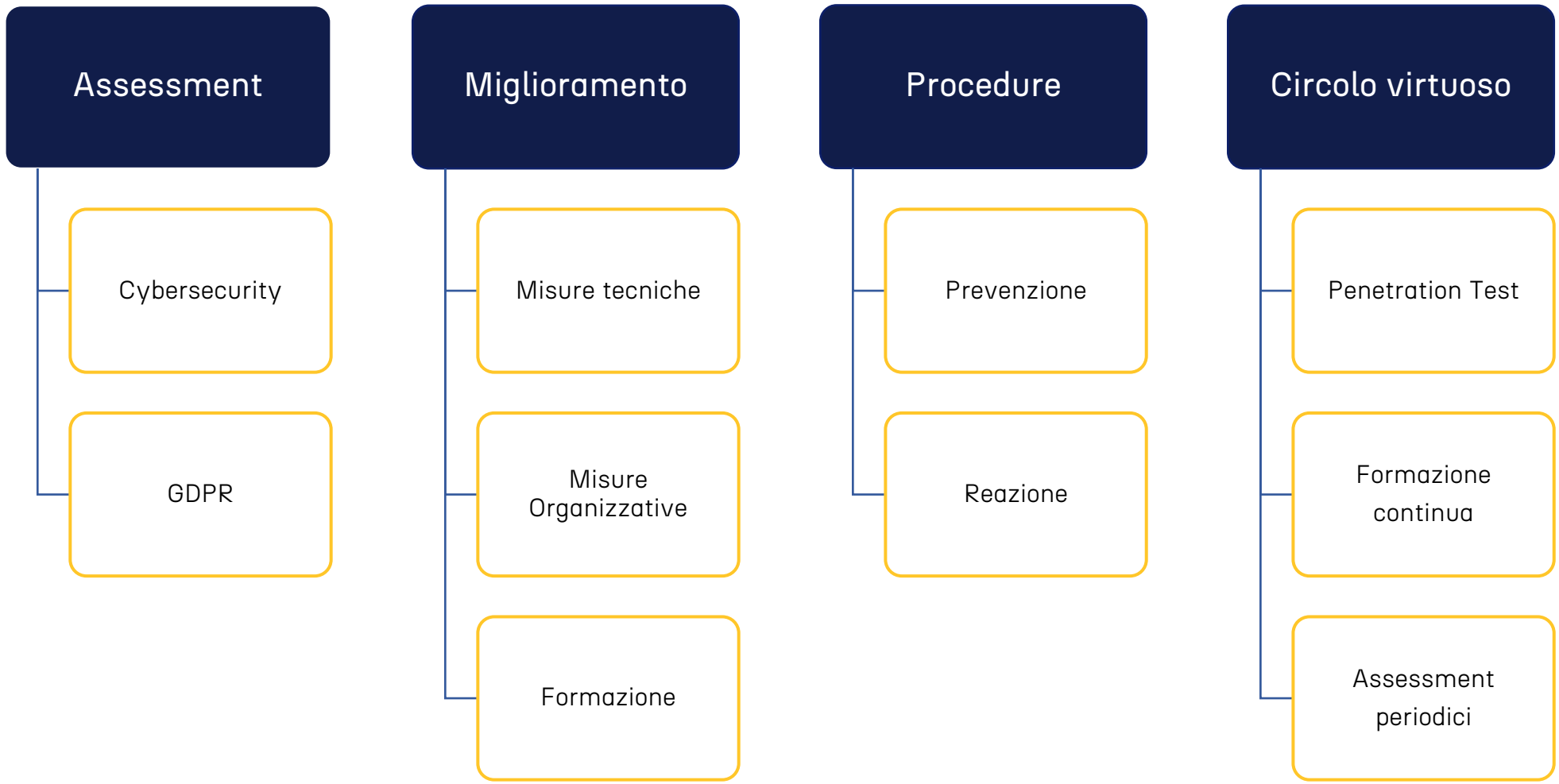
ATTACCHI CELEBRI

Italia	F**ckUnicorn	Ransomware che ha sfruttato la pubblicazione della app Immuni per diffondersi attraverso un sito fake.	Ransomware	Ignoto	300 Euro a vittima
GEOX	Ignoto	Nel giugno 2020 Geox ha subito un attacco di successo che ha bloccato per due giorni i server di posta interna con conseguente blocco di alcune delle attività aziendali	Ransomware	Ignoto	Ignoto
ENEL	Netwalker	In ottobre 2020 un attacco di successo ha sottratto dati relativi a diverse centrali elettriche.	Ransomware	5 Tb	14M Euro
Luxottica	Ignoto	Nel settembre 2020 Luxottica ha subito un attacco che ha sfruttato la vulnerabilità di una appliance di rete. Il tutto ha causato il blocco temporaneo della produzione.	Malware/Vulnerabilità	Ignoto	N/A
Campari	Ragnar-Locker	Nel settembre 2020 un ransomware ha compromesso i dati di circa 4700 dipendenti e consulenti.	Ransomware	2 Tb	15M USD
Ospedale S.Giovanni, Roma	Ignoto	L'attacco ha bloccato tutti i computer della struttura obbligando per giorni tutti i dipendenti a lavorare con carta e penna.	Ransomware	Ignoto	Ignoto
SIAE	Everest	Furto di dati personali, documenti d'identità, opere.	Phshing/Ransomware	60 Tb	3M Euro
Regione Lazio	Ignoto	Attacco avvenuto nel Luglio 2021 che ha bloccato per un mese molti dei servizi della sanità regionale.	Ransomware	Cartelle sanitarie, Green Pass, etc.	5M euro

I SOGGETTI IN UN DATA BREACH

«LE CONTROMISURE, FINO A QUEL PUNTO,
SI LIMITAVANO ALL'INVE(N)TTIVA»

F. De André, Bocca di Rosa, 1967


Assessment
Cybersecurity
GDPR
Miglioramento
Misure tecniche
Misure Organizzative
Formazione
Procedure
Prevenzione
Reazione
Circolo virtuoso
Penetration Test
Formazione continua
Assessment periodici

E PER CONCLUDERE

«Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire».

Edward Snowden, 2019

Avv. Luisa Di Giacomo

C.so Vittorio Emanuele II, n.76
digiacomo@luisadigiacomo.it
347.5379522
Linkedin: https://www.linkedin.com/in/luisa-di-giacomo-cyberavvocato

SOS! FCRT CYBER>> SECURITY