Ciclo di webinar in diretta

Sicurezza informatica & Protezione dei dati negli enti locali

Il Data Breach negli enti locali. Tecniche di prevenzione e strumenti di notifica all'autorità garante di un ente locale 11-01-2024

Relatore: Dottor Antonio Guzzo Funzionario Informatico Agenzia delle Entrate

Cyber security expert

DPO CERTIFIED ISO IEC 17024 e UNI 11697:2017

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54 (int.3)
Web: www.dpoinrete.it, www.asmel.eu

Indice

- **Definizione di data Breach**
- **L’obbligo di notifica**
- **La comunicazione di data breach art. 34**
- **Indagini forensi e data breach**
- **Illeciti e sanzioni**
- **Le linee guida EDB del 14-01-2021**
- **Il case study del Comune di Pisticci (MT)**
- **Considerazioni finali**

IL COSTO MEDIO GLOBALE DI UNA VIOLAZIONE

È doveroso ricordare che i dati vanno altresì protetti, considerando che secondo l' "*IBM Cost of a Data Breach Report 2023*", il costo medio globale di una violazione dei dati nel 2023 è stato di 4,45 milioni di dollari, il 15% in più rispetto al 2020.

4,45 milioni di dollari

Il costo medio globale di una violazione dei dati nel 2023 è stato di 4,45 milioni di dollari, con un aumento del 15% in 3 anni.

51%

Il 51% delle organizzazioni prevede di aumentare gli investimenti in sicurezza a seguito di una violazione, compresa la pianificazione e i test di risposta agli incidenti (IR), la formazione dei dipendenti e gli strumenti di rilevamento e risposta alle minacce.

1,76 milioni di dollari

Il risparmio medio per le organizzazioni che utilizzano ampiamente l'intelligenza artificiale e l'automazione per la sicurezza è di 1,76 milioni di dollari rispetto alle organizzazioni che non lo fanno.

Fonte dati IBM Cost of a Data Breach Report 2023

ALCUNI DATI FINANZIARI I° SEMESTRE 2023

LE FRODI INFORMATICHE E MONETICA Primo semestre 2023	
Frodi Informatiche (Ril. nazionale)	5.354
Persone indagate	388
Somme sottratte	€ 21.536.551

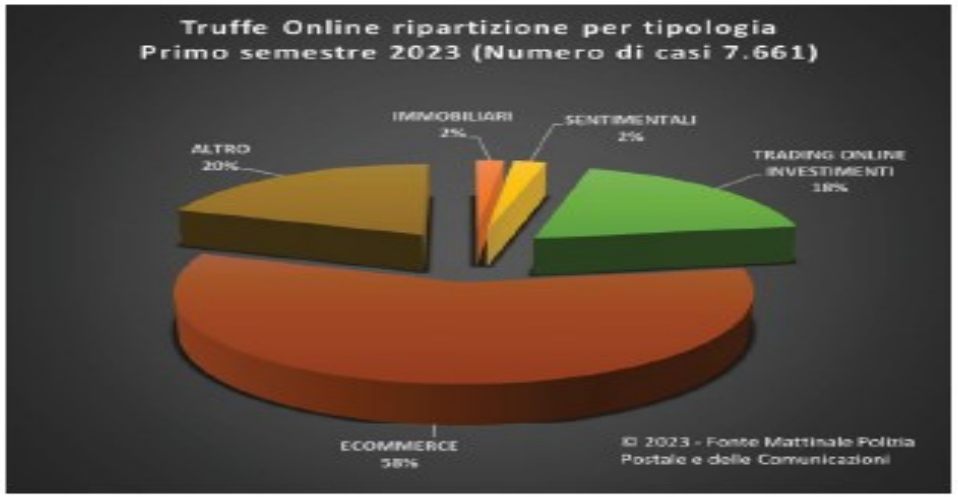
ALCUNI DATI FINANZIARI I° SEMESTRE 2023

TRUFFE ONLINE

Report relativo alle truffe online
Periodo: 01/01/2023 – 30/06/2023

		IMPORTI SOTTRATTI	
IMMOBILIARI	CASI TOTALI 7.661	158.974 €	PERSONE INDAGATE 1.853
SENTIMENTALI ROMANCE SCAM		3.460.589 €	
TRADING ONLINE		44.905.283 €	
E COMMERCE		4.606.297 €	
ALTRO		5.122.424 €	
		TOTALE 58.253.567 €	

© 2023 - Fonte Mattinale Polizia Postale e delle Comunicazioni



IL DATA BREACH

- Per DATA BREACH, nella versione italiana **violazione dei dati personali** (art. .12 GDPR) si intende la **violazione di sicurezza** che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- La notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato

IL DATA BREACH- NOTIFICA

- - L'articolo 33 GDPR ha introdotto l'obbligo generalizzato, in capo al titolare del trattamento di notifica di DATA BREACH all'autorità di controllo (DPA) competente a norma dell'art. 55 GDPR e ss., ovvero l'Autorità di controllo dello stabilimento principale o dello stabilimento unico del Titolare interessato dalla violazione o quello ove vi siano gli interessati alla violazione
- - Le informazioni minime da inserire nella notifica sono incluse nell'art. 33, la DPA competente fornirà una modulistica on line richiedendo informazioni obbligatorie. Tale documentazione consente all'Autorità di controllo di verificare il rispetto delle prescrizioni.
- - in Italia prima dell'approvazione del Regolamento erano già presenti obblighi di notifica in 4 fattispecie di trattamento:
  - Settore comunicazioni elettroniche (Prov. Garante 161/2013)
  - Biometria (Provv. Garante 513/2014)
  - Dati sanitari inseriti in Dossier (Provv. Garante 331/2015)
  - Dati comunicati fra PA (Provv. Garante 393/2015)

IL DATA BREACH- NOTIFICA

- La **notifica** deve:
  - descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni
  - descrivere le probabili conseguenze delle violazioni dei dati personali
  - descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, per attenuarne i possibili effetti negativi.

IL DATA BREACH- COMUNICAZIONE

- **La comunicazione di DATA BREACH art. 34**

- **Comunicazione di una violazione dei dati personali all'interessato**
- Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione

IL DATA BREACH- COMUNICAZIONE

- Non è richiesta la comunicazione all'interessato se:
- ✓ il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura.
- ✓ Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
- ✓ Detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura simile

IL DATA BREACH- NOTIFICA E COMUNICAZIONE DSE

- **NOTIFICA DI DATA BREACH NEL DOSSIER SANITARIO SECONDO LE LINEE GUIDA IN MATERIA DI DSE 4 GIUGNO 2015**
- **Comunicazione al Garante Privacy di una violazione dei dati personali o di incidenti informatici che, pur non avendo impatto diretto sui dati stessi, possono esporli a rischi di violazione**
- Quando la violazione dei dati personali da parte degli incaricati o qualsiasi altro soggetto rischierà di pregiudicare i dati personali p di attentare alla vita privata dell'interessata, il Responsabile del trattamento provvederà alla notificazione all'Autorità Garante e successivamente dovrà provvedere senza ingiustificato ritardo alla comunicazione di quanto avvenuto all'interessato

IL DATA BREACH- NOTIFICA E COMUNICAZIONE DSE

- **NOTIFICA DI DATA BREACH NEL DOSSIER SANITARIO**
- Comunicazione all'interessato
- Il titolare deve comunicare senza ritardo all'interessato le operazioni di trattamento illecito effettuate agli incaricati o da chiunque sui dati personali mediante il relativo Dossier
- I termini per la comunicazione sono:
  1. Riscontro da parte del Titolare o incaricato entro 15 giorni dal ricevimento della richiesta dell'interessato
  2. Se ricorre un giustificato motivo il Titolare o l'incaricato devono comunicarlo all'interessato e il termine per l'integrale riscontro è di 30 giorni

IL DATA BREACH- NOTIFICA E COMUNICAZIONE DSE

- NOTIFICA DI DATA BREACH NEL DOSSIER SANITARIO
- **Comunicazione al Garante Privacy**

- Entro **48 ore** dalla conoscenza del fatto, i Titolari devono comunicare all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati attraverso il Dossier Sanitario

IL DATA BREACH- LA GESTIONE

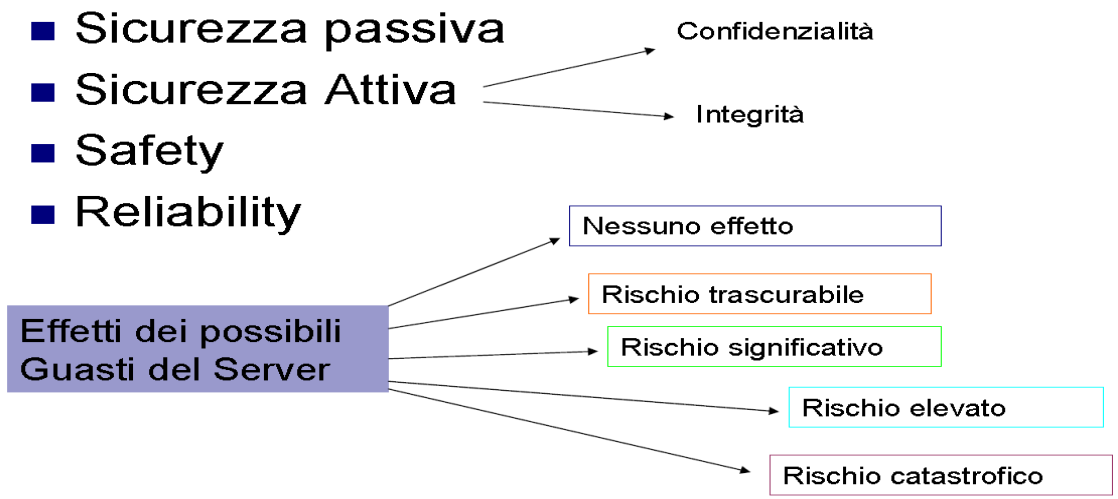
- **Per prevenire, gestire e risolvere episodi di perdita e/o distruzione dei dati personali è necessario:**
- Adottare un protocollo di risposta.
- Effettuare test periodici per controllare la validità del protocollo
- Ottenere una copertura assicurativa per eventuali casi di Data Breach
- Tenere un registro dei casi di Data Breach
- Compiere attività di indagine per individuare la natura e la portata della violazione

IL DATA BREACH- IL PROTOCOLLO DI RISPOSTA

- Il Titolare del trattamento deve adottare un protocollo di risposta, ossia procedure da seguire per gestire e risolvere eventuali episodi di distruzione e/o perdita di dati. L'adozione del protocollo coinvolge numerose dipartimenti aziendali e strutture pubbliche quali Ministeri, Asp, etc
- Questo protocollo dovrà indicare un modo coerente, sistematico e proattivo per gestire questi incidenti che coinvolgono i dati personali. Per la soluzione di questi incidenti l'azienda/ente pubblico potrà farsi coadiuvare da terzi fornitori di servizi quali:
  - Call center
  - Servizi di assistenza agli utenti e pubbliche relazioni
  - Sistemi di monitoraggio
  - Sistemi di risoluzione dei casi di furto di identità

La sicurezza informatica vs Data Breach

- Al fine di prevenire un violazione di data Breach è necessario utilizzare un modello di sicurezza informatica cosi strutturato



Altri strumenti di prevenzione

- SVILUPPO E MANUTENZIONE DI SISTEMI (System Development and Maintenance)
- Accertare che la sicurezza sia stata costruita all'interno delle operazioni di sistema;
- impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione;
- proteggere la riservatezza l'autenticità e l'integrità delle in formazioni;
- accertarsi che le attività di progetto e supporto alle attività siano condotte in modo sicuro e per mantenere la sicurezza del software e dei dati del sistema

IL DATA BREACH- LA GESTIONE

- Il titolare del trattamento o il responsabile privacy o DPO di strutture sanitarie- PA- fornitori di servizi di comunicazione elettronica – biometria deve elaborare un protocollo di risposta che assicuri la tempestiva notifica all'Autorità Garante in caso di episodi di Data Breach
- Esistono vari modelli di notifica di Data Breach disponibili sul portale istituzionale dell'autorità Garante

IL DATA BREACH- LA GESTIONE

- EFFETTUARE TEST PERIODICI

- E’ importante condurre regolarmente dei test di verifica del protocollo adottato per garantire che le procedure seguite dall’Azienda per prevenire e risolvere casi di Data Breach siano efficienti e condotte da personale formato adeguatamente per implementare il protocollo
- E’ importante stipulare un’adeguata polizza assicurativa per assicurare l’Azienda contro il rischio di Data Breach ed ottenere indennizzo dalla Compagnia Assicuratrice in occorrenza di violazioni di dati. L’assicurazione risarcisce i costi che l’Azienda deve sostenere per riparare le conseguenze della violazione e può anche coprire le eventuali spese legali che l’Azienda dovrà affrontare.

IL DATA BREACH- LA GESTIONE

- **TENERE UN REGISTRO DI DATA BREACH**

- Il DPO deve promuovere la tenuta di un Registro dei casi di Data Breach, sia dei casi di violazione effettivamente occorsi sia le minacce potenziali, per identificare il tipo e la natura delle violazioni più ricorrenti

IL DATA BREACH- LA GESTIONE

- **TRACCIARE I CASI DI DATA BREACH**

- Il tracciamento dei casi di violazione dei dati personali viene effettuato allo scopo di:
  - individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali
  - Misurare l'efficacia delle policy e delle procedure adottate
  - Elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere "compliance" rispetto a leggi, best practices, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test

IL DATA BREACH- LA GESTIONE

- INDAGINI FORENSI E DATA BREACH

- Per gestire e risolvere i casi di Data Breach l'azienda/ente pubblico può stabilire al suo interno una funzione investigativa e demandare a personale interno indagini forensi "in house"
- Siglare contratti con investigatori esterni ai quali demandare queste attività di indagine
  - Compiere attività di indagine per individuare la natura e la portata della violazione

IL DATA BREACH- INDAGINI FORENSI

- INDAGINI FORENSI E DATA BREACH

- Le indagini investigative servono per:
  - Determinare la natura e la portata della violazione
  - Aiutare a prevenire ulteriori perdite di dati
  - Conservare le prove della violazione in modo che possano essere usate anche in un’eventuale azione giudiziaria

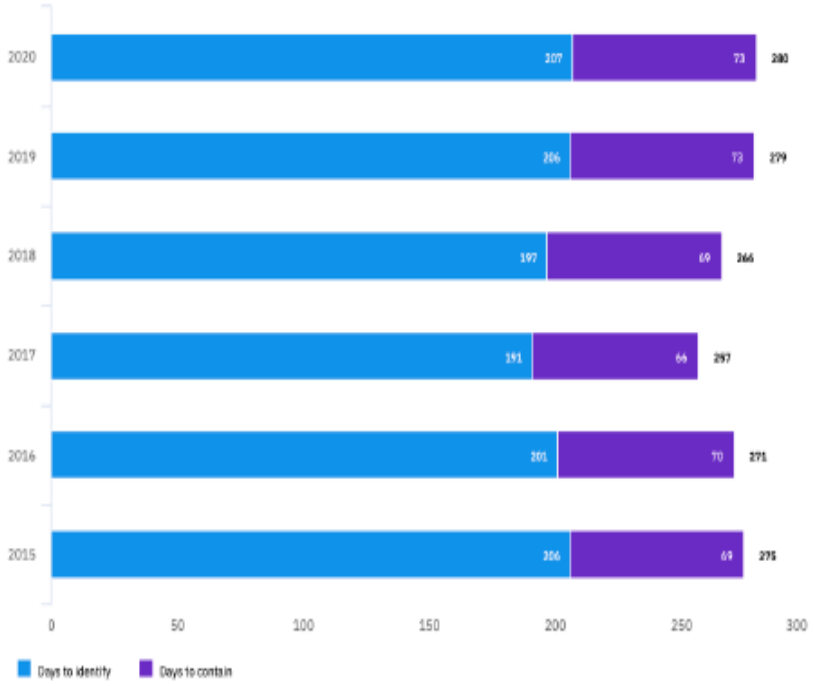
Cyber Data Incident Response Pack

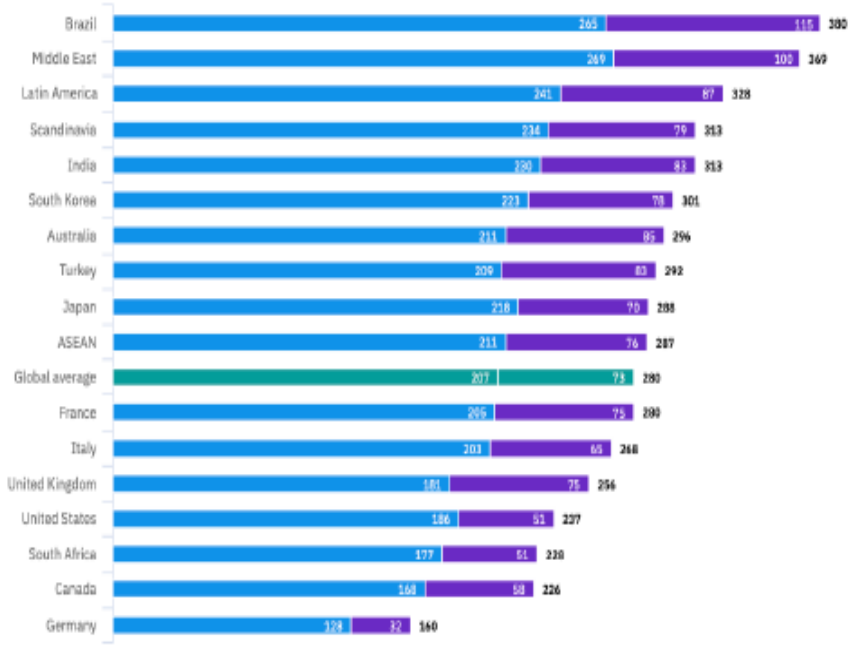
- A tale proposito è necessario approntare un **Cyber Data Incident Response Pack**, in grado di:
- - Gestire l'incident e supportare l'ente nelle attività;
- - Analizzare la natura della violazione;
- - Identificare le evidenze, prove e informazioni tecniche;
- - Determinare la tipologia dei dati compromessi;
- - Stabilire quali dati sono stati compromessi:
- - Formalizzare lo stato delle misure di sicurezza in essere;
- - Predisporre un piano di Remediation.

Cyber Data Incident Response Pack

- Nello specifico il servizio di **Cyber Data Breach Incident Response** permette di essere compliance alla normativa vigente di Data Protection normata nel GDPR. Ma oltre ad avere sempre un piano di “pronta risposta” bisogna anche intervenire giocando sul piano della Cyber Security preventiva, come con attività costanti di vulnerability assessment, penetration testing e Cyber Threat Intelligence per identificare le vulnerabilità e porvi rimedio; formazione e sensibilizzazione dei dipendenti; e sviluppo di policy e procedure in grado di assicurare la massima Cyber Resillience.

Quanto impieghiamo a individuare e gestire un incidente?





Fonte: Ponemon, 220 Cost of a Data Breach Report

DATA BREACH – CASI PRATICI

- I casi secondo il Verizon Data Breach Report 2016 di “data breach” confermati sono stati, per il 2015, pari a 2274. Ciò fa capire quanto sia diffuso il problema. Ma quali sono le cause più comuni di queste violazioni?
- Sempre facendo riferimento al Verizon DBIR 2016, le prime nove cause di “data breach” danno origine ad oltre il 90% delle violazioni

Miscellanous errors

- **Miscellaneous errors – Errori “vari”**
- Errata consegna: quando informazioni sensibili raggiungono i destinatari sbagliati
- Errata pubblicazione: quando informazioni non pubbliche vengono rese note su un web server pubblico
- Mancata o errata distruzione dei dati non più necessari: quando supporti di memorizzazione non più usati e contenenti informazioni sensibili non vengono correttamente distrutti o cancellati.

WEB APP ATTACKS

- **Web App Attacks – Attacchi alle applicazioni Web**
- La parte più interessante dell'analisi di Verizon è che, se restringiamo il campo ai servizi finanziari, il 95% degli incidenti implica il successo da parte degli attaccanti nel raccogliere credenziali rubate dai dispositivi dei clienti e, attraverso queste credenziali, accedere alle applicazioni web.
- Secondo il semplice pattern (modello): "attacco di phishing sul cliente -> ottenimento delle credenziali -> abuso dell'applicazione web -> svuotamento del conto bancario o in bitcoin"
- In questo caso i è opportuno adottare le seguenti precauzioni:
  - tracciare il comportamento degli utenti al fine di identificare comportamenti sospetti, curare ogni componente delle applicazioni web sia dal punto di vista della progettazione (security "by design") dal punto di vista del patching che va effettuato con regolarità.
  - rafforzare le misure e i metodi di autenticazione.

INSIDER MISUSE

- **Insider Misuse**
- Consiste in un abuso dei privilegi concessi a chi, all'interno dell'organizzazione, ha ottenuto fiducia. L'attore in questo caso si trova già all'interno del perimetro difensivo è ha accesso a dati sensibili o comunque di valore e ci si aspetta da esso che faccia buon uso dei privilegi concessi, ma non sempre è così purtroppo.
- Precauzioni da adottare:
  - ritagliare in maniera "chirurgica" i diritti di accesso di ciascun dipendente/addetto/utente
  - comprendere a fondo ogni relazione esistente all'interno dei processi critici, identificare le aree più a rischio e quindi definire le attività da tracciare e le situazioni in cui è opportuno inserire controlli di "audit" o misure di "fraud detection" in modo da prevenire eventuali abusi.

CYBER SPIONAGGIO

- **Cyber spionaggio**
- Analizzando questa causa si può notare come la gran parte delle vittime siano aziende manifatturiere, pubbliche o attività professionali. Inoltre si può osservare come oltre il 75% dei vettori di attacco sia legato ai messaggi di posta elettronica.

- **PRECAUZIONI**

- l'educazione dell'utente finale e un'attenzione particolare alle misure di prevenzione degli attacchi veicolati dalle e-mail al fine custodire la proprietà intellettuale su cui si fonda un business.
- "loggare" tutte le richieste DNS e tutte le richieste di navigazione (proxy) oltre che, ovviamente, investire in soluzioni che aiutino a gestire ed analizzare questo tipo di dati e "log" a scopo investigativo alla ricerca di possibili segni di compromissione ed "esfiltrazione".

CRIMEWARE

- **Crimeware**
- Questa categoria, descrive le infezioni da malware che non sono associate a classificazioni più specifiche come il cyber spionaggio e le intrusioni sui POS. In questo ambito a farla da padrone sono i malware e gli attacchi relativi basati sul concetto di Command & Control (C2) come le botnet.
- Anche in quest'ambito le raccomandazioni sono quelle di fare riferimento a politiche di difesa in profondità e educazione dell'utente finale affinché sia consapevole delle minacce inerenti al phishing e al social engineering.

POINT OF SALE INTRUSIONS

- **Point-of-Sale Intrusions – Intrusioni sui POS**
- Questo tipo di “data breach” è risultato il più diffuso fra quelli censiti dal Verizon DBIR.
- Il report differenzia gli attacchi ai POS di piccole organizzazioni da quelli rivolti a grandi aziende, i primi sono caratterizzati da attacchi di tipo “brute force” sulle password di accesso ai dispositivi, mentre il secondo tipo di attacchi, di alto profilo, tende ad utilizzare un approccio “multi-step” più complesso ed elaborato. L’attacco in quest’ultimo caso ha come obiettivi dei sistemi secondari che poi permettono di fare da “ponte” verso i sistemi POS veri e propri.
- In alcuni casi gli attaccanti hanno avuto gioco facile riuscendo ad installare un “keylogger” attraverso campagne di “Phishing”.

- **CONTRO MISURE**

- difese specifiche e accorgimenti strettamente relativi ai dispositivi POS
- l’attenzione alla gestione e all’utilizzo delle credenziali
- monitoraggio degli accessi e, possibilmente, utilizzo di autenticazione a due fattori

DATA BREACH INVESTIGATIONS 2016 REPORT

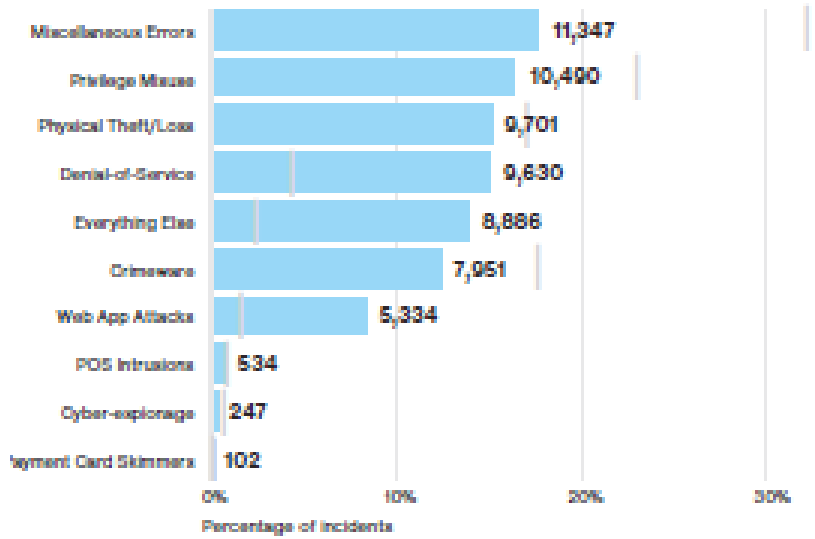


Figure 17.

Percentage (blue bar), and count of incidents per pattern. The gray line represents the percentage of incidents from the 2015 DBIR. (n=64,199)

DATA BREACH INVESTIGATIONS 2016 REPORT

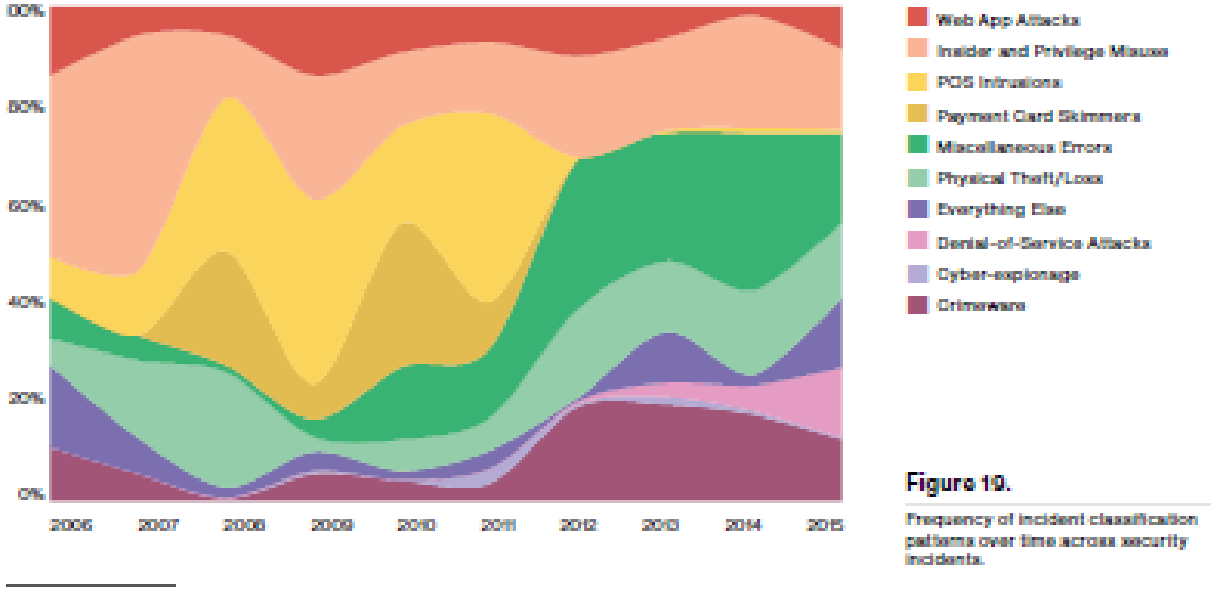


Figure 10.

Frequency of incident classification patterns over time across security incidents.

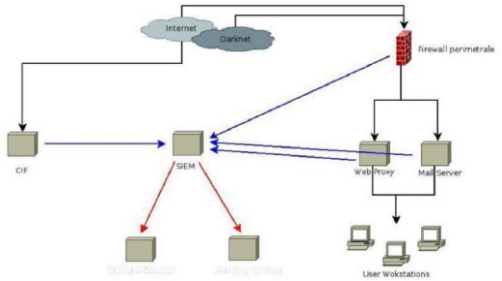
Dieci attacchi rappresentativi del 2016

	Vittima	Attaccante	Tecniche usate
1	Hollywood Presbyterian Medical Center	Cyber Crime	Ransomware
2	FriendFinder Networks	Cyber Crime	Vulnerabilità (LFI)
3	Bangladesh Bank	Cyber Crime	Multiple
4	ADUPS Technology	Cyber Espionage (Cina?)	Multiple
5	Muni (San Francisco Transport System)	Cyber Crime	Ransomware

Dieci attacchi rappresentativi del 2016

	Vittima	Attaccante	Tecniche usate
6	Democratic National Committee (DNC)	Cyber Crime	Multiple
7	Yahoo	Cyber Espionage (Russia?)	Multiple
8	DynDNS	Cyber Crime	DDoS / IoT attack
9	Teseo Bank	Cyber Espionage (Cina?)	Multiple
10	Ministero degli Esteri italiano	State sponsored (Russia?)	Multiple

Alcuni esempi pratici



Data Breach Investigations Report

- GLI ATTACCHI INFORMATICI AI DATI SANITARI
- Dall'attività di analisi svolta dal Data Breach Investigations Report team per la realizzazione del primo Verizon Protected Health Information Data Breach Report è risultato che 18 aziende su 20 sono state interessate da furti di dati sanitari . Oggetto dell'analisi sono state le violazioni confermate che hanno coinvolto oltre 392 milioni di record in 1.931 incidenti in 25 nazioni (incluse alcune europee, ad esempio la Germania) .

Verizon Report Data Breach 2017

- Il Verizon Data Breach Investigations Report ha identificato nove tipologie di incidenti che coprono la maggior parte delle violazioni che le organizzazioni in diversi settori merceologici . Nel settore manifatturiero attacchi denial-of-service, uso improprio di privilegi da parte di insider e cyberspionaggio coprono l'82% degli incidenti
- La condivisione di queste informazioni può aiutare le organizzazioni a implementare soluzioni di sicurezza su misura, in base al loro settore e agli schemi di attacco specifici utilizzati, invece di cercare di combattere su tutti i fronti .

questo approccio può rendere più efficienti ed efficaci le strategie di sicurezza nella lotta contro il crimine informatico

Report Data Breach- CLUSIT 2017

Il 67,5 % ritiene inoltre che ci potrebbero essere delle resistenze da parte dei soggetti designati quali responsabili del trattamento a causa delle corresponsabilità con il Titolare del trattamento dei dati prevista dal GDPR

- **Infatti, secondo l'art . 82 del GDPR, in alcuni casi un responsabile del trattamento può rispondere direttamente e in solido per l'intero ammontare per il danno causato dal trattamento al fine di garantire il risarcimento effettivo dell'interessato .**

In particolare ciò avviene solo se il responsabile "non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del Il principio di ***privacy by design*** **ovvero di protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema oggi risulta applicato solo nel 58,1% dei casi**

Data Breach 2018

- **Data Breach del 2018**
- vi sono stati alcuni casi esemplari come quello avvenuto nel mese di settembre 2018 a Facebook dove un attacco Hacker ha violato i dati degli account di 50 milioni di utenti iscritti sul social di Mark Zuckerberg. Tale attacco è stato prontamente sanzionato dalla Data Protection Authority competente che è quella Irlandese che ha multato Facebook per un importo pari a un 1,63 miliardi di dollari nel mese di ottobre 2018.
- - (5 gennaio 2019) l'attacco informatico avutosi in Germania dove sono stati pubblicati sul web i dati relativi a 1000 politici tedeschi tra cui la Cancelleria Angela Merkel, i dati comprendevano numeri di cellulare, carte di credito, indirizzi e-mail e postali, documenti interni di partito e chat familiari.
- - Altro caso grave avutosi nel mese di ottobre 2018 è quello relativo ai microchip spia dell'azienda Lenovo, tra i più grandi produttori di pc al mondo, ma anche Taiwan Semiconductor e Largean precision, società che realizzano obiettivi per le fotocamere degli iPhone. Secondo un'inchiesta di Bloomberg, nelle schede madri dei server utilizzati da una trentina di grandi aziende americane (tra cui Amazon e Apple) sarebbero installati dei microchip spia.
- - Anche Google nel mese di ottobre è stata vittima di un attacco informatico che ha visto l'azienda americana costretta a chiudere il sociale network Google +, in quanti i dati di mezzo milioni di utenti del servizio sono rimasti accessibili ad hacker e programmatori per qualcosa come tre anni.

Data Breach 2018

- Anche la pubblica amministrazione è stata vittima dei data breach e si segnalano due casi.
- - **Il primo è quello del portale web istituzionale del Comune di Roma dove sono stati pubblicati all'albo pretorio on line i dati di una bimba che frequenta la scuola elementare nell'VIII Municipio e della madre. L'episodio si è verificato nel mese di Ottobre ed i dati della piccola riguardavano i dati economici della famiglia che avevano un debito nei confronti del comune di 73 euro per il mancato pagamento di alcuni bollettini mensa. Il Garante ha aperto in merito all'episodio un'apposita istruttoria.**
- Il secondo caso ancora più grave di data breach si è verificato nel mese di novembre è quello che ha riguardato un vero e proprio attacco informatico al Ministero di Grazia e Giustizia dove nella notte tra il 13 e di 14 novembre i servizi informatici dei distretti di Corte di Appello dell'intero territorio nazionale sono stati interrotti. Secondo il fornitore di accesso al servizio web, Telecom Italia, sarebbe avvenuto un furto delle credenziali delle caselle di posta elettronica certificata gestito da Telecom stesso che prudenzialmente avrebbe interrotto il servizio.

Data Breach 2020

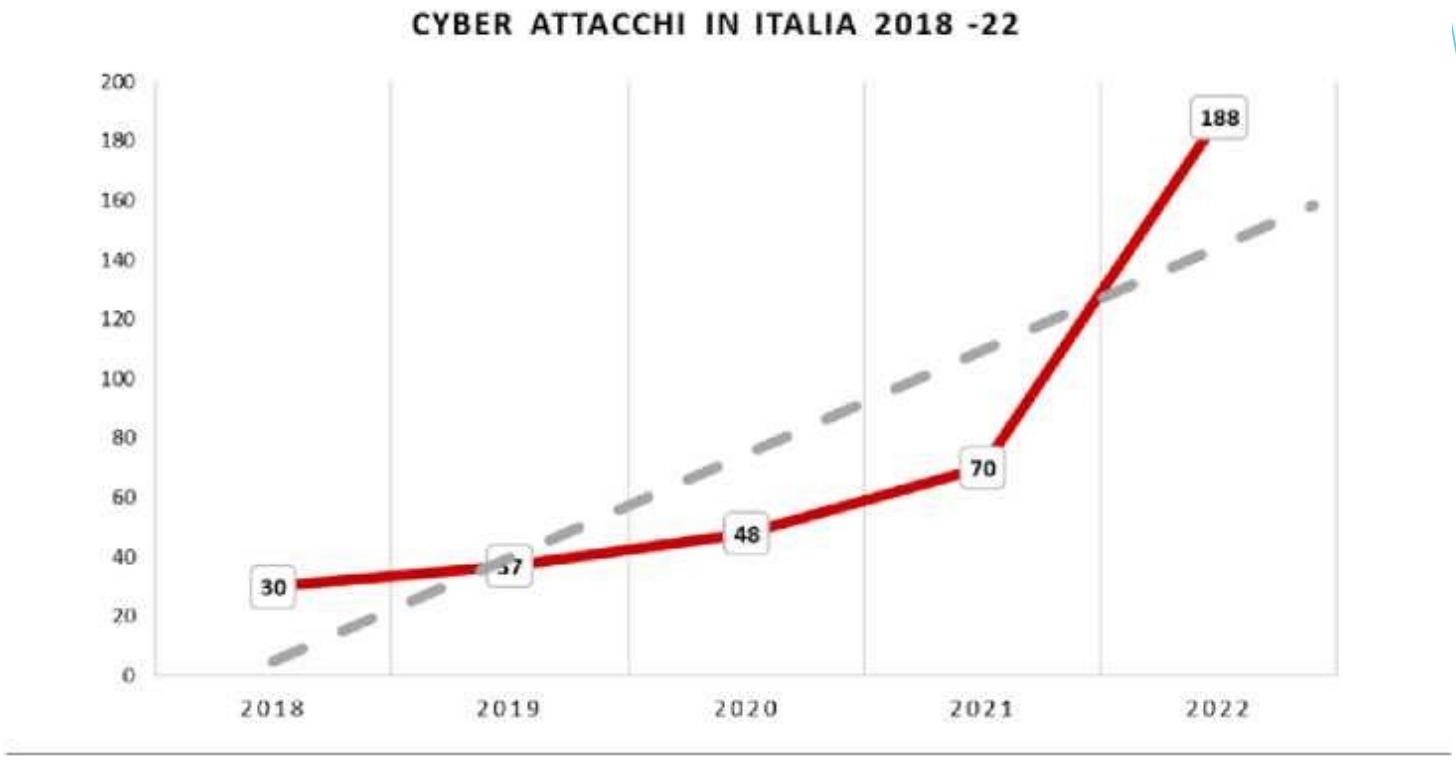
Mancata definizione dei criteri per trattare i dati di determinate categorie di richiedenti il "bonus covid", uso di informazioni non necessarie rispetto alle finalità di controllo, ricorso a dati non corretti o incompleti, inadeguata valutazione dei rischi per la privacy. Con queste motivazioni, il Garante per la protezione dati personali ha ordinato all'Inps il pagamento di una **sanzione di 300 mila euro** in relazione alle violazioni commesse nell'ambito degli accertamenti antifrode effettuati dall'Istituto riguardo al "bonus Covid" per le partite iva. In primo luogo, dopo aver acquisito da fonti aperte i dati di decine di migliaia di persone che ricoprono incarichi di carattere politico, l'Istituto ha effettuato elaborazioni e incroci tra i dati di tutti coloro che avevano richiesto il bonus con quelli dei titolari dei predetti incarichi.

Data Breach 2020

- Ciò senza però aver prima determinato se ai parlamentari e agli amministratori regionali o locali spettasse o meno tale beneficio, anche in considerazione delle differenti caratteristiche delle cariche ricoperte. In questo modo l'Inps ha violato i principi di liceità, correttezza e trasparenza stabiliti dal Regolamento Ue in materia di protezione dei dati personali. L'Inps non ha rispettato neppure il principio di minimizzazione dei dati, avendo avviato i controlli finalizzati al recupero dei bonus anche su tutti quei soggetti che, pur avendolo richiesto, non lo avevano percepito, visto che la loro domanda era già stata respinta per ragioni indipendenti dalla carica ricoperta. E' emerso inoltre che l'Inps non ha valutato adeguatamente i rischi collegati a un trattamento di dati così delicato come è quello riguardante i richiedenti un beneficio economico classificato come ammortizzatore sociale, non effettuando la valutazione di impatto sui diritti e le libertà degli interessati. Per tali motivi, il Garante ha dichiarato illecito il trattamento dei dati personali effettuato dall'Inps e ha applicato la sanzione. L'Autorità ha inoltre prescritto all'Istituto di cancellare i dati non necessari fino ad ora trattati ed effettuare un'adeguata valutazione di impatto privacy.

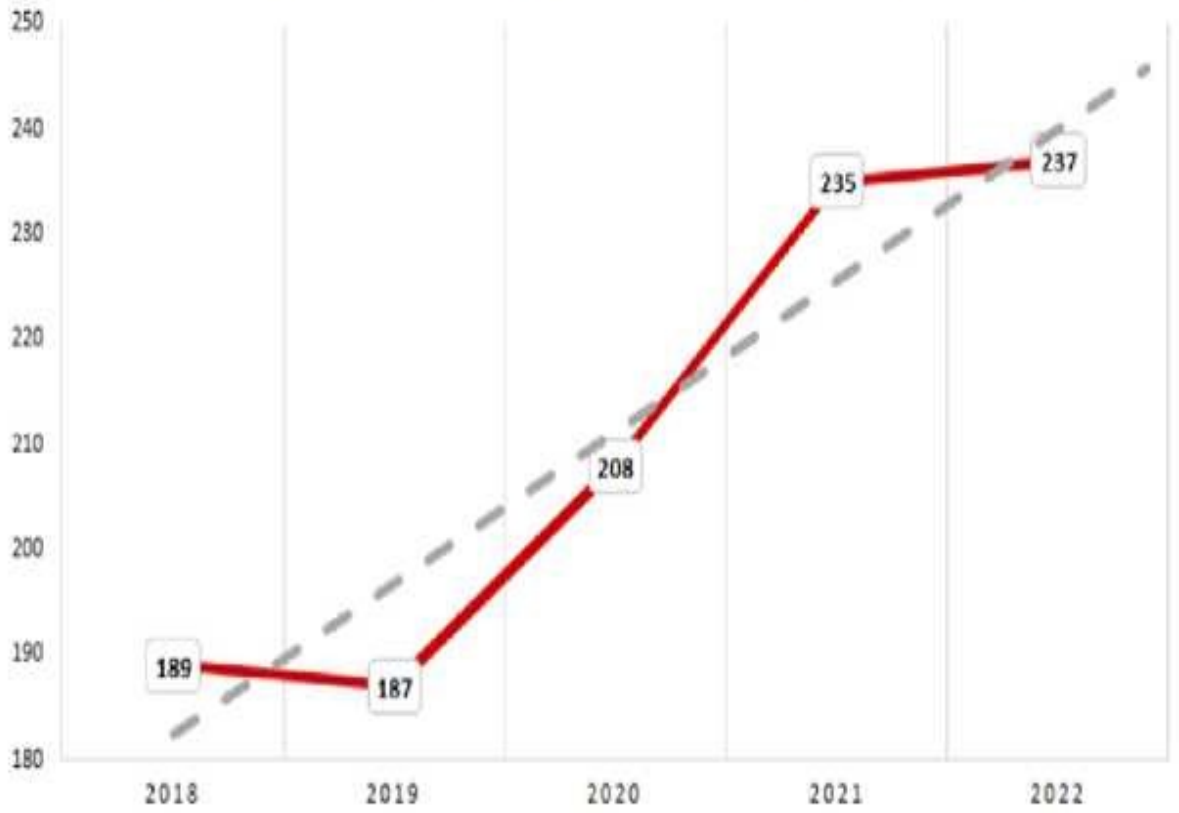
Data Breach 2021 Covid19

- Secondo l'Allianz Risk Barometer 2021, realizzato da Allianz Global Corporate & Specialty (AGCS), **interruzione di attività, pandemia e incidenti informatici sono i 3 principali rischi percepiti per il 2021**.
- Il Covid 19 ha dimostrato la rapidità in cui i crimini informatici sono in grado di adattarsi.
- I cyber-criminali si stanno evolvendo: **utilizzano la scansione automatica per identificare le lacune nei sistemi di sicurezza, attaccano i router scarsamente protetti o addirittura utilizzano i «deepfake», ovvero contenuti multimediali realistici modificati o falsificati dall'intelligenza artificiale**.



Come è possibile vedere nel grafico , in cui il dato del 2022 supera la linea di tendenza degli ultimi anni, lo scorso anno il numero di incidenti rilevati è cresciuto significativamente, con **un aumento del 527% .**

CYBER ATTACCHI GOV (CENTRAL / LOCAL) 2018 -22



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

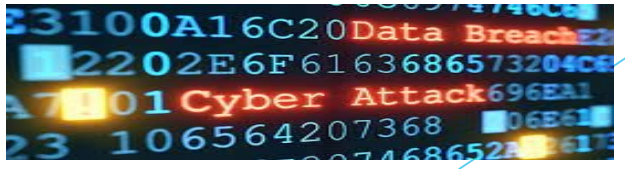
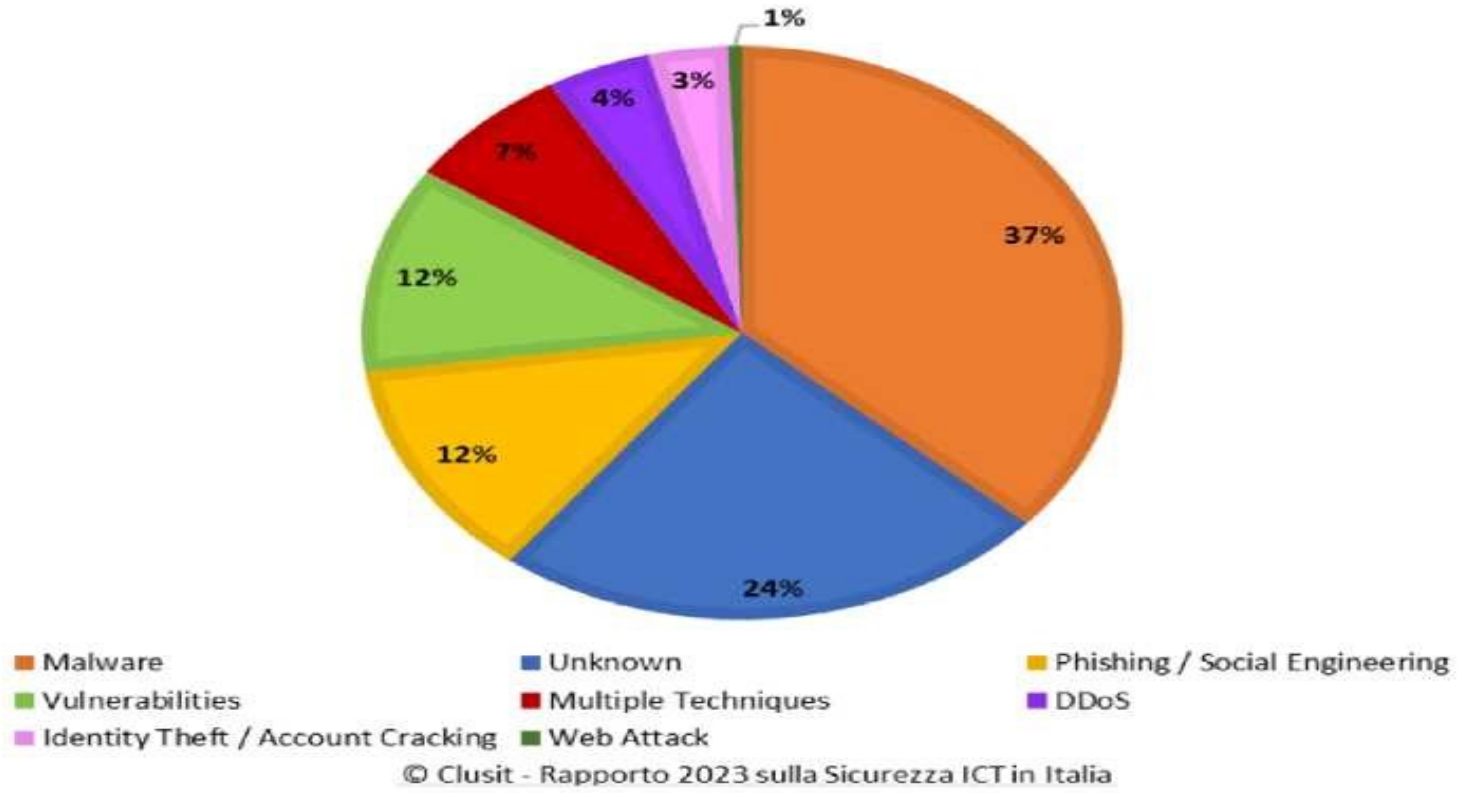


Fig. 1: *Andamento dei cyber attacchi nel periodo 2018 - 22*

DISTRIBUZIONE DELLE TECNICHE 2022



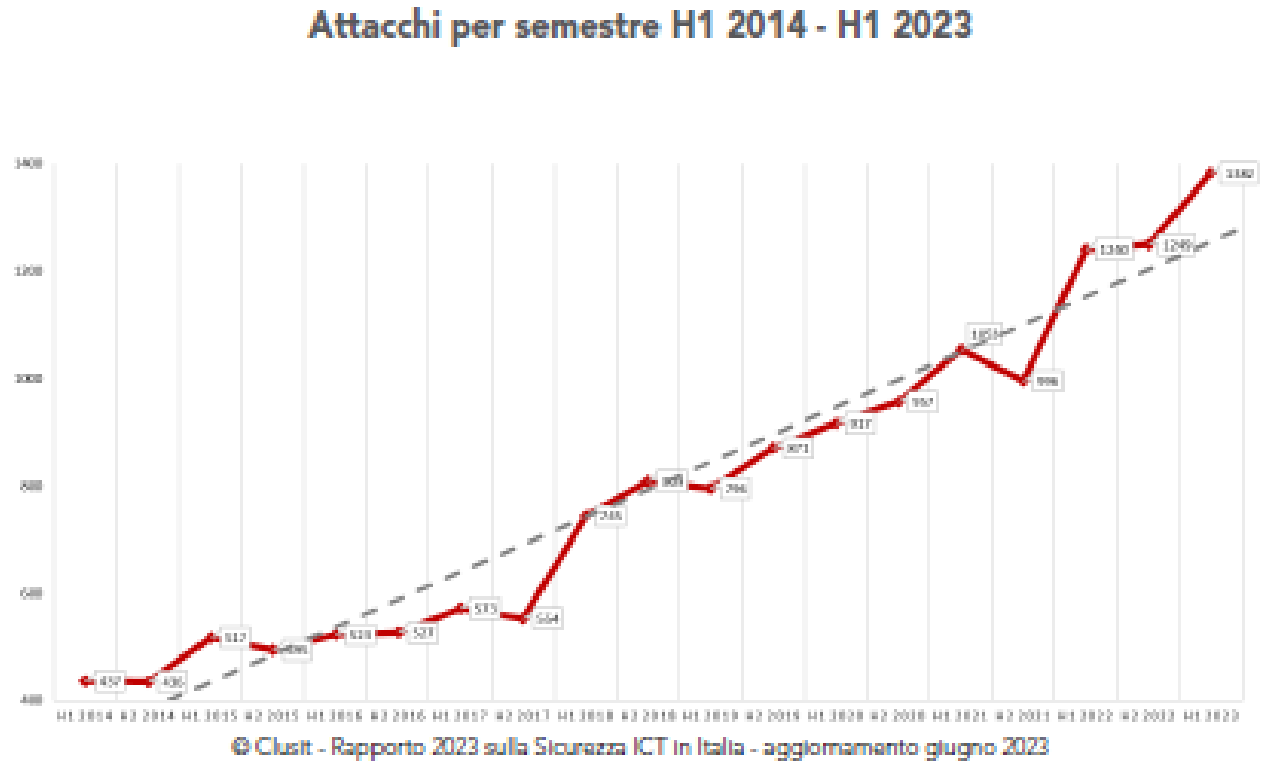


Fig. 1: *Andamento dei cyber attacchi per semestre da H1 2014 a H1 2023*

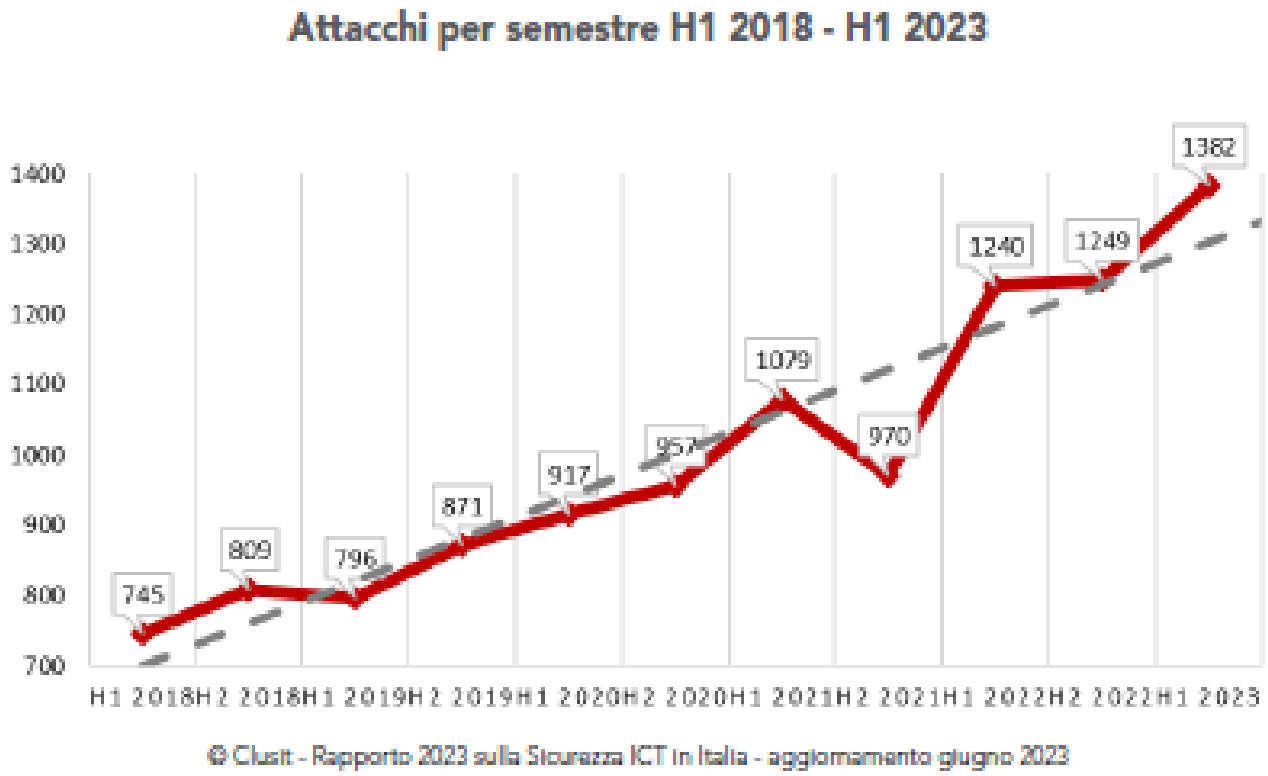


Fig. 2: *Andamento dei cyber attacchi nel periodo 2018 – H1 2023*

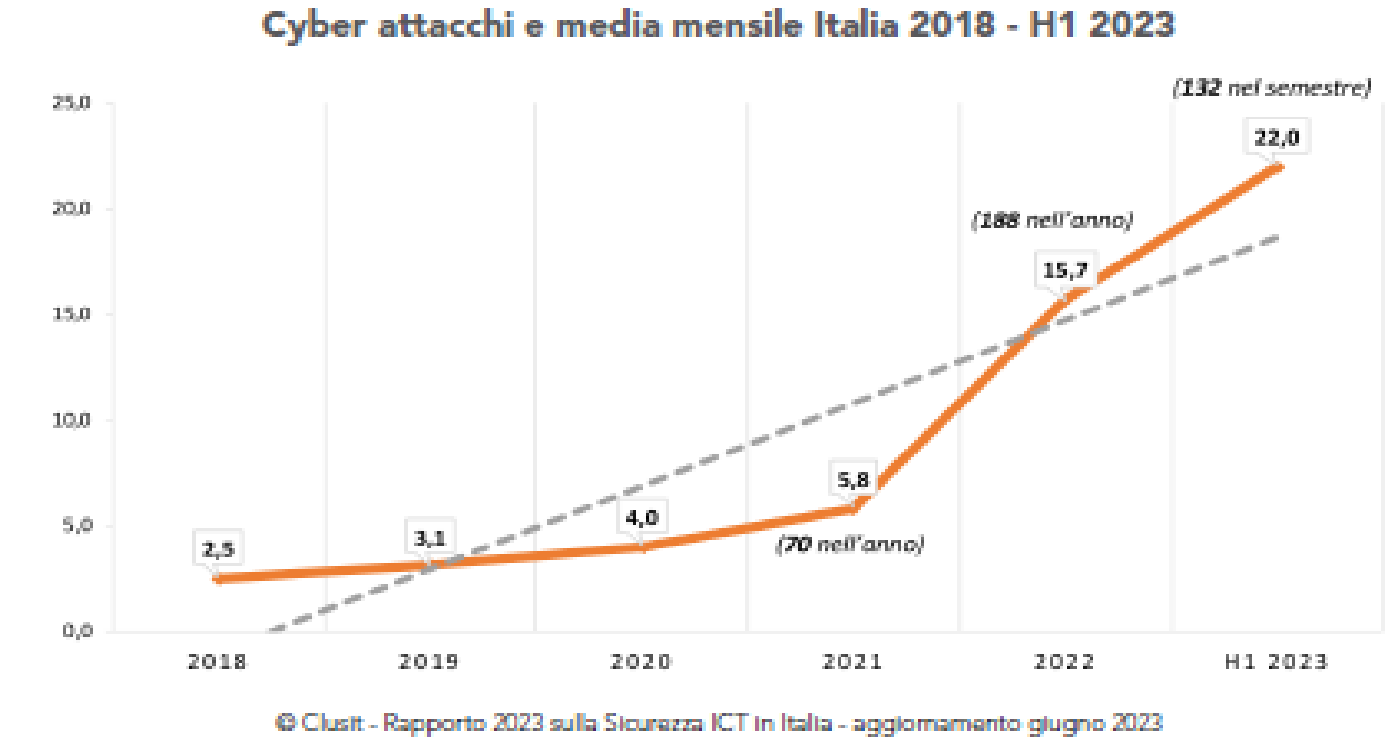


Fig. 21: *Distribuzione dei cyber attacchi e media mensile in Italia nel periodo 2018-H1 2023*

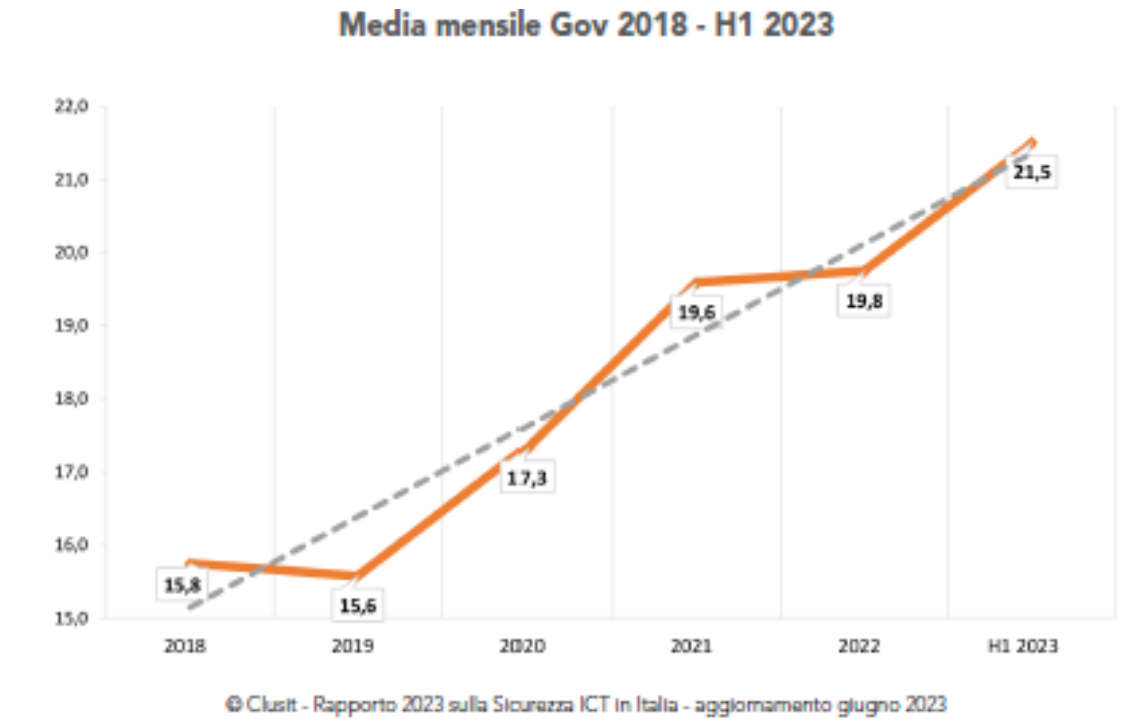
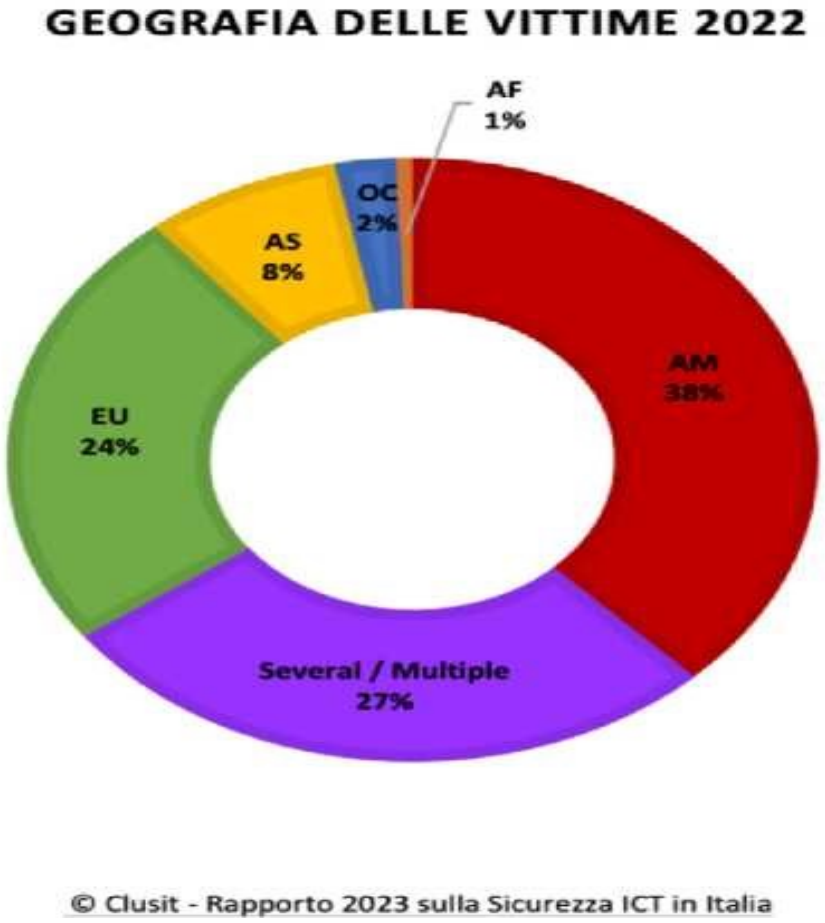
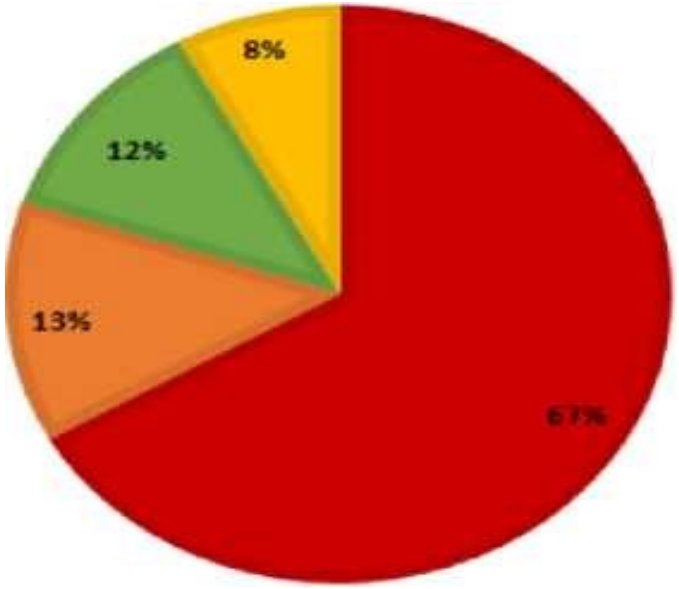


Fig. 32: *Media mensile degli attacchi al settore GOV (CENTRAL/LOCAL) nel periodo 2018- H12023*



Il 64% degli incidenti hanno come causa azioni “maldestre”, degli utenti o del personale ICT



La stragrande maggioranza degli attacchi condotti verso il settore pubblico, ben due terzi, è relativa alla categoria “**Cybercrime**”, con il 67% degli attacchi; seguono, molto distaccati ma quasi a pari merito “**Espionage/Sabotage**” e “**Hacktivism**”, rispettivamente al 13% e 12%, e infine “**Information Warfare**” al 8% ***ANNO 2022 FONTE CLUSIT***

ALCUNI ACCORGIMENTI

- Al fine di prevenire i rischi di un “data breach” è possibile utilizzare le seguenti contromisure
- Trasformare l’utente da anello debole a prima linea di difesa
- Applicare il principio del minimo privilegio per quanto riguarda l’accesso ai dati
- Adottare puntuali politiche di patching dei sistemi
- Crittografare i dati sensibili
- Utilizzare l’autenticazione a due fattori
- Rivolgere grande attenzione anche alla sicurezza fisica

I TRE TIPI DI VIOLAZIONI IN TERMINI DI DATA BREACH
provvedimento garante privacy del 30-07-2019

- - Il primo tipo di violazione tocca la confidenzialità e consiste in un accesso non autorizzato o accidentale
- - Il Secondo tipo riguarda, invece, la sfera dell'integrità e si manifesta in una modifica non autorizzata o accidentale
- - Il terzo infine riguarda la disponibilità dei dati e si manifesta nell'impossibilità dell'accesso, la perdita, distruzione non autorizzata o accidentale

DATA BREACH- DETTAGLI E DATI
provvedimento garante privacy del 30-07-2019

- **DETTAGLI** – Il modello presenta spazi in cui descrivere compitamente l'incidente di sicurezza, le categorie di dati personali violati, i sistemi e le infrastrutture IT coinvolte con indicazione della loro ubicazione e le misure di sicurezza tecniche ed organizzative adottate per ripristinare la situazione ottimale
- **DATI** – Indicare le tipologie di dati che hanno subito l'attacco (dati identificativi, recapiti fisici e virtuali, credenziali di accesso a internet o piattaforme, dati su carte di credito o Pin, dati profilati o dati delicatissimi come quelli sensibili, giudiziari, biometrici o genetici) viene richiesto anche di dare un numero approssimativo di dati violati

DATA BREACH- COMUNICAZIONE AGLI INTERESSATI

provvedimento garante privacy del 30-07-2019

- **COMUNICAZIONE AGLI INTERESSATI** – Il modello chiede di indicare se la violazione è stata comunicata agli interessati o sta per esserlo. In caso negativo bisogna spiegare al Garante la ragione di questa mancata comunicazione. In caso di comunicazione bisogna dettagliare il numero di interessati a cui è stata comunicata la violazione, il contenuto della stessa ed il canale utilizzato (sms, posta cartacea, e-mail, pec, ect)

24 Sabato 20 Febbraio 2021 GIUSTIZIA E SOCIETÀ ItaliaOggi

Tre aziende sanitarie sono finite nel mirino del Garante che ha contestato l'art. 5 Gdpr

Salute, scivolate privacy costose

Info al telefono sbagliato? Sanzione da 50 mila euro

DI ANTONIO CICCIA MESSINA

Uomo anello debole della catena di sicurezza privacy. L'errore umano sta alla base di tre sanzioni irrogate dal Garante della privacy a tre aziende sanitarie. In tutte e tre i casi è capitato che alcuni dipendenti hanno comunicato dati sanitari a persone sbagliate, per posta o per telefono. Vediamo i tre episodi, che impongono di fare attenzione non solo alle reti informatiche, ma anche alle procedure interne. Nel primo caso un dipendente ha spedito all'indirizzo sbagliato una relazione medica contenente le informazioni sulla salute e la vita sessuale di una coppia: risultato 10 mila euro di sanzione. In una seconda vicenda si è trattato di consegna a persone sbagliate di cartelle cliniche contenenti dati e referti riferibili ad altre persone, incluso un minore. Il terzo caso ha riguardato una paziente, che aveva esplicitamente richiesto, sottoscrivendo un apposito modulo, che nessun soggetto esterno, neppure i familiari, fosse informato sul suo stato di salute. Il modulo, però, era stato inserito all'interno della cartella clinica. Un'infermiera del reparto dove la donna stava seguendo delle terapie, non essendo a conoscenza della richiesta, invece che contattarla sul telefono cellulare privato, aveva chiamato il numero di casa registrato nell'anagrafe aziendale, parlando così con un familiare. La Asl ha subito anche una richiesta di risarcimento danni da parte della paziente e, intanto, ha ricevuto una sanzione di 50 mila euro. Il Garante ha in tutti e tre i casi ricordato che le informazioni sullo stato di salute possono essere comunicate a terzi solo sulla base di un presupposto giuridico o su indicazione della persona interessata, previa delega scritta. Senza il benestare o norma di legge la comunicazione viola la privacy. In tutti e tre i casi (provvedimenti 29, 30 e 36 del 27/1/2021) il Garante ha contestato l'art. 5 del regolamento Ue sulla privacy 2016/679 (Gdpr), da solo nei primi due casi e unitamente ad altre disposizioni nel terzo episodio. Questo rilievo è particolarmente preoccupante, perché l'art. 5 Gdpr che è una norma del tutto vaga quanto a dettaglio di condotte doverose o vietate. L'art. 5 si limita a indicazioni generali sul rispetto dei principi di sicurezza e di correttezza del trattamento. Sulla base di questo articolo si possono contestare e sanzionare tutte le condotte possibili, anche quelle non predeterminate in una norma specifica, che siano ritenute in violazione dei principi generali. Con un'ulteriore conseguenza: tutte le condotte rispetto a qualunque aspetto della privacy possono essere sanzionate con la sanzione più grave fino a 20 mln o, per le imprese, fino al 4% del fatturato mondiale annuo: in sostanza c'è trasposizione delle sanzioni sulla fascia più alta. La contestazione dell'art. 5 permette, infatti, di sganciarsi dalla prima fascia di sanzioni (fino a 10 mln o, per le imprese, fino al 2% del fatturato).

Provvedimenti Garante Privacy 29,30 e 36 del 27-01-2021 contestazione articolo 5 del GDPR

DATA BREACH- SANZIONI

- **Data breach sanitari, il Garante privacy sanziona tre strutture - Avevano comunicato informazioni sulla salute alle persone sbagliate**
- Le strutture sanitarie devono adottare tutte le misure tecniche e organizzative necessarie per evitare che i dati dei loro pazienti siano comunicati per errore ad altre persone. Lo ha ricordato il Garante per la privacy nel sanzionare due ospedali e una Asl per le violazioni di dati personali causati non da attacchi informatici esterni, ma da procedure inadeguate e da semplici errori materiali del personale.

- **Un ospedale toscano ha ricevuto la sanzione di 10.000 euro per aver spedito via posta, al paziente sbagliato, una relazione medica contenente le informazioni sulla salute e la vita sessuale di un'altra coppia**.

- A**nche un ospedale dell'Emilia-Romagna ha ricevuto la sanzione di 10.000 euro per aver consegnato a dei pazienti cartelle cliniche contenenti dati e referti riferibili ad altre persone, incluso un minore**.

- **- Un terzo caso riguarda invece una Asl dell'Emilia-Romagna, dove una paziente aveva esplicitamente richiesto – sottoscrivendo un apposito modulo – che nessun soggetto esterno, neppure i familiari, fosse informato sul suo stato di salute. Il modulo, però, era stato inserito all'interno della cartella clinica. Un'infermiera del reparto dove la donna stava seguendo delle terapie, non essendo a conoscenza della richiesta, invece che contattarla sul telefono cellulare privato, aveva chiamato il numero di casa registrato nell'anagrafe aziendale, parlando così con un familiare. La Asl, che ha subito anche una richiesta di risarcimento danni da parte della paziente, dovrà pagare una sanzione di 50.000 euro per la violazione del Gdpr**.

DATA BREACH- SANZIONI

- Alla luce di questi episodi e di altri ancora in corso di valutazione, il Garante ha ricordato che le informazioni sullo stato di salute possono essere comunicate a terzi solo sulla base di un presupposto giuridico o su indicazione della persona interessata, previa delega scritta. E ha invitato tutte le strutture sanitarie al pieno rispetto dei principi di correttezza e trasparenza, adottando misure tecniche e organizzative utili non solo a proteggersi da attacchi informatici, ma anche a evitare violazioni di dati personali, in particolare quelli più delicati, come quelli sulla salute - troppo spesso causate da inadeguate procedure gestionali.

Dai Garanti europei 341 sanzioni per violazioni delle regole privacy

BUSINESS & DIRITTI

Multe pesanti per le Bigtech per «trattamenti illeciti» anche in Turchia e Canada

Tempo di bilanci per le violazioni e le sanzioni alle regole della privacy. Nello Spazio economico europeo (See, 30 Paesi) nel 2020 sono state notificate - stando al report di Federprivacy - 341 sanzioni per un valore di 307.923.725 euro. Il settore più colpito dai Garanti nazionali è stato, per numero, quello delle telecomunicazioni, mentre per valore economico spiccano internet e l'e-commerce. Il 59,2% delle sanzioni europee riguardano trattamenti illeciti, il 20,8% misure di sicurezza, nel 9,1% dei casi i diritti dell'interessato, mentre le violazioni sulle informative sono state solo il 3,8% del totale.

Nelle telecomunicazioni si sono registrate 69 multe, settore seguito da servizi e commercio (47 e 45 sanzioni), mentre la pubblica amministrazione ha ricevuto 41 multe delle autorità di controllo. Con riguardo al valore economico, pagano pegno internet ed e-commerce con 144,9 milioni di euro di multe (47% del totale), seguiti da telecomunicazioni (62,4 milioni) e da commercio e attività produttive con (38,1 milioni in sanzioni). A livello nazionale, primo per incassi è il Grante francese (Cnil) che ha irrogato multe per 138.316.300, pari al 44,9% del totale complessivo. Nello scenario allargato delle politiche di tutela della privacy, in Usa va registrata la sanzione di 80 milioni di dollari alla banca Capital One, conseguenza di un grave data breach. In Turchia una serie di sanzioni sono state inflitte a Facebook, Instagram, YouTube, Periscope, e TikTok dalla Turkey's Information and Communications Technologies Authority per la mancata nomina del rappresentante sul territorio (importo complessivo di 22,8 milioni di dollari). In Francia la conferma della sanzione di 50 milioni di euro a Google nel 2019 ribadita dal Consiglio di Stato. In Canada 9,5 milioni di dollari a Facebook per affermazioni false o fuorvianti sulla privacy e sui trattamenti delle informazioni personali, mentre nell'Isola di Man la prima sanzione del Department of Home Affairs per insufficiente riscontro all'esercizio dei diritti degli interessati (13.500 euro).

—A.Gal.

Venerdì 8 Gennaio 2021 Il Sole 24 Ore

ONERI PESANTI

Le principali sanzioni amministrative previste dal Gdpr

FINO A 10 MILIONI DI EURO O AL 2% DEL FATTURATO

Sanzione fino a 10 milioni di euro o, per le imprese e se l'importo è superiore, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente per le seguenti violazioni:

- Obblighi del titolare o del responsabile del trattamento su consenso dei minori, identificazione dell'interessato, registro delle attività di trattamento, misure di sicurezza, data breach, valutazione d'impatto, certificazione della tutela dei dati
- Obblighi dell'organismo di certificazione sulle procedure di certificazione della tutela dei dati
- Codici di condotta

FINO A 20 MILIONI DI EURO O AL 4% DEL FATTURATO

Sanzione fino a 20 milioni di euro o, per le imprese e se l'importo è superiore, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente per le seguenti violazioni:

- Regole sulla liceità del trattamento e il consenso
- Informativa, diritto di accesso, di rettifica, di cancellazione, di portabilità dei dati, di opposizione
- Procedure di trasferimento dei dati verso Paesi terzi o organizzazioni internazionali
- Norme relative al trattamento dei dati in materia di giornalismo e rapporti di lavoro
- Inosservanza di una prescrizione del Garante

Illeciti e sanzioni

- **Illeciti e sanzioni**
- La violazione della disciplina in tema di data breach notification (art. 33, Regolamento UE), di comunicazione di un data breach all'interessato (art. 34 Regolamento UE) è punita con una sanzione amministrativa fino ad un massimo di 10.000.000,00 euro o, nel caso di imprese fino al 2% del fatturato mondiale annuale, se superiore (art. 43, paragrafo 4 lettera a), Regolamento UE

LE SANZIONI AMMINISTRATIVE E PECUNIARIE ART. 83 GDPR

- Le sanzioni amministrative e pecuniarie inflitte ai sensi del GDPR devono essere EFFETTIVE, DISSUASIVE E PROPORZIONATE
- Le DPA per irrogare sanzioni devono tener conto:
- natura, gravità e durata della violazione
- Carattere doloso o colposo della violazione
- Misure adottate per attenuare il danno
- Grado di responsabilità e misure tecniche e organizzative adottate
- Eventuali precedenti violazioni
- Grado di cooperazione con l'Autorità di Controllo
- Categorie di dati personali
- Rispetto di eventuali provvedimenti precedenti e Notifica all'Autorità
- Adesioni a codici di condotta o meccanismi di certificazione
- Fattori aggravanti e attenuanti

SANZIONI AMMINISTRATIVE E PECUNIARIE

- Nel caso di violazioni del GDPR da parte di imprese ed enti pubblici si dovrà tener conto:
- - Della tipologia di azienda (es. PMI);
- Nel caso di violazione da parte di persone fisiche o professionisti si dovrà tener in debito conto il loro livello generale di reddito e la situazione economica
- Nel caso di Pubbliche Amministrazioni spetta agli Stati determinare se e in che misura debbano essere sanzionate

SANZIONI AMMINISTRATIVE E PECUNIARIE

- Se in relazione allo stesso trattamento o a trattamenti collegati un titolare/responsabile del trattamento viola con dolo o colpa varie disposizioni del Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave

MISURA DELLE SANZIONI AMMINISTRATIVE E PECUNIARIE

- Esistono due classi di violazioni:

a) **Amministrative** – (10 milioni di euro oppure, se superiore e solo in caso di imprese, sino al 2% del fatturato totale a livello mondiale)

b) **Pecuniarie** – (20 milioni di euro, oppure, se superiore e solo in caso di imprese, 4% del fatturato totale a livello mondiale.

- **Le sanzioni per il settore pubblico verranno definite dai rispettivi Stati Membri**

ALTRE SANZIONI

- Le DPA, oltre alle sanzioni amministrative, possono:

- Rivolgere ammonimenti al Titolare del trattamento o al Responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente Regolamento
- Rivolgere ammonimenti al Titolare del Trattamento o al Responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del Regolamento
- Ingiungere al Titolare del trattamento o al Responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal Regolamento
- Ingiungere al Titolare del trattamento o al Responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine
- Ingiungere al Titolare del trattamento di comunicare all'interessato una violazione dei dati personali
- Imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento

ALTRE SANZIONI

- Ordinare la rettifica, cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2 e dell'articolo 19
- Revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43 oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

REGISTRO DELLE SANZIONI

- Ogni autorità di controllo promuove, insieme al Comitato europeo per la protezione dei dati un registro di sanzioni e violazioni
- Tale registro deve contenere:

1) **Tutti gli avvertimenti**
2) **Le sanzioni**
3) **La risoluzione delle violazioni**

- Inoltre ogni DPA offre ai titolari del Trattamento e ai Responsabili del trattamento di micro, piccole e medie imprese, su richiesta, informazioni generali sulle loro responsabilità e i loro obblighi conformemente al GDPR

Le Linee Guida dell'European Data Protection Board (EDB) del 14-01-2021

- Queste nuove linee guida adottate nel mese di Gennaio 2021 dall'EDPB, intendono integrare le Linee guida WP 250 e riflettere le esperienze comuni delle SAs (Security Authority) dello EEA (EEA Member States) da quando il GDPR è diventato applicabile. Il suo scopo è quello di aiutare i responsabili del trattamento dei dati a decidere come gestire le violazioni dei dati e quali fattori considerare durante la valutazione del rischio.

Le Linee Guida dell'European Data Protection Board (EDB) del 14-01-2021

- GUIDELINES EDB del 14-01-2021

Vengono esaminati attacchi svolti mediante ransomware

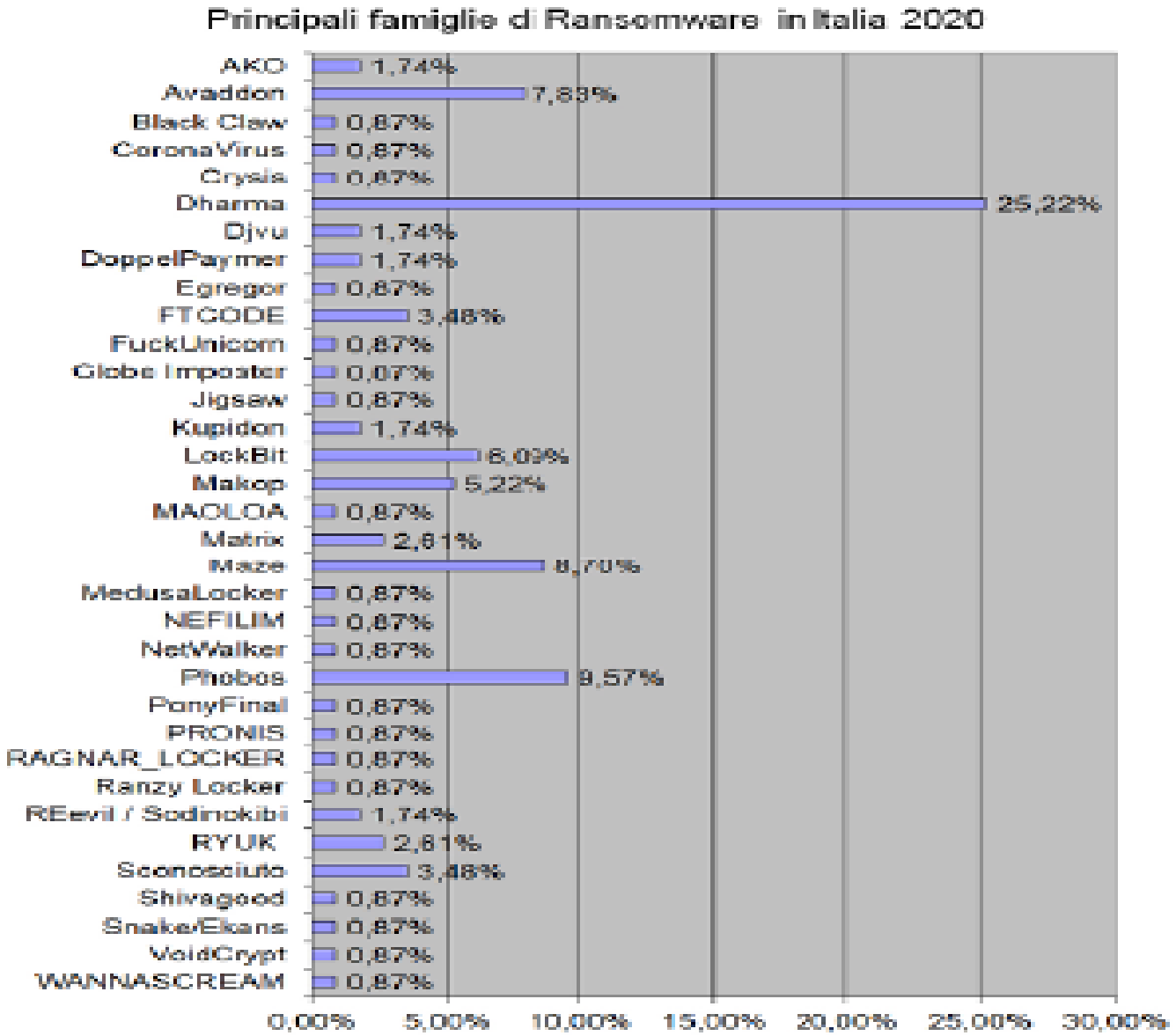
- **Ransomware con backup corretto e senza esfiltrazione**
- **Ransomware senza un backup adeguato**
- **Ransomware con backup e senza esfiltrazione in una pubblica amministrazione**

I ransomware

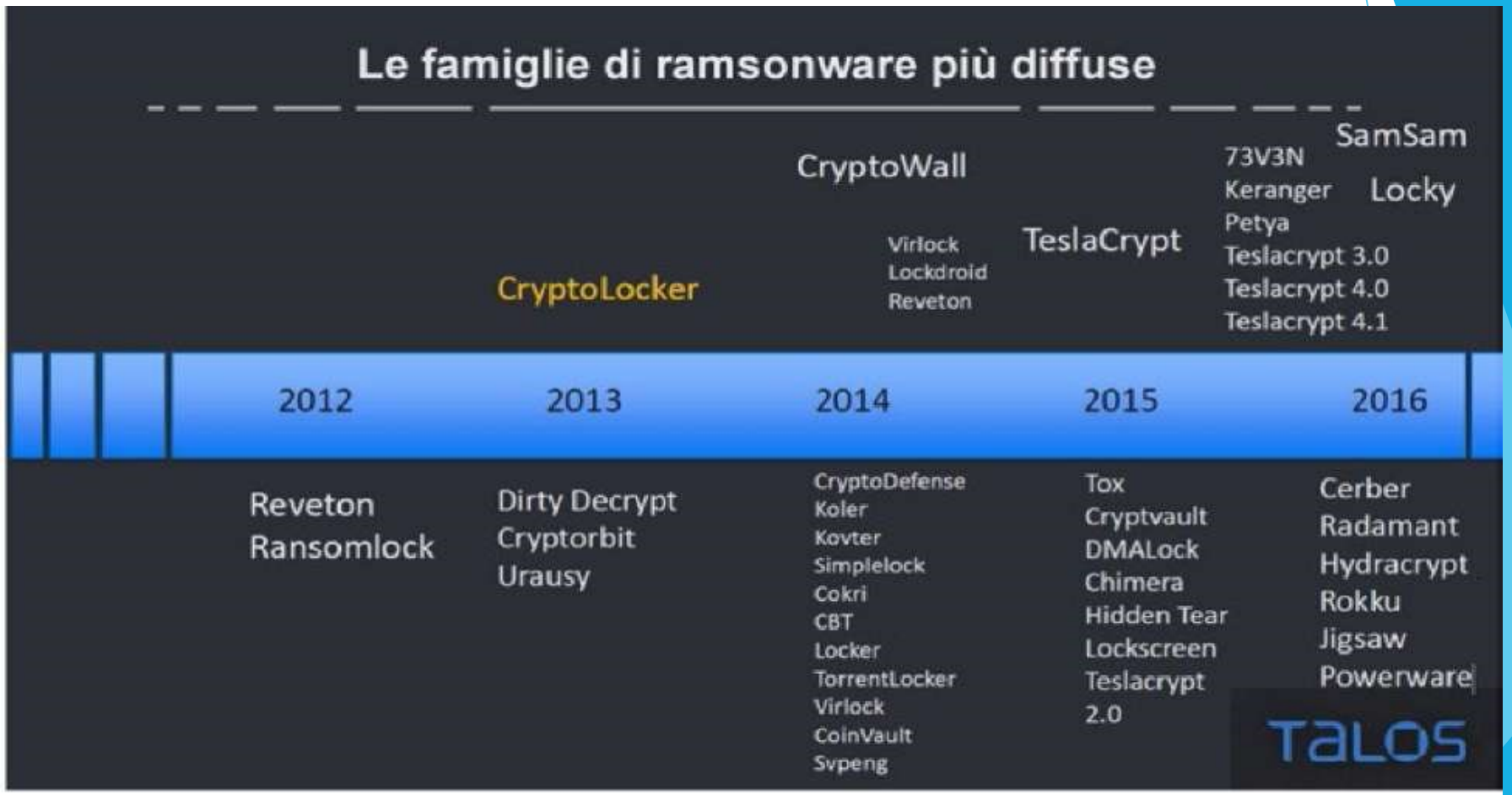
- Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

I ransomware

- La sua prima apparizione documentata risale al lontano 1989 in una modalità piuttosto artigianale, pur vantando molte delle caratteristiche del ransomware moderno. Creato e diffuso da un medico, probabilmente come ripicca per non esser stato scelto per una carica presso l'Organizzazione Mondiale per la Sanità, viaggiava come un virus su dischetto che veniva lasciato presso studi medici e cliniche . Il malware codificava i file del disco fisso e pubblicava poi la richiesta di riscatto che doveva esser pagato spedendo i contanti a una casella postale ospitata a Panama . Una volta ricevuti i soldi, il medico cybercriminale inviava alla vittima il programma necessario alla decodifica


Principali famiglie di Ransomware in Italia 2020
AKO 1,74%
Avaddon 7,83%
Black Claw 0,87%
CoronaVirus 0,87%
Crysis 0,87%
Dharma 25,22%
Djvu 1,74%
DoppelPaymer 1,74%
Egregor 0,87%
FTCODE 3,48%
FuckUnicorn 0,87%
Globe Impostor 0,87%
Jigsaw 0,87%
Kupidon 1,74%
LockBit 6,09%
Makop 5,22%
MAOLOA 0,87%
Matrix 2,61%
Maze 8,70%
MedusaLocker 0,87%
NEFILIM 0,87%
NetWalker 0,87%
Phobos 9,57%
PonyFinal 0,87%
PRONIS 0,87%
RAGNAR_LOCKER 0,87%
Ranzy Locker 0,87%
REevil / Sodinokibi 1,74%
RYUK 2,61%
Sconosciuto 3,48%
Shivagood 0,87%
Snake/Ekans 0,87%
VoidCrypt 0,87%
WANNASCREAM 0,87%
0,00% 5,00% 10,00% 15,00% 20,00% 25,00% 30,00%


3100A16C20Data Breach
2202E6F6163686573
01Cyber Attack
106564207368


Le famiglie di ramsonware più diffuse
CryptoWall
SamSam
73V3N
Keranger
Locky
Petya
Teslacrypt 3.0
Teslacrypt 4.0
Teslacrypt 4.1
Virlock
Lockdroid
Reveton
TeslaCrypt
CryptoLocker
2012
2013
2014
2015
2016
Reveton
Ransomlock
Dirty Decrypt
Cryptorbit
Urausy
CryptoDefense
Koler
Kovter
Simplelock
Cokri
CBT
Locker
TorrentLocker
Virlock
CoinVault
Svpeng
Tox
Cryptvault
DMALock
Chimera
Hidden Tear
Lockscreen
Teslacrypt
2.0
Cerber
Radamant
Hydracrypt
Rokku
Jigsaw
Powerware
TALOS


3100A16C20Data Breach
2202E6F6163686573204C
01Cyber Attack696EA1
106564207368

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

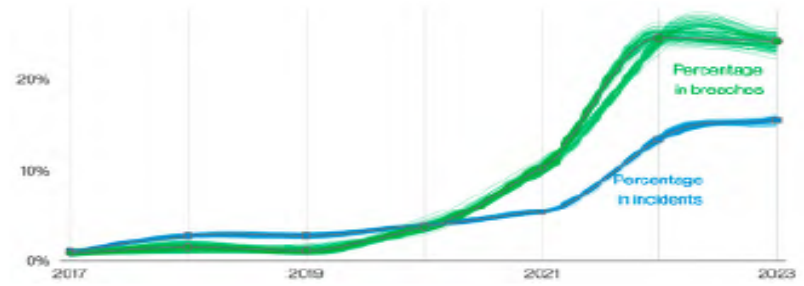


Figure 8. Ransomware action variety over time

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

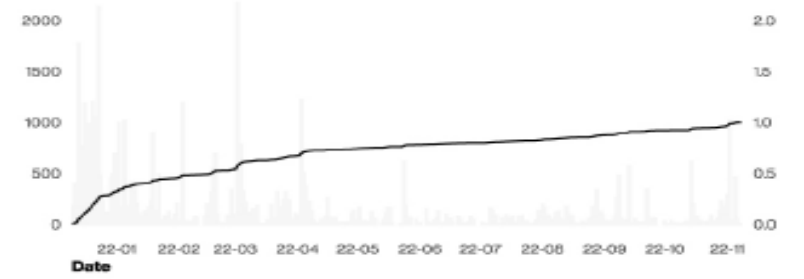


Figure 9. Percentage of Log4j scanning for 2022

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Figure 10. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

Log4j was so top-of-mind in our data contributors' incident response that 90% of incidents with Exploit vuln as an action had "Log4j," or "CVE-2021-44228" in the comments section. However, only 20.6% of the incidents had comments.

Le Linee Guida dell'European Data Protection Board (EDB) del 14-01-2021

GUIDELINES EDB del 14-01-2021

Vengono esaminati le misure tecniche ed organizzative per prevenire e mitigare gli impatti di attacchi ransomware

Successivamente si analizzeranno gli attacchi di esfiltrazione di dati così dettagliati:

- **Esfiltrazione dei dati delle domande di lavoro da un sito web**
- **Esfiltrazione di password con hash da un sito web**
- **Attacco di credential stuffing su un sito Web bancario**

Le Linee Guida dell'European Data Protection Board (EDB) del 14-01-2021

GUIDELINES EDB del 14-01-2021

Vengono esaminati le fonti di rischio umano interno

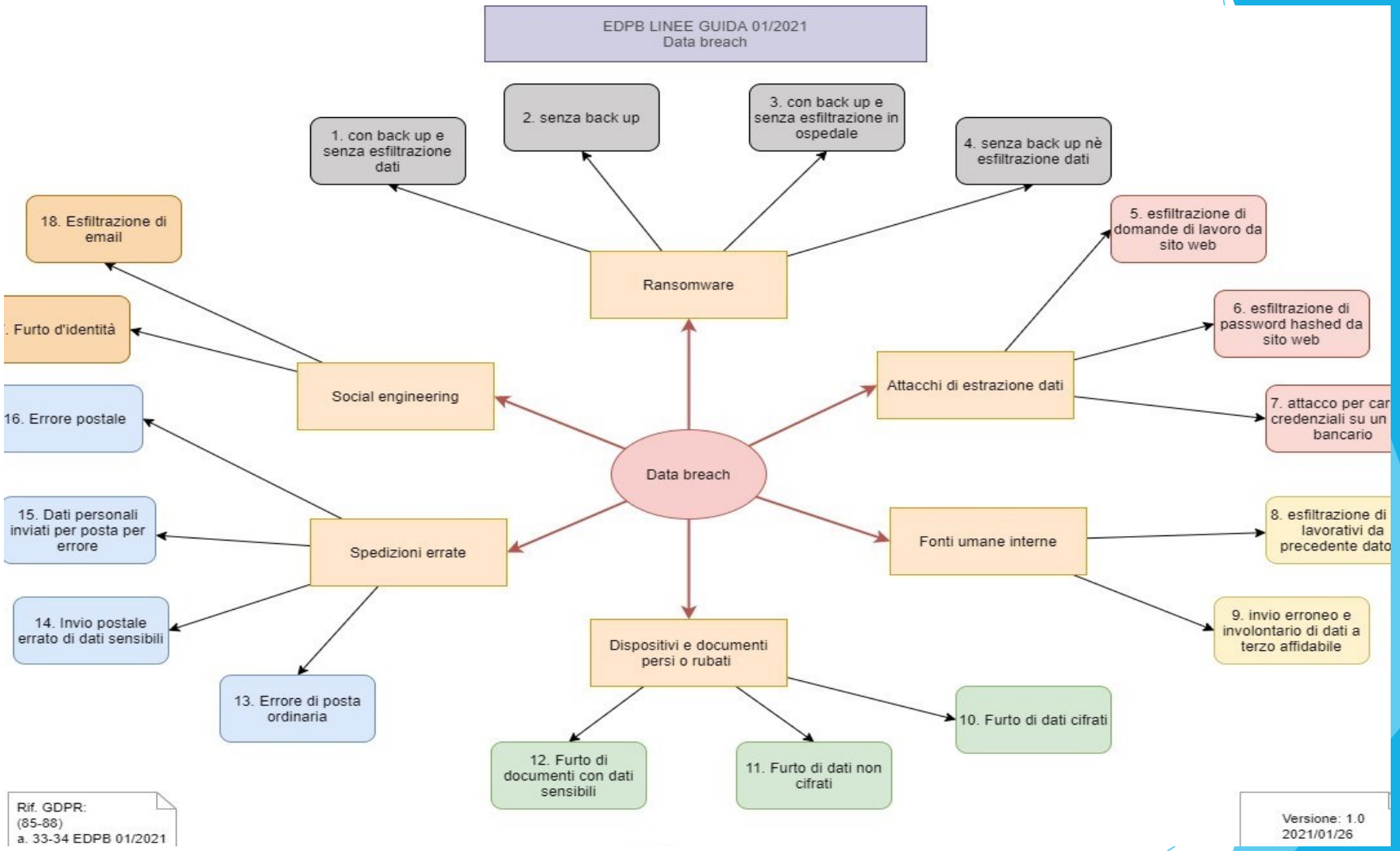
- Esfiltrazione di dati della pa da parte di un ex dipendente
- Trasmissione accidentale di dati a una terza parte fidata
- Errore di posta ordinaria
- Dati personali sensibili inviati per errore
- Dati personali inviati per posta per errore

DISPOSITIVI SMARRITO O RUBATI E DOCUMENTI SU CARTA

- Materiale rubato che memorizza dati personali crittografati
- Materiale rubato che archivia dati personali non crittografati
- File cartacei rubati con dati sensibili

ALTRI CASI - INGEGNERIA SOCIALE

- Furto d'identità
- Esfiltrazione di e-mail


EDPB LINEE GUIDA 01/2021
Data breach
Data breach
Ransomware
1. con back up e senza esfiltrazione dati
2. senza back up
3. con back up e senza esfiltrazione in ospedale
4. senza back up nè esfiltrazione dati
Social engineering
18. Esfiltrazione di email
. Furto d'identità
Attacchi di estrazione dati
5. esfiltrazione di domande di lavoro da sito web
6. esfiltrazione di password hashed da sito web
7. attacco per car credenziali su un bancario
Spedizioni errate
16. Errore postale
15. Dati personali inviati per posta per errore
14. Invio postale errato di dati sensibili
13. Errore di posta ordinaria
Fonti umane interne
8. esfiltrazione di lavorativi da precedente dato
9. invio erroneo e involontario di dati a terzo affidabile
Dispositivi e documenti persi o rubati
10. Furto di dati cifrati
11. Furto di dati non cifrati
12. Furto di documenti con dati sensibili
Rif. GDPR:
(85-88)
a. 33-34 EDPB 01/2021
Versione: 1.0
2021/01/26


Data Breach
Cyber Attack

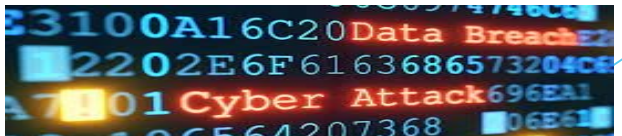
Le Linee Guida dell'European Data Protection Board del 14-01-2021applicata al case study del Comune di Pisticci (Matera)

Il Case Study del Comune di Pisticci (MT)

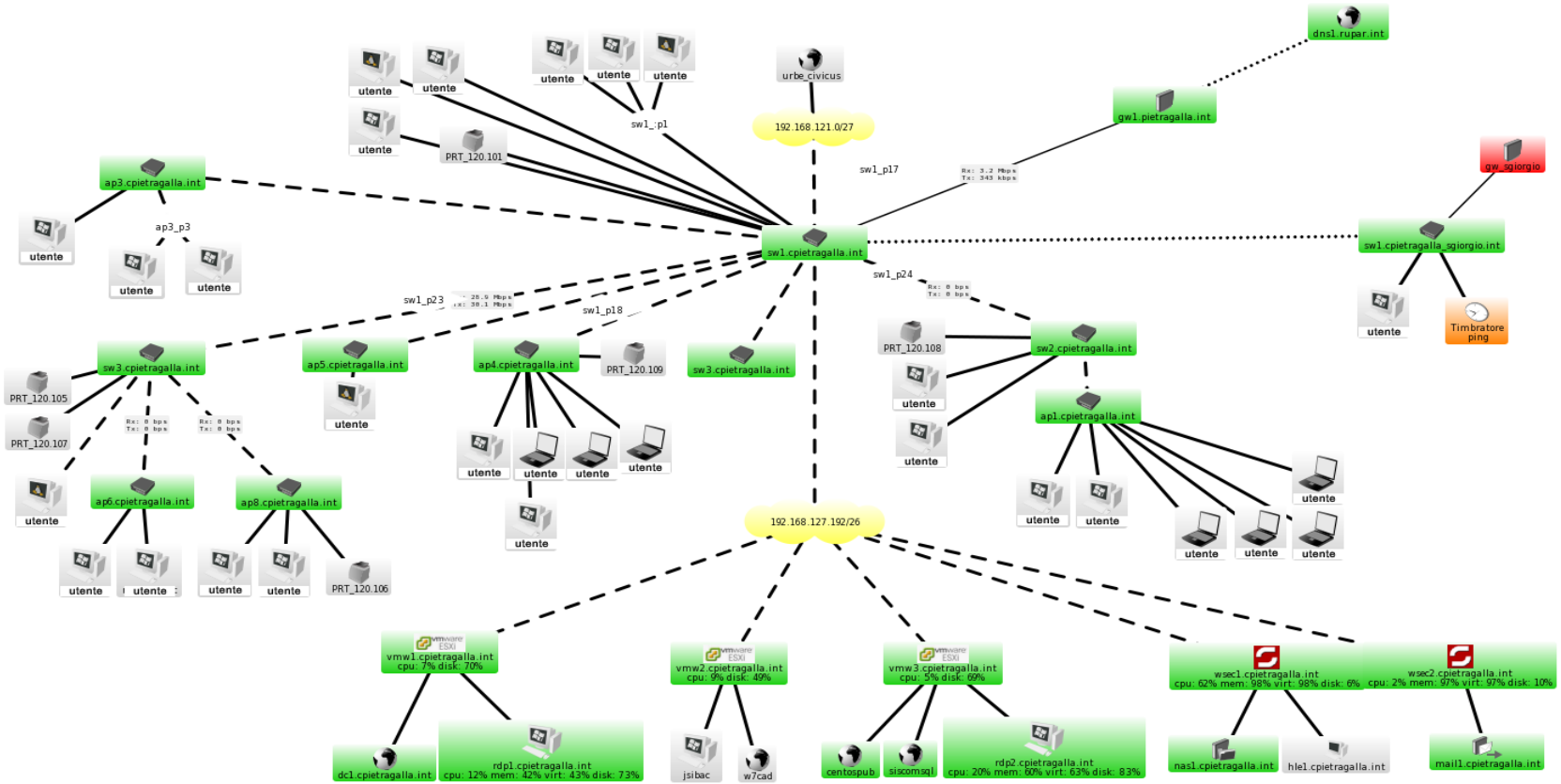
L'applicazione delle linee guida dell'EDB si basano fondamentalmente sull'architettura di rete così dettagliata dalla seguente figura che rappresenta lo stato dell'arte dell'ente

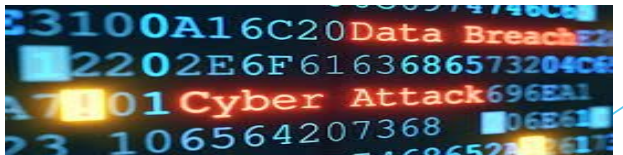
- La dotazione informatica degli uffici del Comune di Pisticci è distribuita su cinque stabili:
- > Palazzo Giannantonio Piazza dei Caduti
- > Palazzo degli Uffici Piazza Umberto I
- > Biblioteca Comunale ex palestra via Cantisani
- > Polizia Locale edificio ex Scuole Elementari via Cantisani
- > Delegazione Comunale via Genova fraz. Marconia

Palazzo Giannantonio, Piazza Umberto I e la Delegazione di Marconia sono in connessione fra di loro attraverso VPN. I restanti 2 stabili non sono interconnessi.



L’Architettura di rete del Comune di Pisticci (Matera)



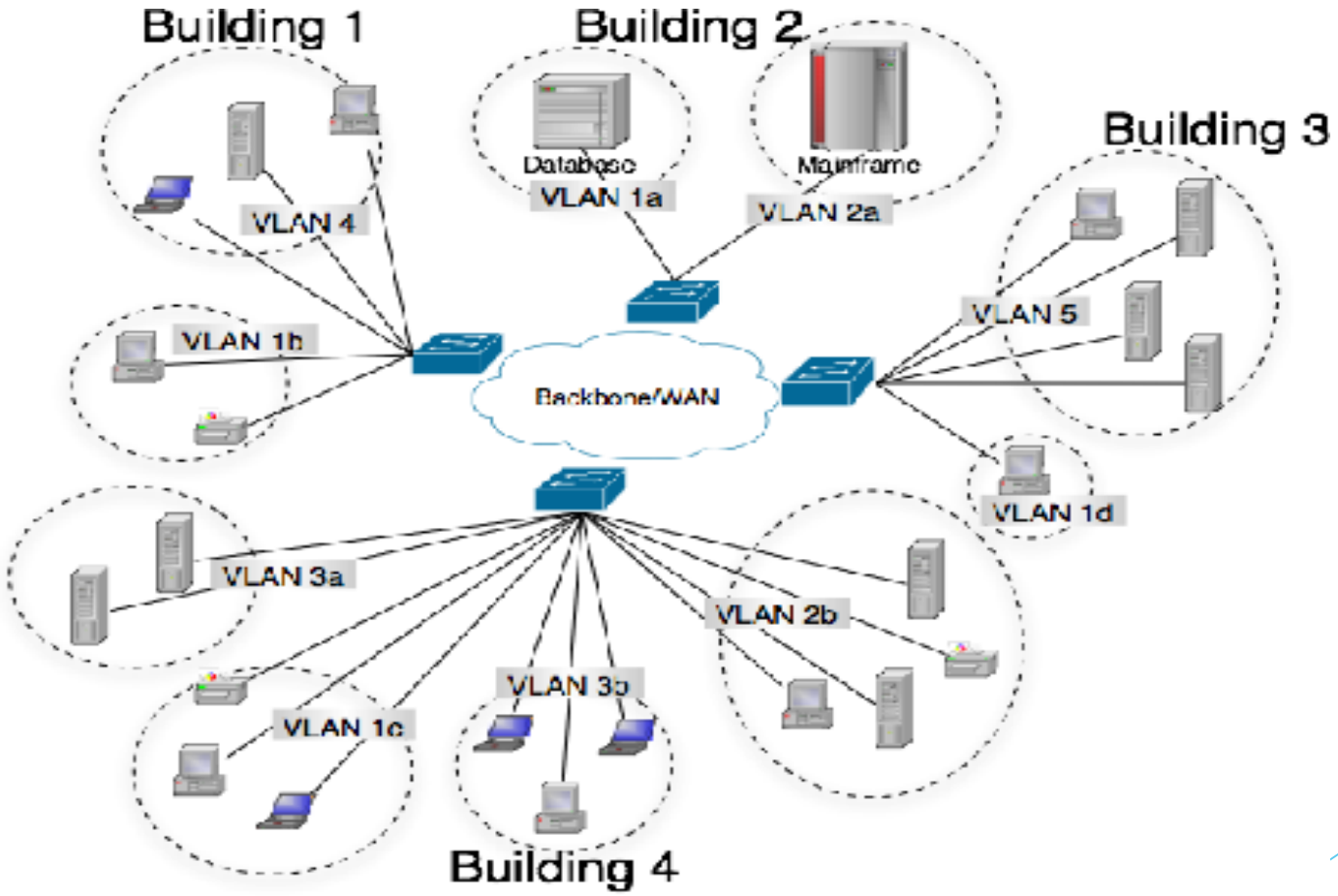


L’Utilizzo della VLAN

L’utilizzo della VLAN ed i suoi vantaggi

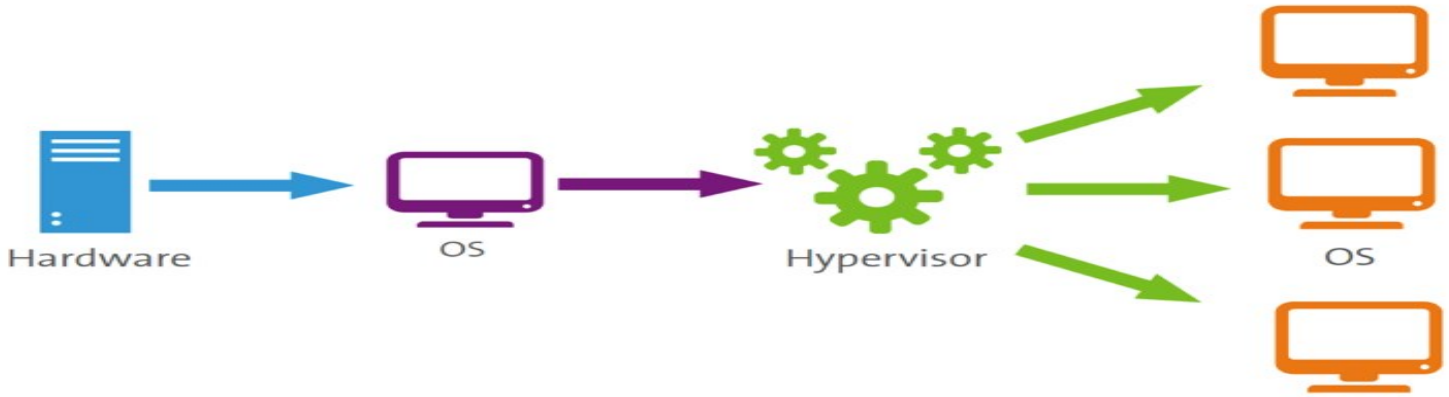
- **Facilità di gestione**: invece di spostare cavi, uplink, aggiungere dispositivi e ricablare intere zone, si gestiscono le VLAN tramite strumenti software
- **Ottimizzazione**: per isolare un segmento di rete non devo aggiungere uno switch e/o un router, ma solo riassegnare le porte.
- **Scalabilità**: riassegnazione veloce di porte e patch; estensioni delle VLAN su diversi switch; estensione di una LAN su piani diversi utilizzando un’unica dorsale di collegamento.
- **Economia e spazio**: con uno switch livello 3, si può fare routing tra le VLAN senza disporre di un router fisico ed invece di diversi switch è possibile utilizzare un solo switch con molte porte, risparmiando anche prese di alimentazione elettrica
- **Minor traffico di rete**: grazie alla limitazione del dominio di broadcast
- **Flessibilità**: le porte dello switch possono essere spostate da una VLAN ad un’altra per mezzo di semplici operazioni di riconfigurazione software magari in remoto. Altre VLAN possono essere aggiunte utilizzando le porte esistenti.

L’Utilizzo della VLAN



IL SISTEMA DI VIRTUALIZZAZIONE

La piattaforma caso di studio fa un utilizzo estensivo delle tecnologie di virtualizzazione. Il termine virtualizzazione si riferisce alla possibilità di astrarre le componenti hardware, cioè fisiche, degli elaboratori al fine di renderle disponibili al software in forma di risorsa virtuale. Tramite questo processo è quindi possibile installare sistemi operativi su hardware virtuale; l'insieme delle componenti hardware virtuali (Disco fisso, RAM, CPU, Scheda di rete) prende il nome di macchina virtuale e su di esse può essere installato il software come, appunto, i sistemi operativi e relative applicazioni. Tale tecnica è applicabile sia su sistemi desktop che su sistemi server. Consente, quindi, l'ottimizzazione di tutte le capacità di una macchina fisica distrib



IL SISTEMA DI STORAGE

Il sistema di storage è basato su un ambiente virtualizzato di derivazione Linux che utilizza differenti tipi di filesystem di nuova generazione BTRFS, XFS, designati per rimpiazzare EXT3 ed EXT4 su sistemi storage. Il filesystem, inoltre, integra la gestione dei volumi, snapshot e RAID finalizzato all'ottimizzazione dello spazio e dell'affidabilità.

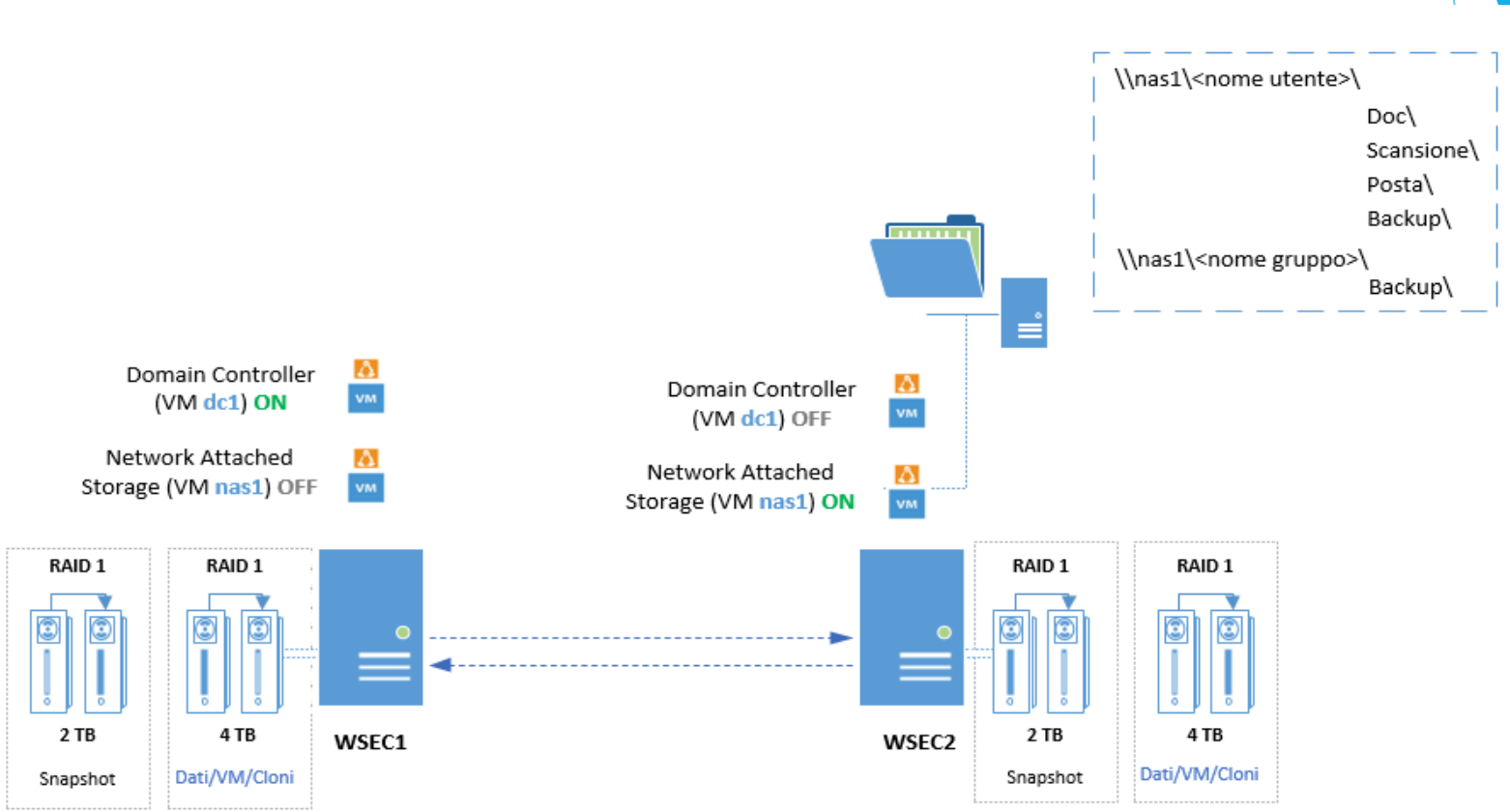
Il sistema di storage presenta i seguenti vantaggi:

- **Alta affidabilità e Backup** Il filesystem organizzato in questo modo consente una gestione agevole delle snapshot, difatti si dispone di una "time machine" che permette di accedere a dati "congelati" in sola lettura, risultando a tutti gli effetti inattaccabili da parte di malware, ransomware ed affini.
- **Crittografia** Gli storage sono progettati in maniera tale da rendere disponibile una partizione crittografata per singolo utente, nella quale poter archiviare dati ritenuti di particolare rilevanza per l'Ente e dati ritenuti sensibili

IL SISTEMA DI STORAGE

- **Prevenzione** effetti dei sistemi di virtualizzazione nei quali girano macchine virtuali dedicate alla fruizione dei dati sul dominio. Tali macchine virtuali, opportunamente ridondate sugli storage, in modalità hot/stand-by presentano al loro interno un servizio costantemente attivo in grado di rilevare un'eventuale attività sospetta sui dati da parte di applicazioni malevole, quali cryptolocker.
- **Rimedio** Il sistema in uso, come su indicato, grazie alla presenza delle snapshot quotidiane, ridondate sui due sistemi di storage, permette al singolo utente della piattaforma il ripristino dei dati storicizzati secondo una temporizzazione limitata esclusivamente dalla capienza dei dischi utilizzati sugli storage stessi – da una settimana ad uno o più mesi.

IL SISTEMA DI STORAGE



CONCLUSIONI

- L’applicazione delle linee guida EDPB di gennaio 2021 applicate all’ente pubblico Comune di Pisticci sito in Provincia di Matera **rappresentano un caso classico ed una best practice in termini di strumenti di prevention per una Pubblica Amministrazione, soprattutto per ciò che concerne le politiche di mitigazione dei ransomware**. Inoltre la soluzione proposta mediante la nuova architettura di rete consente l’introduzione di una modalità di lavoro improntata sulla centralizzazione dei dati e degli accessi, **che evita cosi un utilizzo distorto della PDL nella classica modalità “casalinga” ed educa l’utente al concetto di separazione dei dati dalle applicazioni, modalità che consente una massima prevenzione in caso di data breach.**

BIBLIOGRAFIA

- Agenzia dell'Unione Europea per i diritti fondamentali e Consiglio d'Europa (2018), Manuale sul Diritto Europeo in materia di protezione dei dati
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del regolamento 2016/679), WP250 del 3 ottobre 2017
- **Generali Paola e Iezzi Pierguido** (2019), Conoscere e gestire un Data Breach - Linee Guida Editore Youcanprint
- **Giordano Massimo Lanzo Riccardo** (2020), Data breach» e privacy. Quando la sicurezza dei dati personali viene compromessa. I casi decisi dal garante privacy, Key Editore
- **Provvedimento Autorità Garante sulla Privacy** n. 161 del 4 aprile 2013- Settore comunicazioni elettroniche
- **Provvedimento Autorità Garante sulla Privacy** n. 513 del 12 novembre 2014- Biometria
- **Provvedimento Autorità Garante sulla Privacy** n. 331 del 4 giugno 2015- Dati sanitari inseriti in Dossier
- **Provvedimento Autorità Garante sulla Privacy** del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche"

WEBGRAFIA

- G29 WP250 rev.1, 6 February 2018, Guidelines on Personal Data Breach notification under Regulation 2016/679 - endorsed by the EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item id=612052.
- G29 WP213, 25 March 2014, Opinion 03/2014 on Personal Data Breach Notification, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/index en.htm#maincontentSec4.
- Guzzo Antonio, 28 Maggio 2018, Agenda Digitale *Data breach nel GDPR: cos'è e come fare segnalazione e prevenzione*, https://www.agendadigitale.eu/sicurezza/data-breach-nel-gdpr-cose-e-cosa-sapere-per-segnalazione-e-prevenzione/
- Guzzo Antonio, 25 Giugno 2018, Agenda Digitale *Ransomware nella PA e nella Sanità, così prendono in ostaggio i nostri dati*, https://www.agendadigitale.eu/sanita/ransowmare-nella-pa-e-nella-sanita-cosi-prendono-in-ostaggio-i-nostri-dati/
- The International Conference of Data Protection and Privacy Commissioners, Resolution to address the role of human error in personal Data Breaches, October 2019, http://globalprivacvassemblv.org/wp- content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf
- EDBP Guidelines 01/2021, 14 Jenurary 2021- On Example Regarding Data Breach Notification https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf l

Il fenomeno del Data Breach secondo quanto previsto dal GDPR. Analisi empirica applicata agli strumenti di data prevention: il caso del Comune di Pisticci (MT)

23 AGOSTO 2023

ANTONIO GUZZO

SOCIETA' ITALIANA DI INTELLIGENCE

Socint Press

Pubblicato nell'ottobre 2023
SOCINT Press
https://press.socint.org/
Società Italiana di Intelligence

9 791280 111449

Società Italiana di Intelligence
c/o Università della Calabria
Cubo 18-b, 7° piano
Via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia
https://www.socint.org
ISBN 979-128-0111-44-9