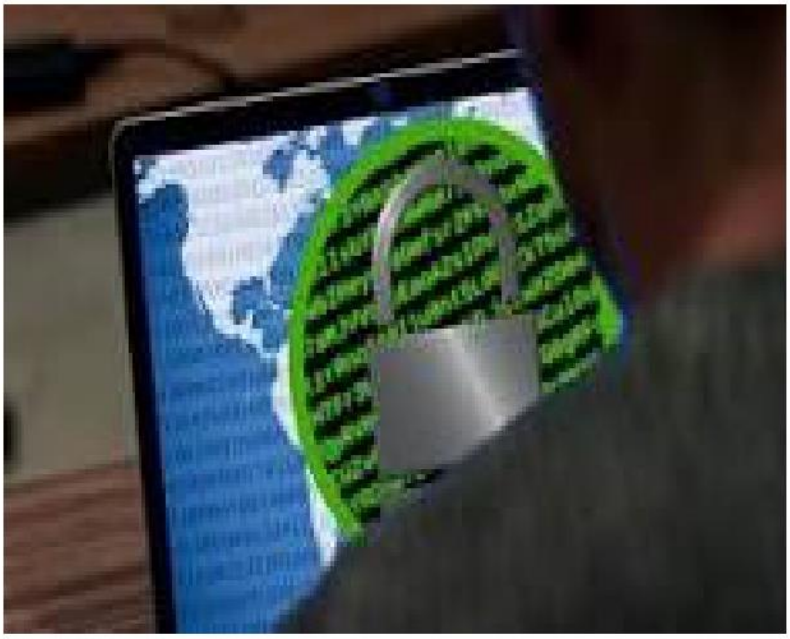
Il fenomeno del Data Breach secondo quanto previsto dal GDPR. Analisi empirica applicata agli strumenti di data prevention: il caso del Comune di Pisticci (MT)



23 AGOSTO 2023

ANTONIO GUZZO

SOCIETA' ITALIANA DI INTELLIGENCE

Socint Press

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

SAPIENZA
UNIVERSITÀ DI ROMA

MASTER DI II LIVELLO
SICUREZZA DELLE INFORMAZIONI E INFORMAZIONE STRATEGICA
- Project Work -
Anno Accademico 2019/2020

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)

Facoltà Ingegneria dell'Informazione, Informatica e Statistica
Dipartimento di Ingegneria Informatica, Automatica e Gestionale
"Antonio Ruberti"

Candidato
Guzzo Antonio

Relatore
Prof. Avv. Giuseppe Corasaniti

INDICE

Indice delle Figure

1. INTRODUZIONE

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati. I rischi di Data Breach e le sue conseguenze sono forse uno dei temi più discussi del Regolamento UE 679/2016 (GDPR). Il Data Breach o "violazione dei dati personali" è definito come «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». Il presente lavoro esamina il concetto di Data Breach introdotto dal vigente regolamento europeo 679/2016 (GDPR) con un focus su alcuni approfondimenti di case study verificatisi in Italia ed all'estero. Il fenomeno del Data Breach secondo quanto previsto dal Regolamento 676/2016 GDPR viene analizzato secondo il sistema del doppio binario: normativo ed IT dal punto di vista della cybersecurity. Il caso che tratterò riguarderà l'ente pubblico Comune di Pisticci (provincia di Matera) dove espleto la funzione di Data Protection Officer (Responsabile della Protezione dei Dati) giusta Determinazione del Responsabile n° 276 del 29-10-2020[1]. L'oggetto della tesi riguarderà l'analisi in forma sperimentale applicata al fenomeno del Data Breach applicata agli strumenti di data prevention che una pubblica amministrazione utilizza in caso di attacco applicata alla legge 133/2019 sul perimetro di sicurezza cibernetica con l'esempio del Comune di Pisticci sito in Basilicata nella provincia di Matera, in collaborazione con il partner tecnologico dell'ente la Società Soluzioni S.r.l. di Potenza. L'analisi verrà effettuata secondo le guidelines n° 1/2021 approvate dall'EDB (European Data Protection Board) e adottate il 14-01-2021. Nello specifico si analizzeranno attacchi svolti mediante ransomware così dettagliati:

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

Verranno identificate le misure organizzative e tecniche per prevenire / 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

Si passerà successivamente ad esaminare le fonti di rischio umano interno così dettagliati:

- 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 posta elettronica per errore
- Dati personali inviati per posta per errore

DISPOSITIVI SMARRITI 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

[1] https://www.comunedipisticci.it/index.php/privacy.html

2. Il Data Breach: la violazione delle misure di sicurezza (articolo 32 GDPR 679/2016)

Per Data Breach, nella versione italiana violazione dei dati personali 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. Sempre secondo il GDPR, 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 GDPR ha previsto l'obbligo di segnalazione Data Breach entro 72 ore è questo risulta essere l'obbligo più gravoso, secondo le aziende italiane, in un recente sondaggio di Idc. Con il Regolamento UE n° 2016/679 la notificazione preventiva viene abolita e sostituita da nuovi obblighi di tenuta di un registro dei trattamenti e dei Data Breach, nonché dal dovere di notificazione delle violazioni di dati personali (Data Breach Notification).
Inoltre, nel 2018 è intervenuto il Gruppo di lavoro Working Party 29 con un'opinione contenente; delle importanti linee guida che hanno distinto in tre macro-categorie il Data Breach:

- "Confidentiality Breach", quando vi è un accesso accidentale o abusivo a dati personali:
- "Availability Breach", quando vi è una perdita o distruzione accidentale o non autorizzata dei Dato personale;
- "Integrity Breach", quando vi è un'alterazione accidentale o non autorizzata del dato personale.

Verranno nei prossimi paragrafi forniti alcuni esempi significativi di Data Breach che potranno essere di grande utilità per inquadrare il contesto con particolare riferimento al caso di "Availability Breach".

2.1 L'obbligo di notifica

A tale proposito, è stato introdotto dall'articolo 33, l'obbligo generalizzato, in capo al titolare del trattamento di notifica di Data Breach all'autorità di controllo (DPO) 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 (Data Protection Authority) competente fornirà una modulistica on line richiedendo informazioni obbligatorie. Tale documentazione consente all'Autorità di controllo di verificare il rispetto delle prescrizioni. Inoltre con l'approvazione del provvedimento dell'autorità garante sulla privacy del 30 luglio 2019 vengono indicati tre tipologie di Data Breach: 1) il primo riguarda la confidenzialità e consiste in una diffusione o in un accesso non autorizzato o accidentale; 2) il secondo riguarda invece la sfera dell'integrità e si manifesta in una modifica non autorizzata o accidentale; 3) il terzo concerne la disponibilità dei dati, l'impossibilità di accesso, la perdita, distruzione non autorizzata o accidentale.

Come dev'essere la notifica di Data Breach
L'art. 33 del GDPR dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 55 senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data Breach).

Tale notifica deve, come minimo:

- 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 della violazione 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, se del caso, per attenuarne i possibili effetti negativi.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto dell'art. 33 del Regolamento.
Tale notifica dovrà essere sottoscritta con firma digitale ed inviata via PEC all'indirizzo PEC del garante protocollo@pec.gdp.it

In Italia prima dell'approvazione del Regolamento erano già presenti obblighi di notifica in quattro fattispecie di trattamento:

- Settore comunicazioni elettroniche (Prov. Garante 161/2013) - Provvedimento del Garante n. 161 del 4 aprile 2013 con il quale viene prescritto l'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) da parte dei fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali). Secondo il provvedimento in caso di violazione dei dati personali, società di Tlc e Isp devono: entro 24 ore dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione entro 3 giorni dalla scoperta, informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013. La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati. Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un inventario costantemente aggiornato delle violazioni subite.
- - Biometria (Provv. Garante 513/2014) - Provvedimento n. 513 del 12 novembre 2014 dove viene previsto che entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.
- Dati sanitari inseriti in Dossier (Provv. Garante 331/2015) Provvedimento n. 331 del 4 giugno 2015 dove viene sancito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.
- Dati comunicati fra PA (Provv. Garante 393/2015)- Provvedimento del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" con il quale il Garante prescrive, ai sensi dell'articolo 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare all'Autorità, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti

informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni dovevano essere redatte secondo uno schema specifico allegato al provvedimento e inviate tramite posta elettronica o posta elettronica certificata.

2.2 La comunicazione di Data Breach art. 34 (violazione dei dati personali all'interessato)

L'art. 34, invece, prevede un'altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all'interessato. Difatti, quando la violazione dei dati personali è suscettibile di presentare 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 predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'art. 33 paragrafo 3, lettere b), c) e d). Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se:

- il titolare del trattamento ha messo in atto le misure tecniche e 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 di cui al paragrafo 1; detta comunicazione richiederebbe sforzi sproporzionati.

In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che non ve ne sia bisogno in quanto una delle condizioni richieste dalla normativa sia da ritenere soddisfatta.
La comunicazione non è un mero atto formale ma uno strumento di tutela di tutti i soggetti coinvolti, compreso il titolare, perché «dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi». Di conseguenza e secondo i normali canoni giuridici, essa permette di ridurre il carico di responsabilità in capo al titolare per tutti quei danni (considerando 85) che a seguito delle raccomandazioni siano evitabili con la normale diligenza dell'interessato e senza sforzi sproporzionati. Infine, il necessario "concerto" con l'autorità di controllo permette il contemperamento di interessi diversi e di carattere generale. Per esempio, giustificando un ritardo nella comunicazione o una variazione nei contenuti della stessa per «contrastare violazioni di dati personali ripetute o analoghe».
Sulla stessa linea, solo se si è predisposto un piano per prevenire e reagire a eventuali violazioni si può accedere alle eccezioni di cui all'art. 34 sia che le misure tecniche e organizzative adeguate di protezione siano state previamente adottate e poi applicate ai dati personali oggetto della violazione o che siano state comunque prontamente adottate «misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati». Va da sé che la terza eccezione alla comunicazione (siano necessari sforzi sproporzionati ai sensi art. 34 comma 3 lett. c), a prescindere dai suoi indistinti contorni applicativi andrebbe tendenzialmente evitata per il grave danno all'immagine che potrebbe derivarne se non opportunamente gestita la comunicazione. In sintesi, la capacità di adempiere agli obblighi in caso di violazione dipende dal grado di preparazione preventiva a questa eventualità, grado di preparazione che è anche elemento utile a valutare la *compliance* del titolare. Lo stesso accesso alle eccezioni appena menzionate presuppone la capacità di dimostrare «conformemente al principio di responsabilizzazione» che «è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche» e dunque presuppone un piano di analisi e di (re)azione idoneo.

È di tutta evidenza che la prevenzione e la reazione alle violazioni sono parte integrante di un unico processo di adeguamento alla normativa che presenta certo dei costi, ma che offre opportunità di riorganizzazione e permette di minimizzare i rischi. Un processo che influenza scelte tecniche, revisioni degli accordi e delle deleghe interne ed esterne relative ai trattamenti del titolare. Esso consiglierà, per esempio, scelte di segregazione dei dati o di tecniche di cifratura particolari piuttosto che di disegno dei processi di trattamento strettamente connessi alle procedure legate alle violazioni dei dati. Sovente poi la violazione coinvolge direttamente o indirettamente terze parti che magari concorrono all'erogazione di un servizio per conto del titolare del trattamento e sarà necessario disciplinare il loro coinvolgimento nel processo di prevenzione e di reazione.
Non va poi dimenticato che le scelte del titolare in materia di comunicazioni e notifiche hanno evidenti riflessi sul piano delle responsabilità e della *compliance* ed ovviamente non escludono mai la prerogativa (art. 58, comma 2, lett. e) delle autorità di controllo di «ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali.

La gestione del Data Breach
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 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 numerosi 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 contro il Data Breach
Al fine di prevenire una violazione di Data Breach è necessario utilizzare un modello di sicurezza informatica così strutturato:

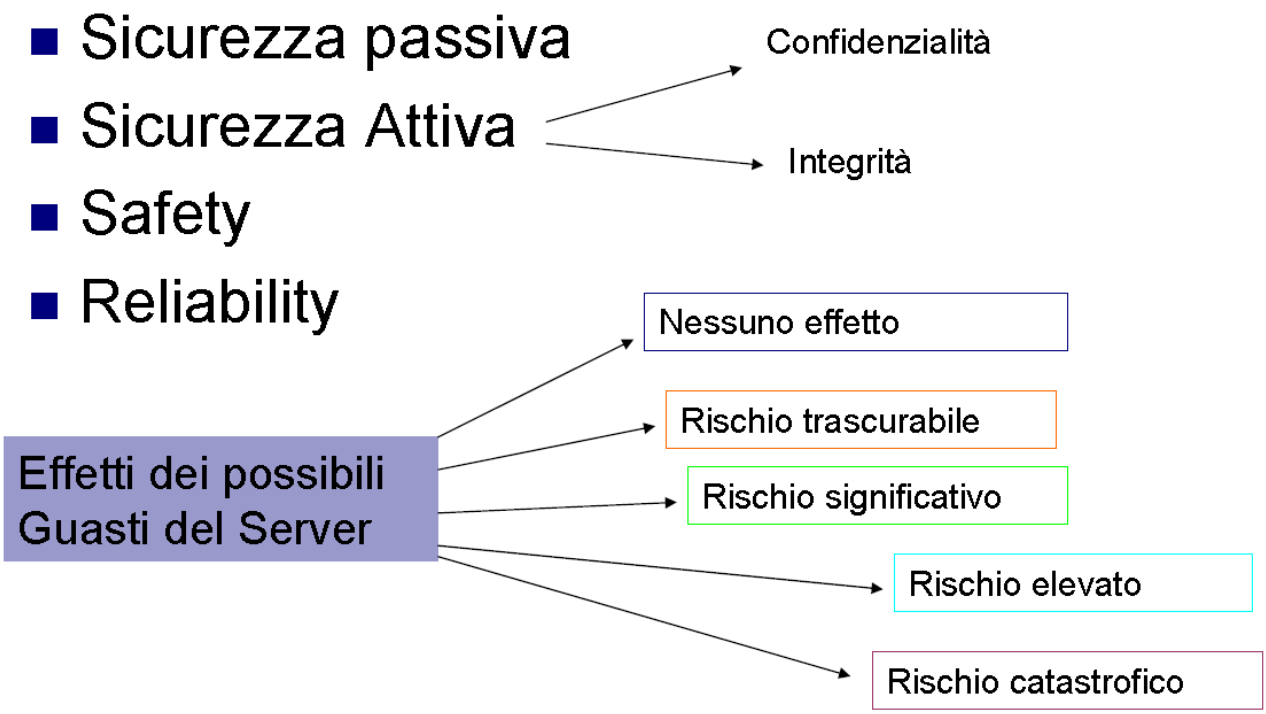


Figura 1 – Un modello di sicurezza

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;
- gestione continuità operativa (Business Continuity Management);
- Neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari e dagli effetti dei guasti;
- adeguatezza (Compliance);
- Evitare il mancato rispetto delle leggi civili, penali e di qualsiasi requisito di sicurezza;
- Per elevare l'efficacia e minimizzare l'interferenza per il processo di verifica del sistema;

Effettuare test periodici

È 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. È altresì, 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.

2.4 Tenere un registro di Data Breach

Il DPO (Data Protection Officer) 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

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 "compliant" rispetto a leggi, best practices, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test

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" e cioè 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. 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

2.5 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 in piano di Remediation.

Nello specifico il servizio di Cyber Data Breach Incident Response permette di essere compliant 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.

3. Illeciti e sanzioni

La violazione della disciplina in tema di Data Breach notification (art. 33, Regolamento UE) e la 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)) del Regolamento UE.

Nel seguente grafico (Fonte Ponemon 2020) vengono analizzati i tempi ed i costi che sosteniamo per individuare e gestire un Data Breach.

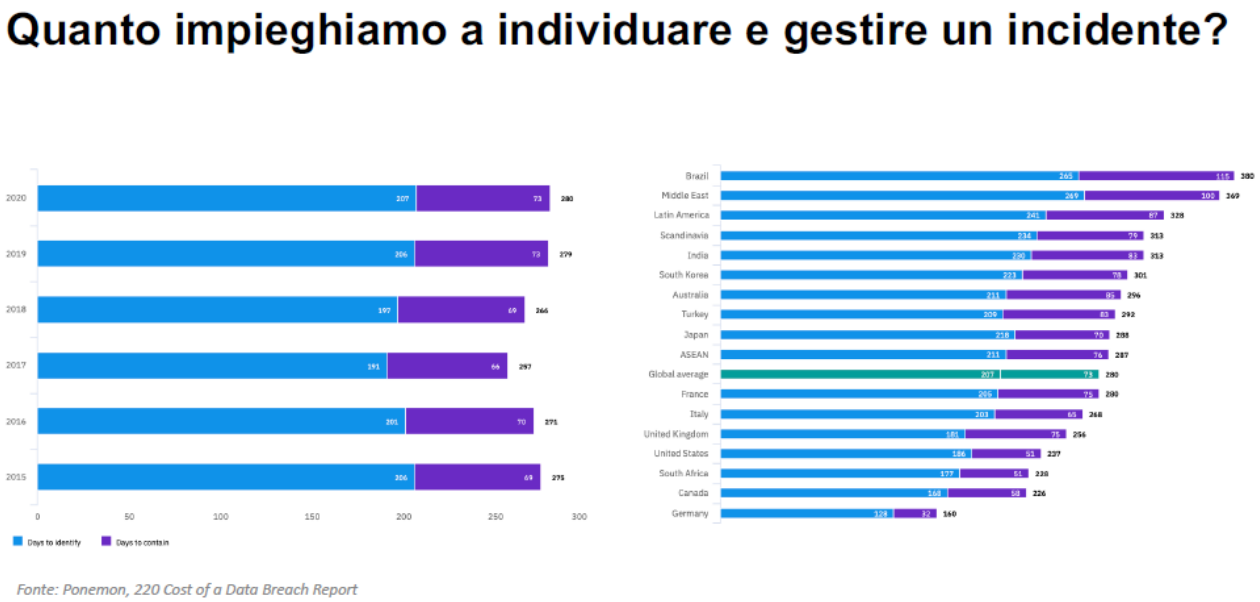


Figura 2 – I costi del data breach

4. Le fattispecie giuridiche di Data Breach introdotte dal Dlgs 101/2018 che ha modificato il codice sulla privacy (Dlgs 196/2003)

Il sistema sanzionatorio del Regolamento UE 679/2016 contempla sia sanzioni amministrative che penali stabilito ed è regolato dagli articoli 83 e 84 e distingue tre diverse sanzioni ai paragrafi 4,5 e 6 dell'articolo 83. Inoltre, il Dlgs 101/2018 ha introdotto i seguenti illeciti penali prevedendo:

- Il trattamento illecito di dati personali;
- L'acquisizione fraudolenta;
- Le false dichiarazioni rese al Garante

In tali fattispecie rientra anche la nomina del DPO nelle pubbliche amministrazioni sia centrali che locali la quale procede molto a rilento e non va meglio per quanto riguarda l'adozione delle misure tecniche informatiche ed organizzative in capo al titolare. Ecco cosa rischiano le amministrazioni inadempienti in termini di sanzioni amministrative ed illeciti penali.

Solo una pubblica amministrazione locale su tre avrebbe provveduto ad effettuare la nomina del DPO, come previsto dal GDPR, e la stragrande maggioranza non ha neanche comunicato il nominativo tramite la procedura telematica messa a disposizione dal Garante Privacy. Lo rivelano le stime pubblicate da organi di stampa autorevoli come il Sole 24 ore.

Se da un lato gli enti locali, alla scadenza del 25 maggio 2018, hanno provveduto mediante apposito atto deliberativo di consiglio comunale all'approvazione formale dello schema di adeguamento al regolamento Ue 679/2016 con la contestuale approvazione del registro dei trattamenti, molte amministrazioni ad oggi non solo non hanno deliberato ma addirittura non hanno neanche proceduto ad effettuare la nomina formale DPO, facendo riferimento alle disposizioni normative che di fatto con il Decreto Legislativo n° 51 del 18 maggio 2018 prorogavano alcuni adempimenti

obbligatori al 21 agosto 2018 introdotti dal Regolamento UE 679/2016 ma non la nomina del DPO che restava ferma al 25 maggio 2018. Inoltre, molti enti locali hanno utilizzato soprattutto la nomina del DPO come persona giuridica. A tale proposito basta citare, in Calabria, il Centro Servizi Territoriali Asmenet Calabria, società consortile formata da comuni, dove la maggior parte degli enti consorziati ha provveduto ad effettuare la nomina congiunta del Responsabile della Protezione dei dati (DPO) come persona giuridica.
Di contro alcune amministrazioni, per ragioni di contenimento della spesa pubblica e spending review hanno nominato al loro interno il responsabile della protezione dei dati individuandolo in dipendenti pubblici che, a mio modo di vedere e di pensare e, secondo quanto previsto dall'Autorità Garante sulla privacy, non erano in possesso dei requisiti e senza apposita esperienza professionale su tematiche di protezione dati e di privacy assessment.

4.2 L'adozione di misure tecniche informatiche e organizzative

Se da un alto ancora in Italia nella pubblica amministrazione locale, la situazione relativa alla nomina del DPO assume dimensioni allarmanti, per quanto concerne invece l'adozione di misure tecniche informatiche ed organizzative che stanno in capo al Titolare secondo quanto previsto dal regolamento e dal Decreto Legislativo n° 51 del 18 maggio 2018 che è andato in vigore dal 21 agosto 2018 la geografia che viene prospettata è devastante.
La stragrande maggioranza degli enti locali di piccole e medie dimensioni non utilizza idonei strumenti di protezione di accesso alla rete, tecniche di crittografia dei dati, etc. ignorando quelle che sono le sanzioni amministrative e penali che il regolamento UE 679/2016 ed il Decreto Legislativo n° 51 del 18 maggio 2018 e cioè:

- ai sensi dell'articolo 16 commi 1 e 2, il titolare del trattamento, tenuto conto delle cognizioni tecniche disponibili e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, l'adozione di misure tecniche e organizzative adeguate, quale la pseudonimizzazione, per garantire la protezione dei dati e per tutelare i diritti degli interessati, in conformità alle norme del presente decreto;
- inoltre, mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;
- ai sensi dell'articolo 25 il titolare del trattamento e il responsabile del trattamento, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati. Per il trattamento automatizzato il titolare o il responsabile del trattamento, previa valutazione dei rischi, adottano misure volte a:

vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);

garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

5. Le sanzioni amministrative in caso di Data Breach

La mancata adozione di tali misure di sicurezza informatica prevede la comminazione di sanzioni amministrative ed illeciti penali, tra cui per quanto concerne le sanzioni amministrative ai sensi dell'articolo 42 del suddetto decreto sono le seguenti:

- Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, la violazione delle disposizioni di cui all'articolo 3, comma 1, lettere a), b), d), e) ed f), all'articolo 4, commi 2 e 3, all'articolo 6, commi 3e 4, all'articolo 7, all'articolo 8, è punita con la sanzione amministrativa del pagamento di una somma da 50.000 euro a 150.000 euro. La medesima sanzione amministrativa si applica al trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale in assenza della decisione di adeguatezza della Commissione europea, salvo quanto previsto dagli articoli 33 e 34.
- Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, è punita con la sanzione amministrativa del pagamento di una somma da 20.000 euro a 80.000 euro la violazione delle disposizioni di cui all'articolo 14, comma 2. Con la medesima sanzione è punita la violazione delle disposizioni di cui all'articolo 17, comma 2, all'articolo 18, commi 1, 2, 3 e 4, all'articolo 19, all'articolo 20, all'articolo 21, all'articolo 22, all'articolo 23, all'articolo 24, commi 1 e 4, all'articolo 26, all'articolo 27, all'articolo 28, commi 1 e 4, all'articolo 29, comma 2.

Nella determinazione della sanzione amministrativa da applicare secondo quanto previsto dai commi 1 e 2 si tiene conto dei criteri di cui all'articolo 83, paragrafo 2, lettere a), b), c), d), e), f), g), h), i), k), del regolamento UE.

Per quanto concerne le sanzioni penali, con la pubblicazione del Dlgs 101/2018, il Capo– Illeciti penali del novellato Dlgs 196/2003 ha introdotto i seguenti articoli:

Articolo 167 – Trattamento illecito dei dati

"1. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.*

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

Articolo 168. Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Articolo 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

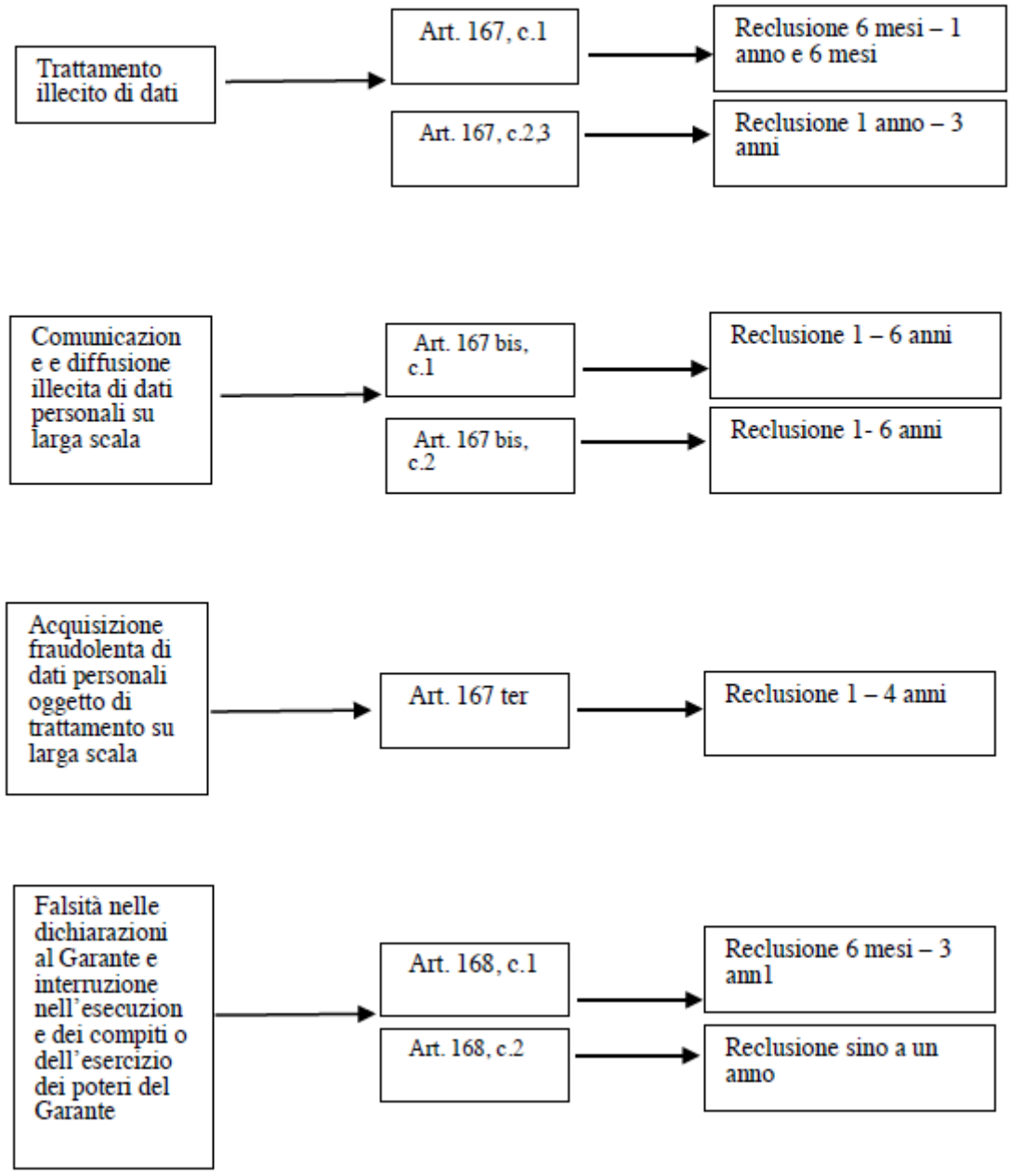
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Art. 170. Inosservanza di provvedimenti del Garante

1. *Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.*

Nella seguente figura sono così dettagliati:

3. Diagramma sanzioni penali – D.Lgs. n. 101/2018



6. Articoli 82 e 83 del Regolamento

Inoltre, ai sensi degli articoli 82 e 83 del regolamento 679/2016 la mancata adozione di tali attività comporterà le comminazioni di sanzioni previste dal regolamento e cioè nel dettaglio:
Chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal responsabile del trattamento
– Articolo 82 (Diritto al risarcimento e responsabilità)
Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti

Articolo 83… Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.
2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure.
4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EURO, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a. gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b. gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c. gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a. i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b. i diritti degli interessati a norma degli articoli da 12 a 22;
c. i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d. qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
e. l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
7.Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

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

Il General Data Protection Regulation introduce l'obbligo di notificare una violazione dei dati personali all'autorità di controllo nazionale competente (di seguito "SA- Security Authority" in Italia la Data Protection Authority – Autorità Garante sulla Privacy) e, in alcuni casi, di comunicare la violazione alle persone i cui dati personali sono stati interessati dalla violazione (Articoli 33 e 34). Il Gruppo di lavoro articolo 29 (WP29 Working Party 29) ha già prodotto una guida generale sulla notifica di violazione dei dati nell'ottobre 2017, analizzando le sezioni pertinenti del GDPR (Linee guida sulla notifica di violazione dei dati personali ai sensi del regolamento 2016/679, WP 250) (di seguito "Linee guida WP250). Tuttavia, a causa della sua natura e tempistica, questa documentazione non ha affrontato, in maniera esaustiva e completa, tutte le casistiche pratiche in modo sufficientemente dettagliato. Pertanto, è sorta la necessità di redigere delle linee guida orientata alla pratica e basata sui casi che utilizzi le esperienze acquisite dalle autorità di vigilanza poiché il GDPR è applicabile.

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.
Nell'ambito di qualsiasi tentativo di porre rimedio a una violazione di dati (Data Breach), il titolare del trattamento dovrebbe prima essere in grado di riconoscerla. Il GDPR definisce una "violazione dei dati personali" nell'articolo 4 (12) come "una violazione della sicurezza che porta alla distruzione, perdita, alterazione accidentale o illegale, divulgazione non autorizzata o accesso ai dati personali trasmessi, archiviati o altrimenti elaborati"
Nel suo parere 03/2014 sulla notifica delle violazioni e nelle sue linee guida WP 250, il WP29 ha spiegato che le violazioni possono essere classificate in base ai seguenti tre noti principi di sicurezza delle informazioni:
• "Violazione della riservatezza": in caso di divulgazione non autorizzata o accidentale di o accesso a dati personali.
• "Violazione dell'integrità": in caso di alterazione non autorizzata o accidentale dei dati personali.
• "Violazione della disponibilità": in caso di perdita accidentale o non autorizzata dell'accesso o distruzione dei dati personali.
Una violazione può potenzialmente avere una serie di effetti negativi significativi sulle persone, che possono provocare danni fisici, materiali o immateriali. Il GDPR spiega che ciò può includere perdita di controllo sui propri dati personali, limitazione dei loro diritti, discriminazione, furto di identità o frode, perdita finanziaria, annullamento non autorizzato della pseudonimizzazione, danno alla reputazione (brand reputation) e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro svantaggio economico o sociale significativo per tali individui. Uno degli obblighi più importanti del responsabile del trattamento dei dati è valutare questi rischi per i diritti e le libertà degli interessati e attuare misure tecniche e organizzative adeguate ad affrontarli. Di conseguenza, il GDPR richiede al titolare del trattamento di:

- documentare eventuali violazioni dei dati personali, compresi i fatti relativi alla violazione dei dati personali, i suoi effetti e le azioni correttive intraprese (Articolo 33 GDPR);
- notificare la violazione dei dati personali all'autorità di controllo, a meno che non sia improbabile che la violazione dei dati comporti un rischio per i diritti e le libertà delle persone fisiche (Articolo 33 GDPR);
- comunicare la violazione dei dati personali all'interessato quando è probabile che la violazione dei dati personali comporti un rischio elevato per i diritti e le libertà delle persone fisiche.

Le violazioni dei dati sono problemi in sé e per sé, ma sono anche sintomi di un regime di sicurezza dei dati vulnerabile, forse obsoleto; quindi, indicano debolezze del sistema da affrontare. In generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, poiché diverse conseguenze sono per natura irreversibili. Prima che un titolare del trattamento possa valutare completamente il rischio derivante da una violazione causata da una qualche forma di attacco, è necessario identificare la causa principale del problema, al fine di identificare se eventuali vulnerabilità che hanno dato origine all'incidente sono ancora presenti e lo sono ancora sfruttabile. In molti casi il responsabile del trattamento è in grado di identificare che l'incidente potrebbe comportare un rischio e deve quindi essere informato. In altri casi non è necessario posticipare la notifica fino a quando il rischio e l'impatto che circondano la violazione non sono stati completamente valutati, poiché la valutazione completa del rischio può avvenire parallelamente alla notifica e le informazioni così ottenute possono essere fornite all'autorità di vigilanza in fasi senza indebito ulteriore ritardo (Articolo 34 GDPR).
La violazione dovrebbe essere notificata quando il responsabile del trattamento ritiene che possa comportare un rischio per i diritti e le libertà dell'interessato. I titolari del trattamento dovrebbero

effettuare questa valutazione nel momento in cui vengono a conoscenza della violazione. Il responsabile del trattamento non dovrebbe attendere un esame forense dettagliato e le (prime) fasi di mitigazione prima di valutare se la violazione dei dati possa o meno comportare un rischio e quindi dovrebbe essere informato.
Se un controllore effettua un'autovalutazione del rischio come improbabile, ma risulta che il rischio si concretizza, la SA competente può utilizzare i suoi poteri correttivi e può decidere di sanzionare.
Ogni titolare del trattamento dovrebbe disporre di piani e procedure per la gestione di eventuali violazioni dei dati. Le organizzazioni dovrebbero avere chiare linee di riporto e persone responsabili di alcuni aspetti del processo di recupero.
La formazione e la consapevolezza sulle questioni relative alla protezione dei dati da parte del personale del responsabile del trattamento, concentrandosi sulla gestione della violazione dei dati personali (identificazione di un incidente di violazione dei dati personali e ulteriori azioni da intraprendere, ecc.) Sono essenziali per i responsabili del trattamento. Questa formazione dovrebbe essere ripetuta regolarmente, a seconda del tipo di attività di elaborazione e delle dimensioni del titolare del trattamento, affrontando le ultime tendenze e gli avvisi provenienti da attacchi informatici o altri incidenti di sicurezza. Il principio di responsabilità (accountability) e il concetto di protezione dei dati fin dalla progettazione (privacy by design) potrebbero incorporare analisi che alimentano il "Manuale sul trattamento della violazione dei dati personali" del titolare del trattamento che mira a stabilire fatti per ogni aspetto del trattamento in ciascuna fase principale dell'operazione. Un manuale di questo tipo preparato in anticipo fornirebbe una fonte di informazioni molto più rapida per consentire ai responsabili del trattamento di mitigare i rischi e adempiere agli obblighi senza indebiti ritardi. Ciò garantirebbe che, se si dovesse verificare una violazione dei dati personali, le persone nell'organizzazione saprebbero cosa fare e l'incidente sarebbe molto probabilmente gestito più rapidamente che se non ci fossero mitigazioni o piani in atto.
Queste linee guida strutturano i casi in base a determinate categorie di violazioni (ad es. Attacchi ransomware). In ogni caso, quando si tratta di una determinata categoria di violazioni, sono necessarie determinate misure di mitigazione. Queste misure non sono necessariamente ripetute in ogni caso di analisi appartenente alla stessa categoria di violazioni. Per i casi appartenenti alla stessa categoria sono previste solo le differenze.
La documentazione interna di una violazione è un obbligo indipendente dai rischi relativi alla violazione e deve essere eseguita in ogni caso. I casi presentati di seguito cercano di far luce sull'opportunità di notificare o meno la violazione alla SA e di comunicarla agli interessati.

8. Le misure tecniche ed organizzative per prevenire e mitigare gli impatti di attacchi Ransomware, attacchi di esfiltrazione dati e il Social Engineering

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.
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.

Figura 2 – Le famiglie di ransomware

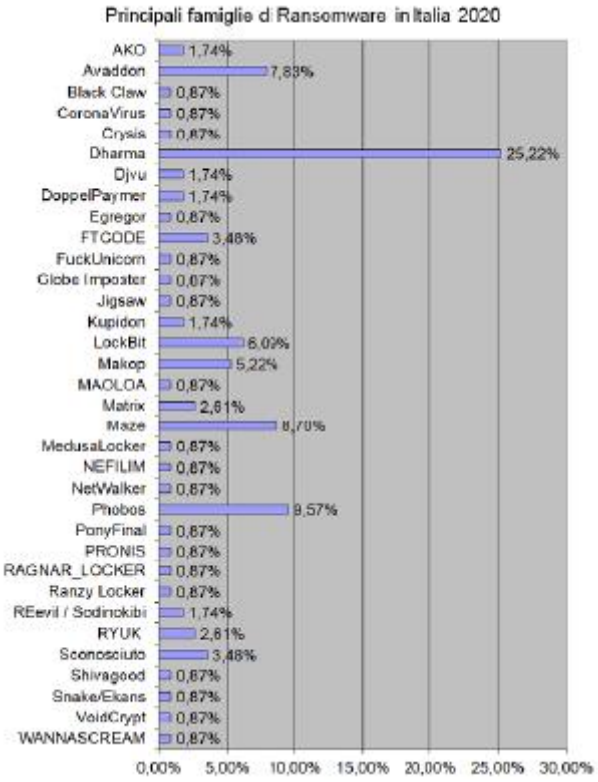


Figura 3 – Le principali famigli in Italia

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

Figura 2 – Fackunicorn- Il ransomware italiano

8.1 Ransomware con backup corretto e senza esfiltrazione

In questa casistica un backup è sempre disponibile e i dati vengono ripristinati poche ore dopo l'attacco. La violazione non comporta alcuna conseguenza sull'operatività quotidiana del titolare del trattamento.

- **Misure preventive e valutazione del rischio.**

Come per tutti i rischi posti da attori esterni, la probabilità che un attacco ransomware abbia successo può essere drasticamente ridotta rafforzando la sicurezza dell'ambiente di controllo dei dati. La maggior parte di queste violazioni può essere prevenuta assicurandosi che siano state adottate misure di sicurezza organizzative, fisiche e tecnologiche adeguate. Esempi di tali misure sono la corretta gestione delle patch e l'uso di un appropriato sistema di rilevamento antimalware. Avere un backup corretto e separato aiuterà a mitigare le conseguenze di un attacco riuscito se dovesse verificarsi. Inoltre, un programma di istruzione, formazione e consapevolezza sulla sicurezza dei dipendenti (SETA- Security, Education, Training e Awareness) aiuterà a prevenire e riconoscere questo tipo di attacco. Tra queste misure, una corretta gestione delle patch che assicuri che i sistemi siano aggiornati e tutte le vulnerabilità note dei sistemi distribuiti siano corrette è una delle più importanti poiché la maggior parte delle Gli attacchi ransomware sfruttano vulnerabilità ben note. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e identificare il tipo di codice dannoso per comprendere le possibili conseguenze dell'attacco. Tra i rischi da considerare c'è il rischio che i dati siano stati esfiltrati senza lasciare traccia nei log dei sistemi. Il titolare del trattamento dovrebbe considerare l'impatto e la gravità della violazione. Avere un adeguato regime di backup rende gli effetti della violazione meno gravi ed in questo modo il titolare del trattamento è in grado di utilizzarlo efficacemente.

- **Mitigazione e obblighi**

Senza un backup, il responsabile del trattamento può intraprendere alcune misure per porre rimedio alla perdita di dati personali e i dati devono essere raccolti di nuovo. Senza un backup, i dati vengono persi e la gravità può aumentare perché possono verificarsi anche rischi o impatti per gli individui.
La tempestività di un ripristino efficace dei dati dal backup immediatamente disponibile è una variabile chiave quando si analizza la violazione. La specifica di un arco temporale predefinito per ripristinare i dati compromessi dipende dalle circostanze uniche della violazione. Il GDPR stabilisce che una violazione dei dati personali deve essere notificata senza indebito ritardo e, ove possibile,

non oltre 72 ore. Pertanto, si potrebbe stabilire che il superamento del limite di 72 ore è sconsigliabile in ogni caso, ma quando si tratta di casi ad alto livello di rischio, anche il rispetto di questo termine può essere considerato insoddisfacente.
Tuttavia, poiché tutte le violazioni dei dati, dovrebbero essere documentate ai sensi dell'articolo 33, paragrafo 5, l'organizzazione potrebbe anche aver bisogno (o successivamente essere richiesto dalla SA) di aggiornare e correggere le proprie misure e procedure di gestione della sicurezza dei dati personali e organizzativi e tecnici.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	X	X

8.2 Ransomware senza un backup adeguato

In questa casistica nessun backup era disponibile in formato elettronico e la maggior parte dei dati è stata ripristinata da backup cartacei. Il ripristino dei dati ha richiesto 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti

- **Misure preventive e valutazione del rischio**

Il titolare del trattamento avrebbe dovuto adottare le stesse misure preventive del caso precedente. La principale differenza rispetto al caso precedente è la mancanza di un backup elettronico e la mancanza di crittografia a riposo. Ciò porta a differenze critiche nei passaggi seguenti. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e identificare il tipo di codice dannoso per comprendere le possibili conseguenze dell'attacco. In questo caso il ransomware ha crittografato i dati personali senza esfiltrarli. Di conseguenza, sembra che i rischi per i diritti e le libertà degli interessati derivino dalla mancanza di disponibilità dei dati personali e la riservatezza dei dati personali non sia compromessa. Un esame approfondito dei log del firewall e delle sue implicazioni è essenziale per determinare il rischio. Il responsabile del trattamento dovrebbe presentare i risultati fattuali di queste indagini su richiesta. Il responsabile del trattamento deve tenere presente che se l'attacco è più sofisticato, il malware ha la funzionalità per modificare i file di registro e rimuovere la traccia. Quindi, dato che i registri non vengono inoltrati o replicati a un server di registro centrale, anche dopo un'indagine approfondita che ha stabilito che i dati personali non sono stati esfiltrati dall'aggressore, il titolare del trattamento non può affermare che l'assenza di una voce di registro dimostra l'assenza di esfiltrazione; quindi, la probabilità di una violazione della riservatezza non può essere completamente eliminata.
Il titolare del trattamento dovrebbe valutare i rischi di questa violazione se l'aggressore ha avuto accesso ai dati. Durante la valutazione del rischio, il titolare del trattamento dovrebbe anche prendere in considerazione la natura, la sensibilità, il volume e il contesto dei dati personali interessati dalla violazione. In questo caso non sono interessate categorie speciali di dati personali e la quantità di dati violati e il numero di soggetti interessati sono bassi.
La raccolta di informazioni esatte sull'accesso non autorizzato è fondamentale per determinare il livello di rischio e prevenire un attacco nuovo o continuato. Se i dati fossero stati copiati dal database, sarebbe stato ovviamente un fattore di aumento del rischio. In caso di incertezza sulle specificità dell'accesso illegittimo, si dovrebbe considerare lo scenario peggiore e il rischio dovrebbe essere valutato di conseguenza.
L'assenza di un database di backup può essere considerata un fattore di aumento del rischio a seconda della gravità delle conseguenze per gli interessati derivanti dalla mancanza di disponibilità dei dati.

- **Mitigazione e obblighi**

Senza un backup, il responsabile del trattamento può intraprendere alcune misure per porre rimedio alla perdita di dati personali e i dati devono essere raccolti di nuovo, a meno che non sia disponibile un'altra fonte (ad esempio e-mail di conferma dell'ordine). Senza un backup, i dati potrebbero andare persi e la gravità dipenderà dall'impatto per gli individui. Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico. (tutto ciò dipenderà dalla complessità e dalla struttura dei dati personali. Negli scenari più complessi, ristabilire l'integrità dei dati, la coerenza con i metadati, garantire le relazioni corrette all'interno delle strutture dei dati e controllare l'accuratezza dei dati può richiedere risorse e sforzi significativi) se i dati sono ancora disponibili su supporto cartaceo, ma data la mancanza di un database elettronico di backup, si ritiene necessaria una notifica alla SA, in quanto il ripristino dei dati ha richiesto tempo e potrebbe causare alcuni ritardi nella consegna degli ordini ai clienti e una notevole quantità di metadati (es. log, timestamp) potrebbe non essere recuperabile.
Informare gli interessati della violazione può anche dipendere dal periodo di tempo in cui i dati personali non sono disponibili e dalle difficoltà che potrebbe causare nel funzionamento del responsabile del trattamento di conseguenza (ad esempio ritardi nel trasferimento dei pagamenti dei dipendenti). Inoltre, potrebbe non essere possibile evitare di informare gli interessati se il loro contributo è necessario per ripristinare i dati crittografati.
Questo caso serve da esempio per un attacco ransomware con rischio per i diritti e le libertà degli interessati, ma che non raggiunge un rischio elevato. Dovrebbe essere documentato in conformità dell'articolo 33, paragrafo 5, e notificato alla SA ai sensi dell'articolo 33, paragrafo 1. L'organizzazione potrebbe anche aver bisogno (o essere richiesta dalla SA) per aggiornare e correggere le proprie misure e procedure di gestione della sicurezza dei dati personali e organizzativi e tecnici.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	X

8.3 Ransomware con backup e senza esfiltrazione in una pubblica amministrazione

I dati personali interessati dalla violazione si riferiscono ai dipendenti e ai pazienti, che rappresentavano migliaia di individui. I backup erano disponibili in formato elettronico. La maggior parte dei dati è stata ripristinata ma questa operazione è durata due giorni lavorativi e ha comportato notevoli ritardi nel trattamento dei pazienti con intervento chirurgico annullato / rinviato, e un abbassamento del livello di servizio per indisponibilità dei sistemi.

- **Misure preventive e valutazione del rischio**

La quantità di dati violati e il numero di soggetti interessati sono elevati, perché gli ospedali di solito elaborano grandi quantità di dati. L'indisponibilità dei dati ha un forte impatto su una parte sostanziale degli interessati. Inoltre, esiste un rischio residuo di elevata gravità per la riservatezza dei dati del paziente. Il tipo di violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono importanti. Anche se esisteva un backup dei dati e poteva essere ripristinato in pochi giorni, esiste ancora un rischio elevato dovuto alla gravità delle conseguenze per gli interessati derivanti dalla mancanza di disponibilità dei dati al momento dell'attacco e dei giorni successivi.

- **Mitigazione e obblighi**

Una notifica alla SA è considerata necessaria, poiché sono coinvolte categorie speciali di dati personali e il ripristino dei dati potrebbe richiedere molto tempo, con conseguenti ritardi maggiori nella cura del paziente. Informare gli interessati della violazione è necessario a causa dell'impatto per i pazienti, anche dopo il ripristino dei dati crittografati. Sebbene i dati relativi a tutti i pazienti trattati in ospedale negli ultimi anni siano stati crittografati, sono stati interessati solo i pazienti che dovevano essere trattati in ospedale durante il periodo in cui il sistema informatico non era disponibile. Il titolare del trattamento dovrebbe comunicare la violazione dei dati direttamente a tali pazienti. La comunicazione diretta agli altri pazienti, alcuni dei quali potrebbero non essere stati ricoverati per più di venti anni, potrebbe non essere richiesta a causa dell'eccezione di cui all'articolo 34, paragrafo 3, lettera c). In tal caso, è invece prevista una comunicazione pubblica o un provvedimento analogo mediante il quale gli interessati sono informati in modo altrettanto efficace. In questo caso, l'ospedale dovrebbe rendere pubblici l'attacco ransomware e i suoi effetti.
Questo caso serve da esempio per un attacco ransomware ad alto rischio per i diritti e le libertà degli interessati. Deve essere documentato in conformità con l'articolo 33 (5), notificato alla SA in conformità con l'articolo 33 e comunicato agli interessati ai sensi dell'articolo 34. L'organizzazione deve inoltre aggiornare e porre rimedio alle proprie misure e procedure di gestione della sicurezza dei dati personali e organizzativi e tecnici e di mitigazione del rischio.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	✓

8.4 Ransomware senza backup e con esfiltrazione

Il tipo di dati violati erano i dati personali di clienti e dipendenti e delle diverse migliaia di persone che utilizzavano i servizi dell'azienda (ad esempio, l'acquisto di biglietti online). Oltre ai dati di identità di base, nella violazione sono coinvolti numeri di carta d'identità e dati finanziari come i dettagli della carta di credito. Esisteva un database di backup, ma è stato anche crittografato dall'autore dell'attacco.

- **Misure preventive e valutazione del rischio**

Sebbene il backup fosse in atto, è stato anche influenzato dall'attacco. Questa disposizione da sola solleva dubbi sulla qualità delle misure di sicurezza IT precedenti del controller e dovrebbe essere ulteriormente esaminata durante l'indagine, poiché in un regime di backup ben progettato il backup deve essere archiviato in modo sicuro senza accesso dal sistema principale, altrimenti potrebbe essere compromesso nello stesso attacco. Questa violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, poiché l'aggressore potrebbe aver modificato e /o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato.
La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di individui interessati è elevato, così come la quantità complessiva di dati personali interessati. Oltre ai dati di identità di base, sono coinvolti anche documenti di identità e dati finanziari come i dettagli della carta di credito. Una violazione dei dati relativa a questi tipi di dati presenta di per sé un rischio elevato e, se elaborati insieme, potrebbero essere utilizzati, tra l'altro, per furto di identità o frode.
A causa di una logica del server difettosa o di controlli organizzativi, i file di backup sono stati colpiti dal ransomware, impedendo il ripristino dei dati e aumentando il rischio.

Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, perché potrebbe portare a danni sia materiali (ad es. Perdita finanziaria poiché i dettagli della carta di credito sono stati influenzati) che non materiali (ad es. colpiti).

- **Mitigazione e obblighi**

Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, in questo caso è obbligatoria anche una notifica alla SA (articolo 33, paragrafo 1) e il responsabile del trattamento è anche obbligato a comunicare la violazione agli interessati (articolo 34). Quest'ultimo potrebbe essere intrapreso da persona a persona, ma per le persone in cui i dati di contatto non sono disponibili il responsabile del trattamento dovrebbe farlo pubblicamente, ad es. mediante notifica sul proprio sito web. In quest'ultimo caso è richiesta una comunicazione precisa e chiara, ben visibile nella home page del titolare del trattamento, con i riferimenti esatti delle relative disposizioni GDPR. L'organizzazione potrebbe anche dover aggiornare e correggere le proprie misure e procedure di gestione della sicurezza dei dati personali e organizzativi e tecnici.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

Misure organizzative e tecniche per prevenire/mitigare gli impatti degli attacchi ransomware
Il fatto che possa aver avuto luogo un attacco ransomware è solitamente un segno di una o più vulnerabilità nel sistema del controller. Ciò vale anche nei casi di ransomware in cui i dati personali sono stati crittografati, ma non sono stati esfiltrati. Indipendentemente dall'esito e dalle conseguenze dell'attacco, l'importanza di una valutazione onnicomprensiva del sistema di sicurezza dei dati, con particolare enfasi sulla sicurezza informatica, non può essere sottolineata abbastanza. Le debolezze e le falle nella sicurezza individuate devono essere documentate e affrontate senza indugio.

Misure consigliate:
L'elenco delle seguenti misure non è in alcun modo esclusivo o completo. L'obiettivo è piuttosto quello di fornire idee di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, quindi il responsabile del trattamento dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione data.

- Mantenere aggiornati il firmware, il sistema operativo e il software applicativo sui server, sulle macchine client, sui componenti di rete attivi e su qualsiasi altra macchina sulla stessa LAN (inclusi i dispositivi Wi-Fi). Garantire che tutte le ragionevoli misure di sicurezza IT siano in atto, assicurandosi che siano efficaci e mantenendole regolarmente aggiornate quando l'elaborazione o le circostanze cambiano o evolvono. Ciò include la conservazione di registri dettagliati di quali patch vengono applicate e in quale data e ora.
- Progettazione e organizzazione di sistemi e infrastrutture di elaborazione per segmentare o isolare reti e sistemi di dati per evitare la propagazione di malware all'interno dell'organizzazione e verso sistemi esterni.
- L'esistenza di una procedura di backup aggiornata, sicura e testata. I supporti per il backup a medio e lungo termine devono essere tenuti separati dall'archiviazione dei dati operativi e fuori dalla portata di terze parti anche in caso di attacco riuscito (come backup incrementale giornaliero e backup completo settimanale).
- Disporre/ottenere un software anti-malware appropriato, aggiornato, efficace e integrato.
- Disporre di un firewall appropriato, aggiornato, efficace e integrato e di un sistema di rilevamento e prevenzione delle intrusioni. Dirigere il traffico di rete attraverso il firewall

rilevamento delle intrusioni, anche in caso di ufficio da casa o lavoro mobile (ad esempio utilizzando connessioni VPN a meccanismi di sicurezza organizzativi quando si accede a Internet).

- Formazione dei dipendenti sui metodi per riconoscere e prevenire gli attacchi IT. Il titolare del trattamento dovrebbe fornire mezzi per stabilire se le e-mail e i messaggi ottenuti con altri mezzi di comunicazione sono autentici e affidabili. I dipendenti dovrebbero essere addestrati a riconoscere quando un attacco di questo tipo si è reso conto, come rimuovere l'endpoint dalla rete e il loro obbligo di segnalarlo immediatamente al responsabile della sicurezza.
- Sottolineare la necessità di identificare il tipo di codice dannoso per vedere le conseguenze dell'attacco ed essere in grado di trovare le giuste misure per mitigare il rischio. Nel caso in cui un attacco ransomware abbia avuto successo e non sia disponibile alcun backup, per recuperare i dati possono essere applicati strumenti disponibili come quelli del progetto "no more ransom" (nomoreransom.org). Tuttavia, nel caso in cui sia disponibile un backup sicuro, è consigliabile ripristinare i dati da esso.
- Inoltro o replica di tutti i registri a un server di registro centrale (possibilmente includendo la firma o il timestamp crittografico delle voci di registro).
- Crittografia e autenticazione avanzate, in particolare per l'accesso amministrativo ai sistemi IT (2FA), gestione di chiavi e password appropriate.
- Test di vulnerabilità e penetrazione su base regolare.
- Istituire un CSIRT (Computer Security Incident Response Team) o un Computer Emergency Response Team (CERT) all'interno dell'organizzazione o unirsi a un CSIRT/CERT collettivo. Crea un piano di risposta agli incidenti, un piano di ripristino di emergenza e un piano di continuità operativa e assicurati che siano accuratamente testati.
- Quando si valutano le contromisure, è necessario rivedere l'analisi del rischio.

9. Attacchi di esfiltrazione di dati

Attacchi che sfruttano le vulnerabilità nei servizi offerti dal titolare del trattamento a terzi su Internet, ad es. commessi tramite attacchi injection (ad es. SQL injection, path trasversali), compromissione del sito Web e metodi simili, possono assomigliare ad attacchi di ransomware in quanto il rischio deriva dall'azione di una terza parte non autorizzata, ma questi attacchi in genere mirano a copiare, esfiltrare e abusare dati personali per fini dannosi. Si tratta quindi principalmente di violazioni della riservatezza e, possibilmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, sono molte le misure a disposizione dei titolari che possono ridurre sostanzialmente il rischio di una corretta esecuzione di un attacco.

9.1 Esfiltrazione dei dati delle domande di lavoro da un sito web

Il particolare toolkit malware installato aveva funzionalità che consentivano all'aggressore di rimuovere qualsiasi cronologia di esfiltrazione e consentivano anche il monitoraggio dell'elaborazione sul server e l'acquisizione di dati personali. Il toolkit è stato scoperto solo un mese dopo la sua installazione.

- **Misure preventive e valutazione del rischio**

La sicurezza dell'ambiente del controllo dei dati è estremamente importante, in quanto la maggior parte di queste violazioni può essere prevenuta assicurando che tutti i sistemi siano costantemente aggiornati, i dati sensibili siano crittografati e le applicazioni siano sviluppate secondo elevati standard di sicurezza come l'autenticazione forte, misure contro la forza bruta, attacchi, "fuga"(La

fuga o la sanificazione degli input dell'utente è una forma di convalida dell'input, che garantisce che solo i dati correttamente formattati vengano inseriti in un sistema informativo) o "disinfezione" input degli utenti, ecc. Sono inoltre necessari audit periodici della sicurezza IT, valutazioni delle vulnerabilità e test di penetrazione per rilevare in anticipo questi tipi di vulnerabilità e risolverli. In questo caso particolare, gli strumenti di monitoraggio dell'integrità dei file nell'ambiente di produzione potrebbero aver contribuito a rilevare l'iniezione di codice.

- **Mitigazione e obblighi**

Se possibile, dopo aver risolto il problema, il database deve essere confrontato con quello archiviato in un backup sicuro. Le esperienze tratte dalla violazione dovrebbero essere utilizzate per l'aggiornamento dell'infrastruttura IT. Il responsabile del trattamento dei dati dovrebbe riportare tutti i sistemi IT interessati a uno stato pulito noto, porre rimedio alla vulnerabilità e attuare nuove misure di sicurezza per evitare violazioni dei dati simili in futuro, ad es. controlli di integrità dei file e controlli di sicurezza. Se i dati personali non sono stati solo esfiltrati, ma anche cancellati, il responsabile del trattamento deve intraprendere azioni sistematiche per recuperare i dati personali nello stato in cui si trovavano prima della violazione. Potrebbe essere necessario applicare backup completi, modifiche incrementali e quindi eventualmente rieseguire l'elaborazione dall'ultimo backup incrementale, il che richiede che il controller sia in grado di replicare le modifiche apportate dall'ultimo backup. Ciò potrebbe richiedere che il controller abbia il sistema progettato per conservare i file di input giornalieri nel caso in cui debbano essere elaborati di nuovo e richiede un metodo di archiviazione robusto e una politica di conservazione adeguata.
Alla luce di quanto sopra, poiché è probabile che la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, gli interessati dovrebbero esserne assolutamente informati (articolo 34, paragrafo 1), il che ovviamente significa che il pertinente Anche le SA dovrebbero essere coinvolte sotto forma di notifica di violazione dei dati. La documentazione della violazione è obbligatoria ai sensi dell'articolo 33, paragrafo 5, del GDPR facilita la valutazione della situazione.
Il titolare del trattamento dovrebbe sempre iniziare a indagare sulla violazione identificando il tipo di attacco e le sue modalità, al fine di valutare le misure da adottare. Per renderlo veloce ed efficiente, il responsabile del trattamento dei dati dovrebbe disporre di un piano di risposta all'incidente che specifichi le fasi rapide e necessarie per assumere il controllo dell'incidente. In questo caso particolare, il tipo di violazione è stato un fattore di aumento del rischio poiché non solo è stata ridotta la riservatezza dei dati, ma l'infiltrato aveva anche i mezzi per stabilire modifiche nel sistema; quindi, anche l'integrità dei dati è diventata discutibile.
La natura, la sensibilità e il volume dei dati personali interessati dalla violazione dovrebbero essere valutati per determinare in quale misura la violazione abbia interessato gli interessati. Sebbene non siano state interessate categorie speciali di dati personali, i dati a cui si accede contengono informazioni considerevoli sugli individui dai moduli online e tali dati potrebbero essere utilizzati in modo improprio in diversi modi (targeting con marketing non richiesto, furto di identità, ecc.), Quindi il la gravità delle conseguenze dovrebbe aumentare il rischio per i diritti e le libertà degli interessati.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

9.2 Esfiltrazione di password con hash da un sito web

Una vulnerabilità di SQL Injection è stata sfruttata per ottenere l'accesso a un database del server di un sito web di cucina. Gli utenti potevano solo scegliere pseudonimi arbitrari come nomi utente. L'uso di indirizzi e-mail a tale scopo è stato sconsigliato. Le password memorizzate nel database sono state sottoposte ad hashing con un algoritmo potente e il sale non è stato compromesso. Dati interessati: password con hash di 1.200 utenti. Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite e-mail e ha chiesto loro di modificare la password, soprattutto se la stessa password è stata utilizzata per altri servizi.

- **Misure preventive e valutazione del rischio**

In questo caso particolare, la riservatezza dei dati è compromessa, ma le password nel database sono state sottoposte ad hashing con un metodo aggiornato, il che ridurrebbe il rischio relativo alla natura, alla sensibilità e al volume dei dati personali. Questo caso non presenta rischi per i diritti e le libertà degli interessati. Inoltre, nessuna informazione di contatto (ad esempio indirizzi e-mail o numeri di telefono) degli interessati è stata compromessa, il che significa che non vi è alcun rischio significativo per gli interessati di essere presi di mira da tentativi di frode (ad esempio ricezione di e-mail di phishing o messaggi di testo fraudolenti e chiamate telefoniche). Non sono state coinvolte categorie speciali di dati personali. Alcuni nomi utente potrebbero essere considerati dati personali, ma l'oggetto del sito non ammette connotazioni negative. Sebbene sia necessario notare che la valutazione del rischio può cambiare, se il tipo di sito Web ei dati a cui si accede potrebbero rivelare categorie speciali di dati personali (ad es. Sito Web di un partito politico o sindacato). L'utilizzo di una crittografia all'avanguardia potrebbe mitigare gli effetti negativi della violazione. Garantire che un numero limitato di tentativi di accesso sia consentito impedirà il successo degli attacchi di accesso di forza bruta, riducendo così in gran parte i rischi imposti dagli aggressori che già conoscono i nomi utente.

- **Mitigazione e obblighi**

La comunicazione agli interessati in alcuni casi potrebbe essere considerata un fattore attenuante, poiché gli interessati sono anche in grado di compiere i passi necessari per evitare ulteriori danni dalla violazione, ad esempio cambiando la propria password. In questo caso, la notifica non era obbligatoria, ma in molti casi può essere considerata una buona pratica. Il responsabile del trattamento dei dati dovrebbe correggere la vulnerabilità e implementare nuove misure di sicurezza per evitare violazioni dei dati simili in futuro come, ad esempio, controlli di sicurezza sistematici del sito web. La violazione dovrebbe essere documentata in conformità dell'articolo 33, paragrafo 5, ma non è necessaria alcuna notifica o comunicazione. Inoltre, è fortemente consigliato comunicare agli interessati in ogni caso una violazione di password anche quando le password sono state memorizzate utilizzando un hash salato con algoritmo conforme allo stato dell'arte. È preferibile l'uso di metodi di autenticazione che ovviano alla necessità di elaborare le password sul lato server. Gli interessati dovrebbero avere la possibilità di adottare misure appropriate per quanto riguarda le proprie password.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

9.3 Attacco di credential stuffing su un sito Web bancario

Una banca ha subito un attacco informatico contro uno dei suoi siti web di online banking. L'attacco mirava a enumerare tutti i possibili ID utente di accesso utilizzando una password banale fissa. Le password sono composte da 8 cifre. A causa di una vulnerabilità del sito web, in alcuni casi sono trapelate all'aggressore informazioni riguardanti gli interessati (nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici identificativi dell'utente), anche se la password utilizzata non era corretta o il conto corrente bancario non è più attivo. La banca era a conoscenza della violazione dei dati perché il suo centro operativo di sicurezza ha rilevato un numero elevato di richieste di accesso dirette al sito web. In risposta, il controller ha disabilitato la possibilità di accedere al sito Web spegnendolo e reimpostando forzatamente la password degli account compromessi. Il titolare ha comunicato la violazione solo agli utenti con account compromessi, ovvero agli utenti le cui password erano state compromesse o i cui dati erano stati divulgati.

- **Misure preventive e valutazione del rischio**

È importante ricordare che i titolari del trattamento che gestiscono dati sensibili, informazioni finanziarie, ecc. Hanno una responsabilità maggiore in termini di fornitura di un'adeguata sicurezza dei dati, ad es. avere un centro operativo di sicurezza e altre misure di prevenzione, rilevamento e risposta agli incidenti. Il mancato rispetto di questi standard più elevati comporterà sicuramente misure più serie durante le indagini di un'autorità di vigilanza. La violazione riguarda i dati finanziari oltre l'identità e le informazioni sull'ID utente, rendendola particolarmente grave. Il numero di individui colpiti è elevato. Il fatto che una violazione possa verificarsi in un ambiente così sensibile indica significative falle nella sicurezza dei dati nel sistema del titolare del trattamento e può essere un indicatore di un momento in cui la revisione e l'aggiornamento delle misure interessate è "necessaria" in linea con l'articolo 24, 25 e 32 del GDPR. I dati violati consentono l'identificazione univoca degli interessati e contengono altre informazioni su di loro (inclusi sesso, data e luogo di nascita), inoltre possono essere utilizzati dall'aggressore per indovinare le password dei clienti o per eseguire una campagna di spear phishing diretta a i clienti della banca. Per questi motivi, si è ritenuto probabile che la violazione dei dati comportasse un rischio elevato per i diritti e le libertà di tutti gli interessati. Pertanto, il verificarsi di danni materiali (ad es. Perdita finanziaria) e non materiali (ad es. Furto di identità o frode) è un risultato concepibile.

- **Mitigazione e obblighi**

Le misure del responsabile del trattamento menzionate nella descrizione del caso sono adeguate. Sulla scia della violazione, ha anche corretto la vulnerabilità del sito Web e ha adottato altre misure per prevenire simili future violazioni dei dati, come l'aggiunta dell'autenticazione a due fattori al sito Web interessato e il passaggio a un'autenticazione forte del cliente. Documentare la violazione ai sensi dell'articolo 33 (5) GDPR e informarne la SA non è facoltativo in questo scenario. Inoltre, il responsabile del trattamento dovrebbe informare tutti gli interessati (compresi gli interessati i cui account non sono stati compromessi) in conformità con l'articolo 34 del GDPR.

Misure organizzative e tecniche per prevenire/mitigare gli impatti degli attacchi degli hacker:
Proprio come nel caso degli attacchi ransomware, indipendentemente dal risultato e dalle conseguenze dell'attacco, la rivalutazione della sicurezza IT è obbligatoria per i controller in casi simili.

Misure consigliate:
L'elenco delle seguenti misure non è in alcun modo esclusivo o completo. L'obiettivo è piuttosto quello di fornire idee per la prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa,

quindi il responsabile del trattamento dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione data.

- Crittografia e gestione delle chiavi all'avanguardia, soprattutto quando vengono elaborate password, dati sensibili o finanziari. L'hashing crittografico e il salting per informazioni segrete (password) sono sempre preferiti rispetto alla crittografia delle password. È preferibile l'uso di metodi di autenticazione che ovviano alla necessità di elaborare le password sul lato server.
- Mantenere aggiornato il sistema (software e firmware). Garantire che tutte le misure di sicurezza IT siano in atto, assicurarsi che siano efficaci e mantenerle regolarmente aggiornate quando l'elaborazione o le circostanze cambiano o evolvono. Per essere in grado di dimostrare la conformità con l'articolo 5, paragrafo 1, lettera f), in conformità con l'articolo 5, paragrafo 2, del GDPR, il responsabile del trattamento dovrebbe conservare una registrazione di tutti gli aggiornamenti eseguiti, incluso anche il momento in cui sono stati applicati.
- Utilizzo di metodi di autenticazione forte come l'autenticazione a due fattori e i server di autenticazione, integrati da una politica delle password aggiornata.
- Gli standard di sviluppo sicuro includono il filtraggio dell'input dell'utente (utilizzando la lista bianca per quanto possibile), la fuga degli input degli utenti e le misure di prevenzione della forza bruta (come la limitazione del numero massimo di tentativi). I "Web Application Firewall" possono aiutare nell'uso efficace di questa tecnica.
- Forti privilegi utente e criteri di gestione del controllo degli accessi in atto.
- Utilizzo di firewall appropriati, aggiornati, efficaci e integrati, rilevamento delle intrusioni e altri sistemi di difesa perimetrale.
- Audit sistematici della sicurezza IT e valutazioni delle vulnerabilità (test di penetrazione).
- Revisioni e test regolari per garantire che i backup possano essere utilizzati per ripristinare i dati la cui integrità o disponibilità è stata compromessa.
- •Nessun ID sessione nell'URL in testo normale.

10. Fonti di rischio umano interno

Il ruolo dell'errore umano nelle violazioni dei dati personali deve essere evidenziato, a causa del suo aspetto comune. Poiché questi tipi di violazioni possono essere sia intenzionali che non intenzionali, è molto difficile per i responsabili del trattamento identificare le vulnerabilità e adottare misure per evitarle. La Conferenza internazionale dei commissari per la protezione dei dati e la privacy ha riconosciuto l'importanza di affrontare tali fattori umani e ha adottato la risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali nell'ottobre 2019. Questa risoluzione sottolinea che dovrebbero essere adottate misure di salvaguardia appropriate per prevenire errori umani e fornisce un elenco non esaustivo di tali salvaguardie e approcci.

10.1 Esfiltrazione di dati della pa da parte di un ex dipendente

Durante il periodo di preavviso, il dipendente di un'azienda copia i dati aziendali dal database dell'azienda a cui è autorizzato ad accedere e che deve svolgere il proprio lavoro. Mesi dopo, dopo aver lasciato il lavoro, utilizza i dati così acquisiti (principalmente dati di contatto di base) per contattare i clienti dell'azienda per invogliarli alla sua nuova attività.

- **Misure preventive e valutazione del rischio**

In questo caso particolare, non sono state prese misure preventive per impedire al dipendente di copiare le informazioni di contatto della clientela dell'azienda, poiché aveva bisogno e aveva accesso legittimo a queste informazioni. Poiché la maggior parte dei lavori relativi alle relazioni con

i clienti richiede un qualche tipo di accesso dei dipendenti ai dati personali, queste violazioni dei dati possono essere le più difficili da prevenire. Le limitazioni all'ambito di accesso possono limitare il lavoro che un determinato dipendente è in grado di svolgere. Tuttavia, politiche di accesso ben ponderate e un controllo costante possono aiutare a prevenire tali violazioni.
Come di consueto, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione e la natura, la sensibilità e il volume dei dati personali interessati. Questi tipi di violazioni sono in genere violazioni della riservatezza, poiché il database viene solitamente lasciato intatto e il suo contenuto viene "semplicemente" copiato per un ulteriore utilizzo. Anche la quantità di dati interessati è generalmente bassa o media. In questo caso particolare non sono state interessate categorie speciali di dati personali, il dipendente necessitava solo delle informazioni di contatto dei clienti per consentirgli di mettersi in contatto con loro dopo aver lasciato l'azienda. Pertanto, i dati in questione non sono sensibili.
Sebbene l'unico obiettivo dell'ex dipendente che ha copiato i dati in modo dannoso possa essere limitato all'acquisizione delle informazioni di contatto della clientela dell'azienda per i propri scopi commerciali, il responsabile del trattamento non è in grado di considerare il rischio che gli interessati basso, in quanto il titolare del trattamento non ha alcun tipo di rassicurazione sulle intenzioni del dipendente. Pertanto, mentre le conseguenze della violazione potrebbe essere limitato all'esposizione all'auto-marketing non richiesto dell'ex dipendente, non è escluso un ulteriore e più grave abuso dei dati rubati.

- **Mitigazione e obblighi**

La mitigazione degli effetti negativi della violazione nel caso di cui sopra è difficile. Potrebbe essere necessario coinvolgere un'azione legale immediata per impedire all'ex dipendente di abusare e diffondere ulteriormente i dati. Come passo successivo, l'obiettivo dovrebbe essere quello di evitare situazioni future simili. Il responsabile del trattamento potrebbe tentare di ordinare all'ex dipendente di smettere di utilizzare i dati, ma il successo di questa azione è nella migliore delle ipotesi dubbia.
Non esiste una soluzione "valida per tutti" a questi tipi di casi, ma un approccio sistematico può aiutare a prevenirli. Ad esempio, l'azienda può prendere in considerazione, quando possibile, la revoca di determinate forme di accesso ai dipendenti che hanno segnalato la propria intenzione di uscire o l'implementazione dei log di accesso in modo che gli accessi indesiderati possano essere registrati e contrassegnati. Il contratto firmato con i dipendenti dovrebbe includere clausole che vietano tali azioni.
Tutto sommato, poiché la violazione in questione non comporterà un rischio elevato per i diritti e le libertà delle persone fisiche, sarà sufficiente una notifica alla SA. Tuttavia, le informazioni agli interessati potrebbero essere vantaggiose anche per il titolare del trattamento, poiché potrebbe essere meglio che sentano dalla società in merito alla fuga di dati piuttosto che dall'ex dipendente che cerca di contattarli. La documentazione sulla violazione dei dati ai sensi dell'articolo 33, paragrafo 5, è un obbligo legale.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

10.2 Trasmissione accidentale di dati a una terza parte fidata

Un agente assicurativo ha notato che - reso possibile dalle impostazioni errate di un file Excel ricevuto via e-mail - ha potuto accedere a informazioni relative a due dozzine di clienti non appartenenti al suo ambito. È vincolato dal segreto professionale ed era l'unico destinatario dell'e-mail. L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga l'agente a segnalare senza indebito ritardo al titolare del trattamento una violazione dei dati personali. Pertanto, l'agente ha immediatamente segnalato l'errore al controller, che ha corretto il file e lo ha inviato di nuovo,

chiedendo all'agente di eliminare il messaggio precedente. Secondo l'accordo di cui sopra, l'agente deve confermare la cancellazione in una dichiarazione scritta, cosa che ha fatto. Le informazioni ottenute non includono categorie speciali di dati personali, ma solo dati di contatto e dati sull'assicurazione stessa (tipo di assicurazione, importo). Dopo aver analizzato i dati personali interessati dalla violazione, il titolare del trattamento non ha individuato alcuna caratteristica particolare da parte delle persone o del titolare del trattamento che possa influire sul livello di impatto della violazione.

- **Misure preventive e valutazione del rischio**

A differenza del caso precedente, qui la violazione non deriva da un'azione deliberata di un dipendente, ma da un errore umano non intenzionale causato da disattenzione. Questi tipi di violazioni possono essere evitati a) applicando programmi di formazione, istruzione e sensibilizzazione in cui i dipendenti acquisiscono una migliore comprensione dell'importanza della protezione dei dati personali; b) riducendo lo scambio di file tramite e-mail, utilizzando invece sistemi dedicati per l'elaborazione dei dati dei clienti, per esempio; c) ricontrollare i file prima dell'invio; d) separare la creazione e l'invio dei file. Questa violazione dei dati riguarda solo la riservatezza dei dati e l'integrità e l'accessibilità degli stessi rimangono intatte. La violazione dei dati ha riguardato solo circa due dozzine di clienti; quindi, la quantità di dati interessati può essere considerata bassa. Inoltre, i dati personali interessati non contengono dati sensibili. Il fatto che il responsabile del trattamento abbia contattato immediatamente il titolare del trattamento dopo essere venuto a conoscenza della violazione dei dati può essere considerato un fattore di attenuazione del rischio. (Dovrebbe essere valutata anche la possibilità che i dati siano stati inviati ad altri agenti assicurativi e, se confermata, dovrebbero essere prese misure adeguate.) A causa delle misure appropriate prese dopo la violazione dei dati, probabilmente non avrà alcun impatto sugli interessati diritti e libertà.
La combinazione del basso numero di persone colpite, l'immediata individuazione della violazione e le misure adottate per minimizzarne gli effetti rendono questo caso particolare privo di rischi.

- **Mitigazione e obblighi**

Inoltre, sono in gioco anche altre circostanze di attenuazione del rischio: l'agente è vincolato dal segreto professionale; lui stesso ha segnalato il problema al controllore; e ha cancellato il file su richiesta. Aumentare la consapevolezza ed eventualmente includere ulteriori passaggi nel controllo dei documenti che coinvolgono dati personali aiuterà probabilmente a evitare casi simili in futuro.
Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

Misure organizzative e tecniche per prevenire/mitigare gli impatti delle fonti di rischio umano interne:
Una combinazione delle misure sotto menzionate, applicate a seconda delle caratteristiche uniche del caso, dovrebbe aiutare a ridurre la possibilità che una violazione simile si ripresenti.

Misure consigliate:
L'elenco delle seguenti misure non è in alcun modo esclusivo o completo. L'obiettivo è piuttosto quello di fornire idee di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, quindi il responsabile del trattamento dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione data.

- Attuazione periodica di programmi di formazione, istruzione e sensibilizzazione per i dipendenti sui loro obblighi in materia di privacy e sicurezza e rilevamento e segnalazione di minacce alla sicurezza dei dati personali. Sviluppare un programma di sensibilizzazione per ricordare ai dipendenti gli errori più comuni che portano a violazioni dei dati personali e come evitarli.
- Creazione di pratiche, procedure e sistemi solidi ed efficaci per la protezione dei dati e la privacy.
- Valutazione delle pratiche, delle procedure e dei sistemi in materia di privacy per garantire un'efficacia continua.
- Definizione di criteri di controllo degli accessi adeguati e obbligazione degli utenti a seguire le regole.
- Implementazione di tecniche per forzare l'autenticazione dell'utente durante l'accesso a dati personali sensibili.
- Disattivazione dell'account relativo alla società dell'utente non appena la persona lascia l'azienda.
- Controllo del flusso di dati insolito tra il file server e le workstation dei dipendenti.
- Configurazione della protezione dell'interfaccia I/O nel BIOS o tramite l'uso di software che controlla l'uso delle interfacce del computer (blocco o sblocco, ad esempio USB/CD / DVD, ecc.).
- Revisione della politica di accesso dei dipendenti (ad es. Registrazione dell'accesso a dati sensibili e richiesta all'utente di inserire un motivo aziendale, in modo che sia disponibile per gli audit).
- Disabilitazione dei servizi cloud aperti.
- Proibire e impedire l'accesso a noti servizi di posta aperti.
- Disattivazione della funzione di stampa dello schermo nel sistema operativo.
- Applicazione di una politica della scrivania pulita.
- Blocco automatico di tutti i computer dopo un certo periodo di inattività.
- Utilizzare meccanismi (ad es. Token (wireless) per accedere/aprire account bloccati) per cambi utente rapidi in ambienti condivisi.
- Utilizzo di sistemi dedicati per la gestione dei dati personali che applichino adeguati meccanismi di controllo degli accessi e che prevengano errori umani, come l'invio di comunicazioni al soggetto sbagliato. L'uso di fogli di calcolo e altri documenti d'ufficio non è un mezzo appropriato per gestire i dati dei clienti.

Il fattore umano, tradizionalmente, è stato da sempre una delle maggiori fonti di incidenti di sicurezza, sia per errori involontari sia per comportamenti intenzionali (ad esempio, per ritorsione riguardo a situazioni ritenute ingiustamente penalizzanti o per infedeltà e comportamenti illeciti). Con la pandemia si è aggiunto un ulteriore fattore incrementale dovuto alle persone che lavorano da remoto, costringendo ad un superlavoro degli addetti IT per configurare gli accessi e i controlli di sicurezza per il personale.

In tutti i casi, poche sono le misure preventive per ridurre il verificarsi di tali incidenti.

La newsletter del Garante del 19/2/2021 menziona 3 casi di incidenti umani nel settore sanitario che hanno portato a sanzioni:

- «*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*»
- *«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'infermiera del reparto dove una paziente stava seguendo delle terapie la contatta sul numero di casa, parlando così con un familiare, sebbene la donna avesse «*esplicitamente richiesto – sottoscrivendo un apposito modulo – che nessun soggetto esterno*» venisse informato.

In aggiunta, è da osservare che, quando l'errore non riguarda il contesto tecnico, come nei casi sopra riportati, spesso non viene considerato come incidente e, di conseguenza, come violazione di dati personali, in quanto la tradizionale cultura del Data Breach è orientata verso quegli incidenti che coinvolgono le infrastrutture tecnologiche aziendali.

La terza tipologia di casi di Data Breach affrontati nelle linee guida EDPB 01/2021 è appunto quella degli incidenti da fonti umane interne.

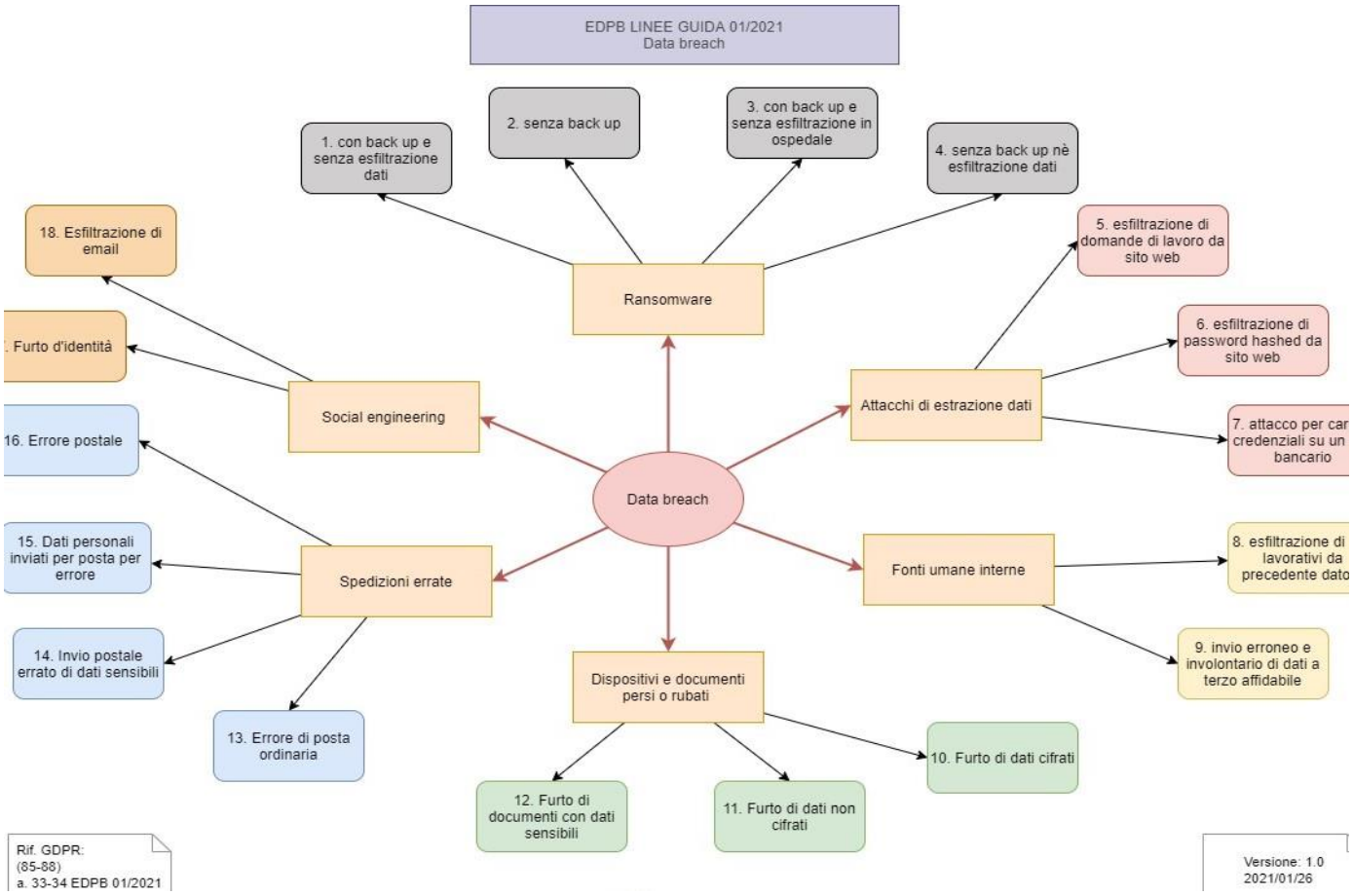


Figura 3 – Schema EDBP

11. Dispositivi smarriti o rubati e documenti su carta

Un tipo frequente di caso è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze dell'operazione di trattamento, come il tipo di dati memorizzati sul dispositivo, nonché le risorse di supporto, e le misure adottate prima della violazione per garantire un livello appropriato di sicurezza. Tutti questi elementi influenzano i potenziali impatti della violazione dei dati. La valutazione del rischio potrebbe essere difficile, poiché il dispositivo non è più disponibile.
Un tipo frequente di caso è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze dell'operazione di trattamento, come il tipo di dati memorizzati sul dispositivo, nonché le risorse di supporto, e le misure adottate prima della violazione per garantire un livello appropriato di sicurezza. Tutti questi elementi influenzano i potenziali impatti della violazione dei dati. La valutazione del rischio potrebbe essere difficile, poiché il dispositivo non è più disponibile.

11.1 Materiale rubato che memorizza dati personali crittografati

Durante un'irruzione in un asilo nido per bambini, sono state rubate due compresse. I tablet contenevano una App che conteneva dati personali sui bambini che frequentavano l'asilo nido. Nome, data di nascita, dati personali sull'educazione dei bambini erano interessati. Sia i tablet crittografati che erano stati spenti al momento dell'irruzione, sia l'app erano protetti da una password complessa. I dati di backup erano effettivamente e prontamente disponibili per il controller. Dopo essere venuto a conoscenza dell'irruzione, l'asilo ha emesso a distanza un comando per pulire le compresse poco dopo la scoperta dell'irruzione.

- **Misure preventive e valutazione del rischio**

In questo caso particolare, il titolare del trattamento ha adottato misure adeguate a prevenire e mitigare gli impatti di una potenziale violazione dei dati utilizzando la crittografia del dispositivo, introducendo un'adeguata protezione con password e garantendo il backup dei dati memorizzati sui tablet. (Un elenco di misure consigliate si trova nella sezione 5.7).
Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte del rischio, i sistemi a supporto del trattamento dei dati, il tipo di dati personali coinvolti e i potenziali impatti della violazione dei dati sulle persone interessate. La violazione dei dati sopra descritta avrebbe riguardato la riservatezza, la disponibilità e l'integrità dei dati interessati; tuttavia, a causa degli opportuni procedimenti del titolare del trattamento prima e dopo la violazione dei dati nessuno di questi si è verificato.

- **Mitigazione e obblighi**

La riservatezza dei dati personali sui dispositivi non è stata compromessa grazie alla forte protezione con password sia sui tablet che sulle app. I tablet sono stati configurati in modo tale che l'impostazione di una password significa anche che i dati sul dispositivo sono crittografati. Ciò è stato ulteriormente migliorato dall'azione del controller di tentare di cancellare da remoto tutto dai dispositivi rubati.
A causa delle misure adottate, anche la riservatezza dei dati è stata mantenuta intatta. Inoltre, il backup ha garantito la continua disponibilità dei dati personali; quindi, nessun potenziale impatto negativo potrebbe essersi verificato.
A causa di questi fatti, era improbabile che la violazione dei dati sopra descritta comportasse un rischio per i diritti e le libertà degli interessati, pertanto non è stata necessaria alcuna notifica all'autorità di vigilanza o agli interessati. Tuttavia, anche questa violazione dei dati deve essere documentata ai sensi dell'articolo 33, paragrafo 5.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

11.2 Materiale rubato che archivia dati personali non crittografati

Il notebook elettronico di un dipendente di una società di servizi è stato rubato. Il taccuino rubato conteneva nomi, cognomi, sesso, indirizzi e date di nascita di oltre 100000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile identificare se fossero interessate anche altre categorie di dati personali. L'accesso al disco rigido del notebook non era protetto da password. I dati personali possono essere ripristinati dai backup giornalieri disponibili.

- **Misure preventive e valutazione del rischio**

Nessuna misura di sicurezza preventiva è stata adottata dal titolare del trattamento; quindi, i dati personali memorizzati sul notebook rubato sono stati facilmente accessibili per il ladro o per qualsiasi altra persona venuta in possesso del dispositivo successivamente.
Questa violazione dei dati riguarda la riservatezza dei dati memorizzati sul dispositivo rubato.
Il notebook contenente i dati personali era vulnerabile in questo caso perché non possedeva alcuna protezione con password o crittografia. La mancanza di misure di sicurezza di base aumenta il livello di rischio per gli interessati. Inoltre, anche l'identificazione degli interessati è problematica, il che aumenta anche la gravità della violazione. Il numero considerevole di persone interessate aumenta il rischio, tuttavia, nessuna categoria speciale di dati personali è stata interessata dalla violazione dei dati.
Durante la valutazione del rischio, il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza. A seguito della violazione, gli interessati potrebbero subire frodi di identità facendo affidamento sui dati disponibili sul dispositivo rubato, pertanto il rischio è considerato elevato.

- **Mitigazione e obblighi**

L'attivazione della crittografia del dispositivo e l'uso di una forte protezione tramite password del database archiviato avrebbero potuto impedire che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati. A causa di queste circostanze è necessaria la notifica alla SA, è necessaria anche la notifica agli interessati.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

11.3 File cartacei rubati con dati sensibili

Un registro cartaceo è stato rubato da una struttura di riabilitazione per tossicodipendenti. Il libro conteneva i dati di base sull'identità e sulla salute dei pazienti ammessi alla struttura di riabilitazione. I dati sono stati memorizzati solo su carta e nessun backup era disponibile per i medici che curano i pazienti. Il libro non era conservato in un cassetto chiuso a chiave o in una stanza, il titolare del trattamento non aveva né un regime di controllo degli accessi né alcuna altra misura di salvaguardia della documentazione cartacea.

- **Misure preventive e valutazione del rischio**

Nessuna misura di sicurezza preventiva è stata adottata dal titolare del trattamento; quindi, i dati personali memorizzati in questo libro erano facilmente accessibili per la persona che li ha trovati. Inoltre, la natura dei dati personali memorizzati nel libro rende la mancanza di dati di backup un

fattore di rischio molto serio. Questo caso serve da esempio per una violazione dei dati ad alto rischio. A causa del mancato rispetto di adeguate precauzioni di sicurezza, i dati sanitari sensibili ai sensi dell'articolo 9, paragrafo 1, del GDPR sono andati persi. Poiché in questo caso si trattava di una categoria speciale di dati personali, i potenziali rischi per gli interessati sono stati aumentati, il che dovrebbe essere preso in considerazione anche dal responsabile del trattamento che valuta il rischio. Questa violazione riguarda la riservatezza, la disponibilità e l'integrità dei dati personali interessati. Come risultato della violazione, il segreto medico viene infranto e terze parti non autorizzate possono avere accesso alle informazioni mediche private dei pazienti, il che può avere un grave impatto sulla vita personale del paziente. La violazione della disponibilità può inoltre disturbare la continuità del trattamento dei pazienti. Poiché non è possibile escludere la modifica / cancellazione di parti del contenuto del libro, viene compromessa anche l'integrità dei dati personali.

- **Mitigazione e obblighi**

Durante la valutazione delle misure di salvaguardia dovrebbe essere considerata anche la tipologia del bene di supporto. Poiché il registro del paziente era un documento fisico, la sua salvaguardia avrebbe dovuto essere organizzata in modo diverso da quella di un dispositivo elettronico. La pseudonimizzazione dei nomi dei pazienti, l'archiviazione del libro in un locale protetto e in un cassetto o una stanza chiusa a chiave e un corretto controllo degli accessi con autenticazione all'accesso avrebbero potuto prevenire la violazione dei dati.
La violazione dei dati sopra descritta può avere un impatto grave sugli interessati; pertanto, la notifica alla SA e la comunicazione della violazione agli interessati è obbligatoria.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	ommunication to data subjects
✓	✓	✓

Misure organizzative e tecniche per prevenire/mitigare gli impatti di smarrimento o furto di dispositivi

Una combinazione delle misure sotto menzionate, applicate a seconda delle caratteristiche uniche del caso, dovrebbe aiutare a ridurre la possibilità che una violazione simile si ripresenti.

Misure consigliate:
L'elenco delle seguenti misure non è in alcun modo esclusivo o completo. L'obiettivo è piuttosto quello di fornire idee di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, quindi il responsabile del trattamento dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione data.

- Attiva la crittografia del dispositivo (come Bitlocker, Veracrypt o DM-Crypt).
- Usa passcode/password su tutti i dispositivi. Crittografa tutti i dispositivi elettronici mobili in un modo che richiede l'inserimento di una password complessa per la decrittografia.
- Utilizzare l'autenticazione a più fattori.
- Attivare le funzionalità dei dispositivi altamente mobili che consentono di localizzarli in caso di smarrimento o smarrimento.
- Utilizzare il software/app MDM (Mobile Devices Management) e la localizzazione. Usa filtri antiriflesso. Chiudi tutti i dispositivi incustoditi.
- Se possibile e appropriato al trattamento dei dati in questione, salvare i dati personali non su un dispositivo mobile, ma su un server centrale di back-end.

- Se la workstation è collegata alla LAN aziendale, eseguire un backup automatico dalle cartelle di lavoro a condizione che sia inevitabile che i dati personali siano archiviati lì
- Utilizzare una VPN sicura (ad es. che richiede una chiave di autenticazione del secondo fattore separata per stabilire una connessione sicura) per connettere i dispositivi mobili ai server back-end.
- Fornire serrature fisiche ai dipendenti per consentire loro di proteggere fisicamente i dispositivi mobili che utilizzano mentre rimangono incustoditi.
- Regolamentazione corretta dell'utilizzo del dispositivo all'esterno dell'azienda.
- Corretta regolamentazione dell'utilizzo dei dispositivi all'interno dell'azienda.
- Utilizzare il software/app MDM (Mobile Devices Management) e abilitare la funzione di cancellazione remota.
- Utilizzare la gestione centralizzata dei dispositivi con diritti minimi per gli utenti finali per l'installazione del software.
- Installare i controlli di accesso fisico.
- Evitare di archiviare informazioni sensibili su dispositivi mobili o dischi rigidi. Se è necessario accedere al sistema interno dell'azienda, è necessario utilizzare canali protetti come indicato in precedenza.

12 MISPOSTAL

Anche in questo caso la fonte del rischio è un errore umano interno, ma qui nessuna azione dannosa ha portato alla violazione. È il risultato della disattenzione. Poco può essere intrapreso dal responsabile del trattamento dopo che è accaduto; quindi, la prevenzione è ancora più importante in questi casi che in altri tipi di violazione.

11.4 Errore di posta ordinaria

Due ordini di scarpe sono stati confezionati da una società di vendita al dettaglio. A causa di un errore umano, due fatture di imballaggio sono state confuse con il risultato che entrambi i prodotti e le relative fatture di imballaggio sono state inviate alla persona sbagliata. Ciò significa che i due clienti si sono scambiati gli ordini, comprese le bolle di accompagnamento contenenti i dati personali. Il titolare del trattamento, venuto a conoscenza della violazione, ha richiamato gli ordini e li ha trasmessi ai destinatari giusti.

- **Misure preventive e valutazione del rischio**

Le fatture contenevano i dati personali necessari per una corretta consegna (nome, indirizzo, più l'articolo acquistato e il suo prezzo). È importante identificare in primo luogo come sarebbe potuto accadere l'errore umano e, se in qualche modo, avrebbe potuto essere prevenuto. Nel caso specifico descritto il rischio è basso, poiché non sono state coinvolte categorie speciali di dati personali o altri dati il cui abuso potrebbe comportare effetti negativi sostanziali, la violazione non è il risultato di un errore sistemico da parte del controllerà e solo due persone sono ha riguardato. Non è stato possibile identificare alcun effetto negativo sugli individui.

- **Mitigazione e obblighi**

Il titolare del trattamento dovrebbe provvedere alla restituzione gratuita degli articoli e delle fatture di accompagnamento, nonché richiedere ai destinatari sbagliati di distruggere / cancellare tutte le eventuali copie delle fatture contenenti i dati personali dell'altra persona. Anche se la violazione in sé non rappresenta un rischio elevato per i diritti e le libertà delle persone interessate, e quindi la comunicazione agli interessati non è prevista dall'articolo 34 GDPR, la

comunicazione della violazione agli stessi non può essere evitata, poiché è necessaria la loro collaborazione per mitigare il rischio.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

11.5 Dati personali sensibili inviati per posta elettronica per errore

Il dipartimento del lavoro di un ufficio della pubblica amministrazione ha inviato un messaggio di posta elettronica - sui prossimi corsi di formazione - alle persone registrate nel suo sistema come persone in cerca di lavoro. Per errore, a questa e-mail è stato allegato un documento contenente tutti i dati personali di queste persone in cerca di lavoro (nome, indirizzo e-mail, indirizzo di postai, codice fiscale). Il numero delle persone interessate è superiore a 60000. Successivamente l'ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.

- **Misure preventive e valutazione del rischio**

Avrebbero dovuto essere implementate regole più severe per l'invio di tali messaggi. È necessario considerare l'introduzione di meccanismi di controllo aggiuntivi.
Il numero di persone colpite è considerevole e il coinvolgimento del loro numero di previdenza sociale, insieme ad altri dati personali più basilari, aumenta ulteriormente il rischio, che può essere identificato come alto. L'eventuale diffusione dei dati da parte di uno qualsiasi dei destinatari non può essere contenuta dal titolare.

- **Mitigazione e obblighi**

Come accennato in precedenza, i mezzi per mitigare efficacemente i rischi di una violazione simile sono limitati. Sebbene il titolare del trattamento abbia chiesto la cancellazione del messaggio, non può obbligare i destinatari a farlo e, di conseguenza, né può essere certo che rispettino la richiesta.
L'esecuzione di tutte e tre le azioni sottoindicate dovrebbe essere evidente in un caso come questo.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

11.6 Dati personali inviati per posta per errore

Un elenco dei partecipanti a un corso di inglese legale che si svolge in un hotel per 5 giorni viene inviato per errore a 15 ex partecipanti al corso invece che all'hotel. L'elenco contiene nomi, indirizzi e-mail e preferenze alimentari dei 15 partecipanti. Solo due partecipanti hanno inserito le loro preferenze alimentari, affermando di essere intolleranti al lattosio. Nessuno dei partecipanti ha un'identità protetta. Il titolare del trattamento scopre l'errore subito dopo aver inviato la lista e informa i destinatari dell'errore e chiede loro di cancellare la lista.

- **Misure preventive e valutazione del rischio**

Si sarebbero dovute attuare regole più severe per l'invio di tali messaggi. È necessario considerare l'introduzione di meccanismi di controllo aggiuntivi
I rischi derivanti dalla natura, dalla sensibilità, dal volume e dal contesto dei dati personali sono bassi. I dati personali includono dati sensibili sulle preferenze alimentari di due dei partecipanti.

Anche se le informazioni sull'intolleranza al lattosio di una persona sono dati sulla salute, il rischio che questi dati vengano utilizzati in modo dannoso dovrebbe essere considerato relativamente basso. Mentre nel caso dei dati relativi alla salute si presume solitamente che la violazione possa comportare un rischio elevato per l'interessato, allo stesso tempo in questo caso particolare non è possibile identificare alcun rischio che la violazione comporti o danni non materiali dell'interessato a causa della divulgazione non autorizzata di informazioni sull'intolleranza al lattosio. Contrariamente ad altre preferenze alimentari, l'intolleranza al lattosio normalmente non può essere collegata a credenze religiose o filosofiche. Anche la quantità di dati violati e il numero di interessati sono molto bassi.

- **Mitigazione e obblighi**

In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore attenuante.
Se un'e-mail viene inviata a un destinatario errato/non autorizzato, si consiglia al titolare del trattamento di inviare in Ccn un'e-mail di follow-up ai destinatari non intenzionali chiedendo scusa, istruendo che l'e-mail incriminata deve essere eliminata e avvisando i destinatari che non hanno il diritto per utilizzare ulteriormente gli indirizzi e-mail a loro identificati.
A causa di questi fatti, era improbabile che questa violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati, pertanto non era necessaria alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche questa violazione dei dati deve essere documentata ai sensi dell'articolo 33, paragrafo 5.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

11.7 Errore di posta elettronica ordinaria

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia regolarmente tramite posta ordinaria le politiche di contribuzione adeguate. Oltre al nome e all'indirizzo del contraente, la lettera contiene il numero di immatricolazione del veicolo, le tariffe assicurative dell'anno in corso e quello successivo, il chilometraggio annuo approssimativo e la data di nascita del contraente. I dati sanitari ai sensi dell'articolo 9 GDPR, i dati di pagamento (coordinate bancarie), i dati economici e finanziari non sono inclusi.
Le lettere vengono imballate con macchine avvolgitrici automatiche. A causa di un errore meccanico, due lettere per diversi assicurati vengono inserite in una busta e inviate a un assicurato per posta. Il contraente apre la lettera a casa e prende visione della sua lettera recapitata correttamente nonché della lettera recapitata in modo errato di un altro contraente.

- **Misure preventive e valutazione del rischio**

La lettera erroneamente consegnata contiene il nome, l'indirizzo, la data di nascita, il numero di targa e l'annullamento della rata assicurativa dell'anno in corso e dell'anno successivo. Se il tasso di assicurazione aumenta nell'anno successivo, ciò indica un reclamo automobilistico presentato alla compagnia di assicurazione. Gli effetti sulla persona interessata sono da considerarsi medi, poiché informazioni non pubblicamente disponibili come la data di nascita o il numero di immatricolazione del veicolo, e se il tasso di assicurazione aumenta, è stata divulgati al destinatario non autorizzato. La probabilità di un uso improprio di questi dati è valutata tra bassa e media. Tuttavia, mentre molti destinatari probabilmente smaltiranno la lettera erroneamente ricevuta nella spazzatura, in singoli casi non si può escludere

completamente che la lettera venga pubblicata sui social network o che l'assicurato venga contattato.

- **Mitigazione e obblighi**

Il responsabile del trattamento dovrebbe richiedere la restituzione del documento originale a proprie spese. Il destinatario sbagliato dovrebbe anche essere informato che non può utilizzare impropriamente le informazioni lette.
Probabilmente non sarà mai possibile prevenire completamente un errore di consegna postale in un invio di massa utilizzando macchine completamente automatizzate. Tuttavia, in caso di aumento della frequenza, è necessario verificare se le macchine avvolgitrici sono impostate e mantenute sufficientemente correttamente, o se qualche altro problema sistemico porta a tale violazione.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

Misure organizzative e tecniche per prevenire / mitigare gli impatti del mispostal
Una combinazione delle misure di seguito indicate, applicate in base alle caratteristiche uniche del caso, dovrebbe contribuire a ridurre la possibilità che una violazione simile si ripresenti.

Misure consigliate:
L'elenco delle seguenti misure non è in alcun modo esclusivo o completo. L'obiettivo è piuttosto fornire idee di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, quindi il responsabile del trattamento dovrebbe prendere la decisione su quali misure si adattano maggiormente alla situazione data.

- Stabilire standard precisi - senza spazio per l'interpretazione - per l'invio di lettere/e-mail.
- Adeguata formazione del personale su come inviare lettere/e-mail.
- Quando si inviano e-mail a più destinatari, vengono elencati nel campo "Ccn" per impostazione predefinita.
- È richiesta una conferma aggiuntiva quando si inviano e-mail a più destinatari, e lo sono non elencato nel campo "Ccn".
- Applicazione del principio dei quattro occhi.
- Indirizzamento automatico anziché manuale, con dati estratti da un disponibile e aggiornato database delle date; il sistema di indirizzamento automatico deve essere riesaminato regolarmente per verificare la presenza di errori nascosti e impostazioni errate.
- Applicazione del ritardo del messaggio (ad es. il messaggio può essere cancellato/modificato entro un determinato periodo di tempo dopo aver cliccato sul pulsante).
- Disattivazione del completamento automatico durante la digitazione di indirizzi e-mail.
- Sessioni di sensibilizzazione sugli errori più comuni che portano a una violazione dei dati personali.

Sessioni di formazione e manuali su come gestire gli incidenti che portano a una violazione dei dati personali e chi informare (coinvolgere il DPO).
Nelle figure successive alcuni casi di phishing verificatesi nel 2020 (Fonte Report Clusit 2020).

Dear alessandro [redacted]
Employee [redacted] Company,

We are deeply saddened to inform you that your term of employment at [redacted] company has come to an immediate end. Due to the covid-19 epidemic, we have no choice but to end your employment with us.This decision is effective immediately.

Find attached your 2 months salary receipt.

We thank you for your service and we wish it didn't have to end this way.

Sincerely,

Human Resources Manager

cc: ceo@[redacted]

Campagna di phishing, finto licenziamento causa COVID. Fonte: Libraesva

Figura 4 – Casi di Phishing 2020

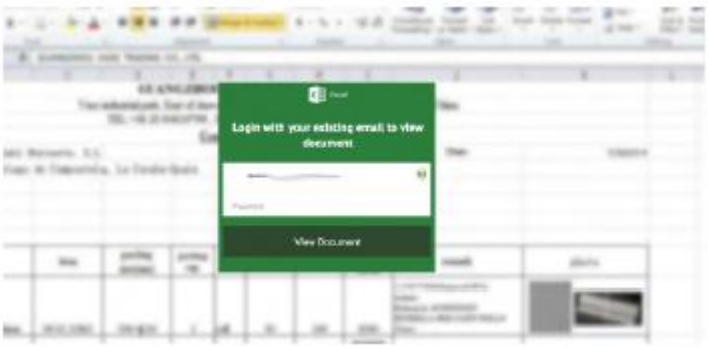


Figura 5 – Allegato malevolo

Figura 6 – il Caso MEF

12. Altri casi - Ingegneria Sociale

12.1 Furto d'identità

Il contact center di una società di telecomunicazioni riceve una telefonata da qualcuno che si atteggia a cliente. Il presunto cliente richiede all'azienda di modificare l'indirizzo e-mail a cui devono essere inviate le informazioni di fatturazione da lì in poi. L'operatore del contact center convalida l'identità del cliente richiedendo alcuni dati personali, come definiti dalle procedure dell'azienda. Il chiamante indica correttamente il numero fiscale e l'indirizzo postale del cliente richiesto (perché aveva accesso a questi elementi). Dopo la convalida, l'operatore apporta la modifica richiesta e, da lì in poi, le informazioni di fatturazione vengono inviate al nuovo indirizzo di posta elettronica. La procedura non prevede alcuna notifica all'ex contatto email. Il mese successivo il cliente legittimo contatta l'azienda, chiedendo perché non riceve la fatturazione al suo indirizzo e-mail e rifiuta qualsiasi chiamata da parte sua chiedendo il cambio del contatto e-mail. Successivamente, l'azienda si rende conto che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

- **Valutazione, mitigazione e obblighi del rischio**

Questo caso serve da esempio sull'importanza delle misure preliminari. La violazione, dal punto di vista del rischio, presenta un alto livello di rischio, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (es. Abitudini, contatti) e potrebbero portare a danni materiali (es. Stalking, rischio per l'integrità fisica). I dati personali ottenuti durante questo attacco possono essere utilizzati anche per facilitare l'acquisizione di account in questa organizzazione o sfruttare ulteriori misure di autenticazione in altre organizzazioni. Considerando questi rischi, la misura di autenticazione "appropriata" dovrebbe soddisfare un livello elevato, a seconda dei dati personali che possono essere elaborati a seguito dell'autenticazione.
Di conseguenza, sono necessarie sia una notifica alla SA che una comunicazione all'interessato da parte del responsabile del trattamento.
Il processo di convalida del cliente precedente deve essere chiaramente perfezionato alla luce di questo caso. I metodi utilizzati per l'autenticazione non erano sufficienti. Il malintenzionato è stato in grado di fingere di essere l'utente previsto utilizzando le informazioni e le informazioni disponibili pubblicamente a cui avrebbe altrimenti accesso.
L'uso di questo tipo di autenticazione statica basata sulla conoscenza (dove la risposta non cambia e dove le informazioni non sono "segrete" come nel caso di una password) è sconsigliato.
L'organizzazione dovrebbe invece utilizzare una forma di autenticazione che si traduca in un alto grado di fiducia che l'utente autenticato sia la persona designata e non chiunque altro. L'introduzione di un metodo di autenticazione a più fattori fuori banda risolverebbe il problema, ad es. verificare la richiesta di modifica, inviando una richiesta di conferma al contatto precedente, o aggiungendo domande extra e richiedendo informazioni visibili solo sulle bollette precedenti. È responsabilità del controllerà decidere quali misure introdurre, poiché conosce al meglio i dettagli e le esigenze del proprio funzionamento interno.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

12.2 Esfiltrazione di e-mail

Una catena di ipermercati ha rilevato, 3 mesi dopo la sua configurazione, che alcuni account di posta elettronica erano stati modificati e regole create in modo che ogni e-mail contenesse determinate espressioni (ad es. "Fattura", "pagamento", "bonifico bancario", "autenticazione carta di

credito", "i dettagli del conto bancario") verrebbero spostati in una cartella inutilizzata e inoltrati anche a un indirizzo e-mail esterno. Inoltre, a quel punto, era già stato eseguito un attacco di ingegneria sociale, vale a dire che l'aggressore, fingendosi un fornitore, aveva fatto modificare i dettagli del conto bancario del fornitore nei suoi. Infine, a quel punto, erano state inviate diverse fatture false che includevano i dettagli del nuovo conto bancario. Il sistema di monitoraggio della piattaforma di posta elettronica ha finito per fornire un avviso relativo alle cartelle. La società non è stata in grado di rilevare come l'aggressore sia stato in grado di accedere agli account di posta elettronica per cominciare, ma ha supposto che un'e-mail infetta fosse la colpa per aver dato accesso al gruppo di utenti incaricati dei pagamenti.
A causa dell'inoltro di e-mail basato su parole chiave, l'aggressore ha ricevuto informazioni su 99 dipendenti: nome e stipendio di un determinato mese riguardante 89 interessati; nome, stato civile, numero di figli, stipendio, orario di lavoro e resto informazioni sulla ricevuta del salario di 10 dipendenti i cui contratti sono stati risolti. Il responsabile del trattamento ha notificato solo i 10 dipendenti appartenenti a quest'ultimo gruppo.

- **Valutazione, mitigazione e obblighi del rischio**

Anche se l'aggressore probabilmente non mirava a raccogliere dati personali, poiché la violazione potrebbe portare a danni sia materiali (ad es. Perdita finanziaria) che non materiali (ad es. Furto di identità o frode), oppure i dati potrebbero essere utilizzati per facilitare altri attacchi (ad es. phishing), è probabile che la violazione dei dati personali comporti un rischio elevato per i diritti e le libertà delle persone fisiche. Pertanto, la violazione dovrebbe essere comunicata a tutti i 99 dipendenti e non solo ai 10 dipendenti di cui sono trapelate le informazioni sullo stipendio. Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha forzato una modifica della password per gli account compromessi, bloccato l'invio di e-mail all'account e-mail dell'aggressore, informato il fornitore di servizi dell'e-mail utilizzata dall'aggressore in merito alle sue azioni, rimosso le regole impostate dall'attaccante e perfezionato gli avvisi del sistema di monitoraggio in modo da dare un avviso non appena viene creata una regola automatica. In alternativa, il controller potrebbe rimuovere il diritto per gli utenti di impostare regole di inoltro, richiedendo che il team del servizio IT lo faccia solo su richiesta o potrebbe introdurre una politica che gli utenti dovrebbero controllare e riferire sulle regole impostate sui propri account una volta alla settimana o più spesso, nelle aree che trattano dati finanziari.
Il fatto che una violazione potesse verificarsi e non fosse rilevata per così tanto tempo e il fatto che, in un tempo più lungo, l'ingegneria sociale avrebbe potuto essere utilizzata per alterare più dati, ha evidenziato problemi significativi nel sistema di sicurezza IT del responsabile del trattamento. Questi dovrebbero essere affrontati senza indugio, come l'enfasi sulle revisioni dell'automazione e sui controlli delle modifiche, il rilevamento degli incidenti e le misure di risposta. I titolari del trattamento dei dati sensibili, delle informazioni finanziarie, ecc. Hanno una responsabilità maggiore in termini di fornitura di un'adeguata sicurezza dei dati.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

13. Il caso del Comune di Pisticci: il modello organizzativo

Per poter applicare in toto tutto ciò quanto previsto dalle linee guida EDB in materia di Data Breach Notification è necessario dapprima analizzare l'architettura di rete del Comune di Pisticci (provincia di Matera) consta alla data odierna di circa 71 client di cui solo 22 con sistema operativo Windows 10. 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.

La dotazione dei beni strumentali ed informatici che corredano le stazioni di lavoro è la seguente:

- n. 3 SERVER
- N. 67 PC
- N. 1 NOTEBOOK

Nella seguente tabella viene dettagliata l'ubicazione delle singole macchine.

EDIFICIO	UFFICIO	POSTAZIONI DI LAVORO
Palazzo Giannantonio	Anagrafe	3
	Contratti	3
	Legale	3
	Messi	1
	Protocollo	2
	Segretario Generale	2
	Segreteria	3
	Sindaco	1
	Sociale	1
	/	1 server
Piazza Umberto I	Ambiente	2
	Economato	3

EDIFICIO	UFFICIO	POSTAZIONI DI LAVORO
	Patrimonio	2
	Personale	3
	Ragioneria	5 + 1 server
	Tributi	4
	Tecnico	5 + 1 server
Via Cantisani	Polizia Locale	2
	Biblioteca	2
Delegazione Marconia	Demografici/Anagrafe	7
	Biblioteca	5
	SUAP	4
	Sociale	2
	URP	1
	/	1 server

Tutte le postazioni di lavoro sono dotate di sistema operativo proprietario Microsoft.

13.1 L'architettura di rete

L'analisi effettuata nel paragrafo precedente rappresentava lo stato dell'ente a Dicembre 2019. Successivamente in collaborazione con il partner tecnologico Soluzioni srl di Potenza dell'ente è stato successivamente implementato un nuovo modello architetturale che è compliance alle line guida EDPB del 14-01-2021.

L'architettura di rete implementata utilizza in maniera uniforme le prescrizioni previste dalle linee guida EDPB di gennaio 2021 e si basa sul seguente modello di riferimento:

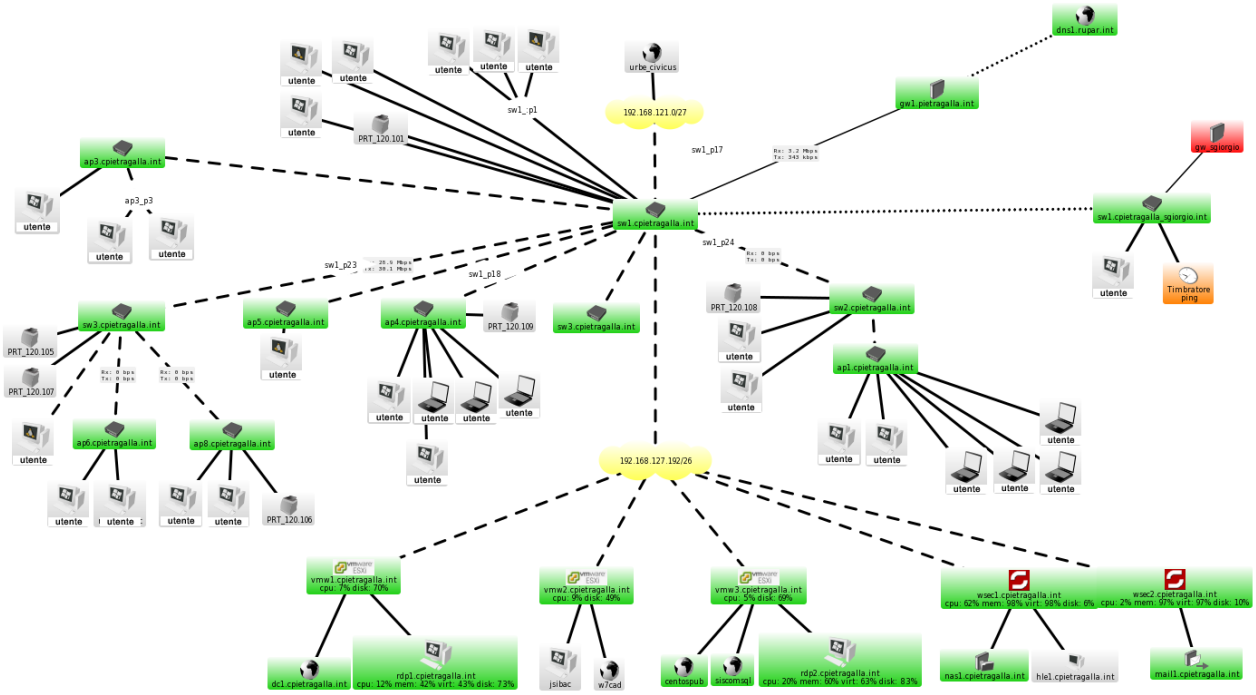


Figura 7 – Architettura di rete

L'architettura di rete implementata è basata su una topologia a stella. Consiste in uno switch, detto di centro stella, che funge da punto centrale per la trasmissione delle informazioni a cui ogni host è connesso e da una serie di switch secondari o distribuzione. In questa tipologia di rete, i dati attraversano lo switch prima di arrivare a destinazione. Ciò consente di ridurre l'impatto di un guasto sulla linea trasmissiva, collegando in modo indipendente ciascun host allo switch. La scelta di questa topologia di rete ricade sull'elevata affidabilità e flessibilità.

I vantaggi

Grande affidabilità dal momento che eventuali guasti non compromettono il funzionamento dell'intera rete. Rimane isolato solo il nodo guasto, mentre gli altri continuano a funzionare attraverso la mediazione del nodo centrale;

Facile espandibilità, cioè si possono collegare più reti a stella tra loro andando a collegare solamente gli switch come se fossero due nodi della stessa stella. Si crea dunque un concatenamento, o collegamento in cascata, da cui ha origine la cosiddetta **rete a stella in espansione.**

Rete sempre disponibile grazie a tale tipo di collegamento, per cui ogni computer può inviare dati in qualsiasi momento.

VLAN

Da questa necessità è nata l'idea di creare su un singolo switch diverse reti "virtuali" (VLAN), assegnando alle porte di esso un singolo host o un'intera rete. In questo modo, gli host appartenenti ad una rete possono comunicare solo tra loro e non con quelli collegati alle altre reti, se non per mezzo di un router connesso ad entrambe le VLAN o se consentito esplicitamente dalle policy dello switch. Invece di utilizzare uno switch "tradizionale" per ciascuna rete, su uno switch VLAN è possibile avere più reti logicamente separate come lo sono fisicamente per normali cablaggi strutturati, ma con indubbi 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.

Tecnicamente la VLAN modifica il frame di Layer 2 che viene taggato con un identificativo univoco (in sostanza il numero della VLAN), lo switch si occupa di ricevere il dato su una porta associata ad una determinata VLAN e renderlo visibile in modo trasparente solo agli apparati collegati alla porta della stessa VLAN.

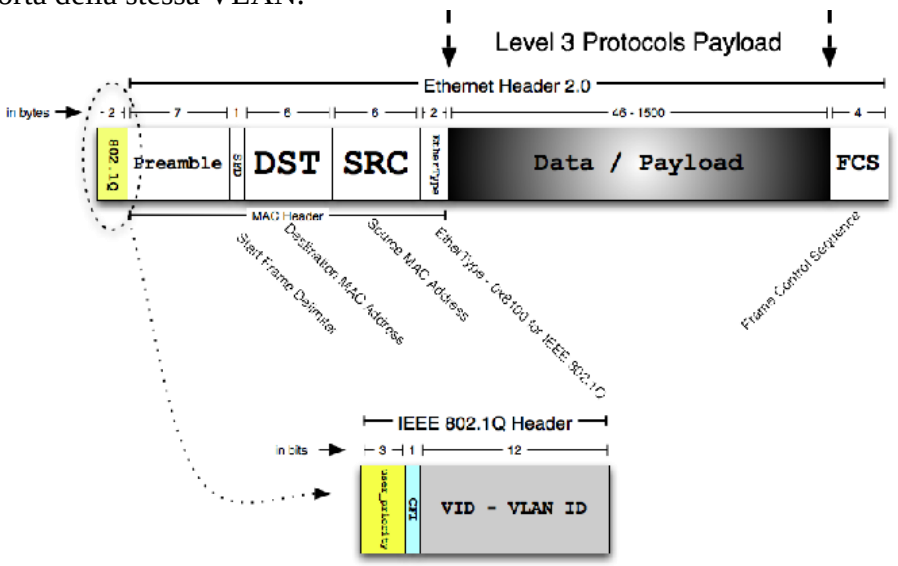


Figura 8 – VLAN Tagging

Ogni segmento di rete consente una sicurezza equivalente a reti fisiche distinte, separando granularmente i dati che la attraversano in base alla loro tipologia (rete client, rete ospiti, WiFi, VOIP, server, etc.) nonché ottimizzare le regole di protezione e privacy e di integrare la priorizzazione del traffico (QoS - Quality of Service), aumentando le prestazioni di ogni segmento.

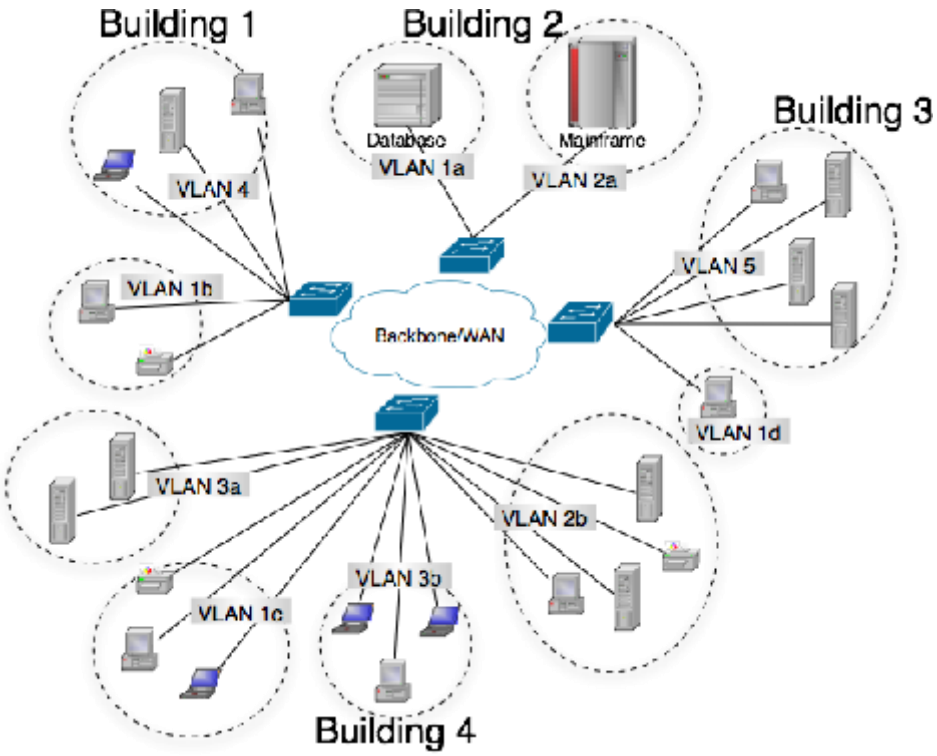


Figura 9 – Rete basata su switch e VLAN logiche

Difatti, da un punto di vista tecnico, la segmentazione della rete consente la riduzione del dominio di broadcast; pertanto, i pacchetti di rete vengono confinati all'interno del segmento.
Ciò determina una riduzione del "rumore" di rete ed un'ottimizzazione del traffico, con conseguente aumento delle prestazioni. L'associazione della segmentazione tramite VLAN all'applicazione di specifiche regole sul traffico di rete consente l'attuazione di misure preventive rispetto alla diffusione di traffico non autorizzato, determinato sia da eventuali host non conformi/autorizzati, sia a software malevolo (es. malware/cryptolocker).
Nello specifico, a titolo di esempio, l'innesco di un cryptolocker genererebbe la diffusione al solo segmento di rete interessato e non conivolgerebbe il resto della rete.

13.2 Firewall

Una corretta progettazione dell'architettura di rete, con lo scopo ultimo di garantire affidabilità, prestazioni e sicurezza, non può prescindere dall'implementazione di un sistema Firewall opportunamente configurato. Nello scenario considerato, il firewall viene implementato sullo stesso apparato che funge da centro stella, andando ad ottimizzare l'hardware in uso, a garanzia di una maggiore scalabilità. La soluzione adottata non rappresenta il classico firewall perimetrale, bensì un sistema proattivo in grado di filtrare il traffico dei vari segmenti di rete sui vari layer applicativi, ottenendo una gestione granulare delle policy di sicurezza. Il sistema dispone di automatismi in grado di implementare ACL (Access Control List), inibire l'accesso alla rete agli apparati ritenuti non idonei e bloccare in anticipo i tentativi di accesso in maniera non autorizzata sia verso l'interno della rete, sia verso l'esterno.
In particolare, viene una utilizzata una tecnologia di filtraggio degli indirizzi basata su un sistema centralizzato in Cloud, che, facendo leva su un database di sorgenti costantemente aggiornate, permette di bloccare il traffico verso indirizzi Internet catalogati come non sicuri, differenziati per categoria, ad es. indirizzi inerenti:

- pornografia
- armi
- pubblicità

- host utilizzati da malware e/o spyware
- etc.

L’implementazione di tale sistema, oltre a garantire una maggiore sicurezza per gli host presenti sulla rete locale e prevenire eventuali attacchi dall’esterno e dall’interno della rete, consente un’ulteriore ottimizzazione delle prestazioni e l’abbattimento di una notevole mole di traffico normalmente generato durante la navigazione WEB verso indirizzi non autorizzati.
Implementazione di un sistema di controllo degli accessi dei dispositivi in rete (ACL – Access Control List). Gli host presenti in rete vengono identificati e catalogati, in modo tale da identificare eventuali apparati non autorizzati collegati alla rete.

13.3 Virtualizzazione

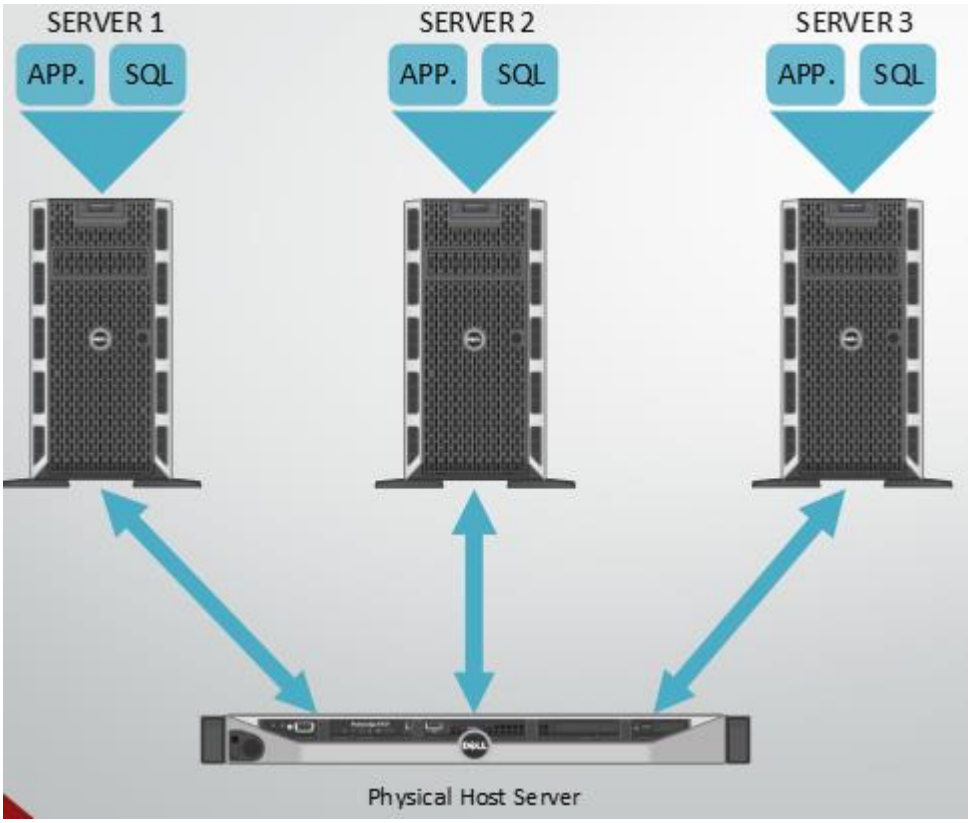


Figura 10 – Sistema di virtualizzazione

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 distribuendo le funzionalità tra più utenti o ambienti.

L'ampia applicabilità della virtualizzazione ha contribuito a ridurre il vendor lock-in e ha posto le basi del Cloud Computing, difatti la piattaforma implementata dispone a tutti gli effetti delle caratteristiche essenziali per essere migrata su sistemi Cloud in maniera piuttosto agevole.

Come funziona la virtualizzazione?

I software definiti hypervisor separano le risorse fisiche dagli ambienti virtuali che le richiedono. Gli hypervisor possono essere eseguiti in un sistema operativo (ad esempio, su un laptop) oppure installati direttamente su un hardware (server), che rappresenta la modalità di virtualizzazione utilizzata da gran parte delle aziende. Gli hypervisor ripartiscono le risorse fisiche in modo che gli ambienti virtuali possano utilizzarle.

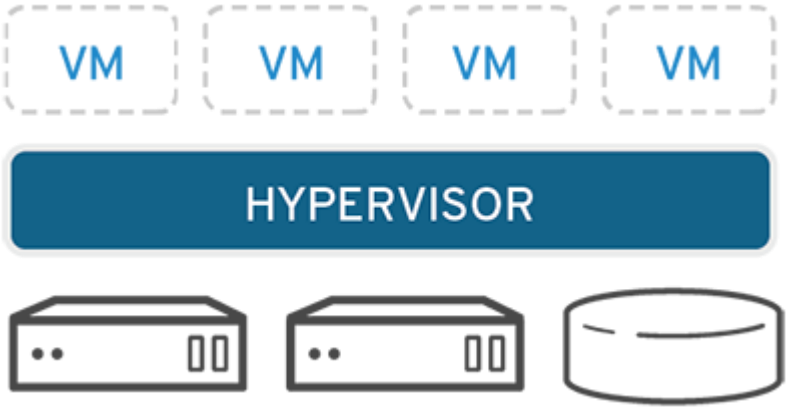


Figura 11 – Virtualizzazione dei sistemi – Virtual Machine

A seconda delle esigenze, le risorse vengono suddivise e trasferite dall'ambiente fisico ai vari ambienti virtuali. Gli utenti interagiscono ed eseguono calcoli all'interno dell'ambiente virtuale (in genere definito macchina guest o macchina virtuale). La macchina virtuale funziona come un unico file dati, che, a differenza di qualsiasi file digitale, è utilizzabile anche nel momento in cui viene spostato da un computer a un altro e aperto su più computer.

Virtualizzazione dei desktop

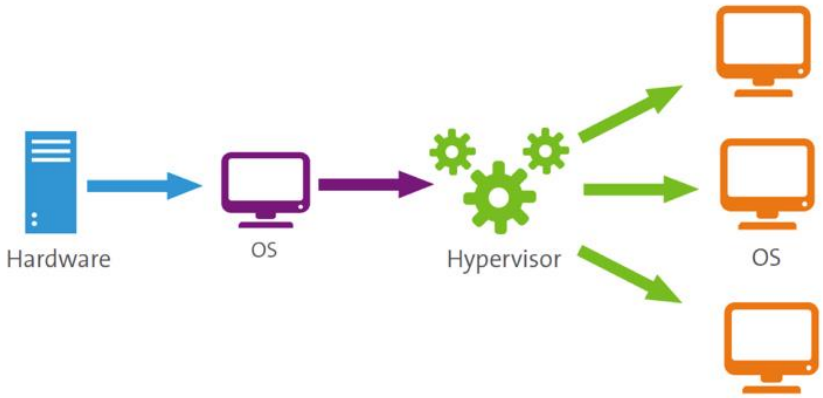


Figura 12 – Virtualizzazione dei desktop

La virtualizzazione dei desktop consente invece ad un amministratore centrale, o a uno strumento di amministrazione centralizzato basato su un dominio, di distribuire ambienti desktop simulati su centinaia di macchine fisiche, simultaneamente. A differenza di quanto accade con gli ambienti desktop convenzionali, installati, configurati e aggiornati fisicamente su ogni macchina, la virtualizzazione dei desktop consente agli amministratori di eseguire configurazioni, aggiornamenti e controlli di sicurezza in blocco, su tutti i desktop virtuali. Seguendo i dettami delle nuove normative in tema di sicurezza, gestione e centralizzazione delle informazioni, l'applicazione della

virtualizzazione ai desktop consente un controllo granulare dei profili utente e permette l'applicazione di specifiche regole di utilizzo delle "postazioni virtuali" grazie alla centralizzazione.

Virtualizzazione dei server

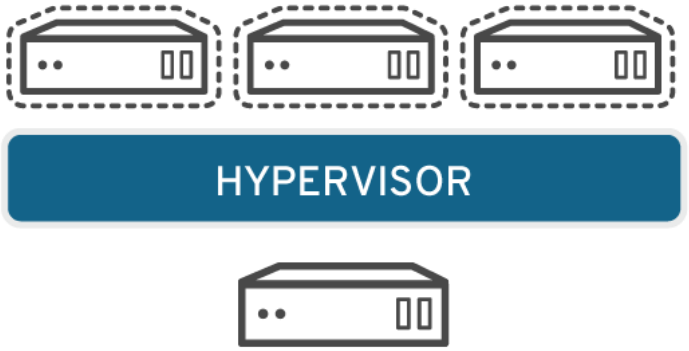


Figura 13 – Virtualizzazione dei server

I server sono computer progettati per elaborare in modo ottimale un volume elevato di attività specifiche, in modo che altri computer, come i portatili e i desktop, possano eseguire altre attività. La virtualizzazione di un server consente di eseguire più funzioni specifiche e prevede il partizionamento, in modo che i componenti possano essere utilizzati per assolvere varie funzioni.

Virtualizzazione dei sistemi operativi

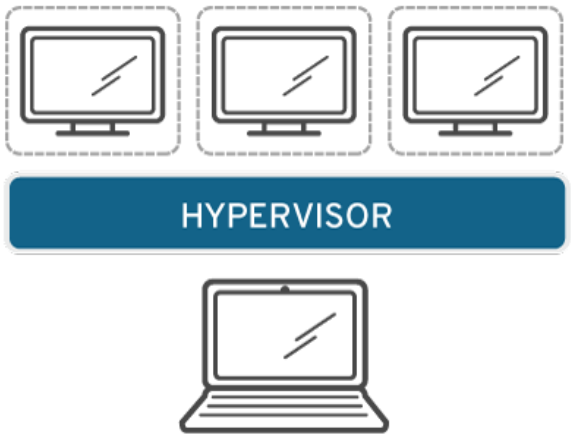


Figura 14 – Virtualizzazione dei sistemi operativi

La virtualizzazione del sistema operativo si verifica nel kernel, il sistema di gestione centrale delle attività dei sistemi operativi. È un modo utile per eseguire in modo affiancato gli ambienti Linux e Windows.

Consente di ottenere una serie di vantaggi, quali:

- ridurre il costo complessivo dell'hardware, poiché i computer non richiedono un livello elevato di funzionalità predefinite;
- incrementare la sicurezza, dato che tutte le istanze virtuali possono essere monitorate e isolate;
- limitare il tempo impiegato per servizi IT, come gli aggiornamenti software.

L'impiego della virtualizzazione, base della piattaforma, consente di ottimizzare una serie di costi, talvolta occulti, spesso non rilevati dall'Ente.

La migrazione verso i sistemi di virtualizzazione, tra l'altro, può essere applicata sistematicamente ad infrastrutture fisiche già esistenti che ne abbiano i requisiti in termini computazionali, consentendo il riutilizzo dell'hardware esistente, con notevole risparmio in termini di costi e spazio fisico utilizzato.

13.4 Storage

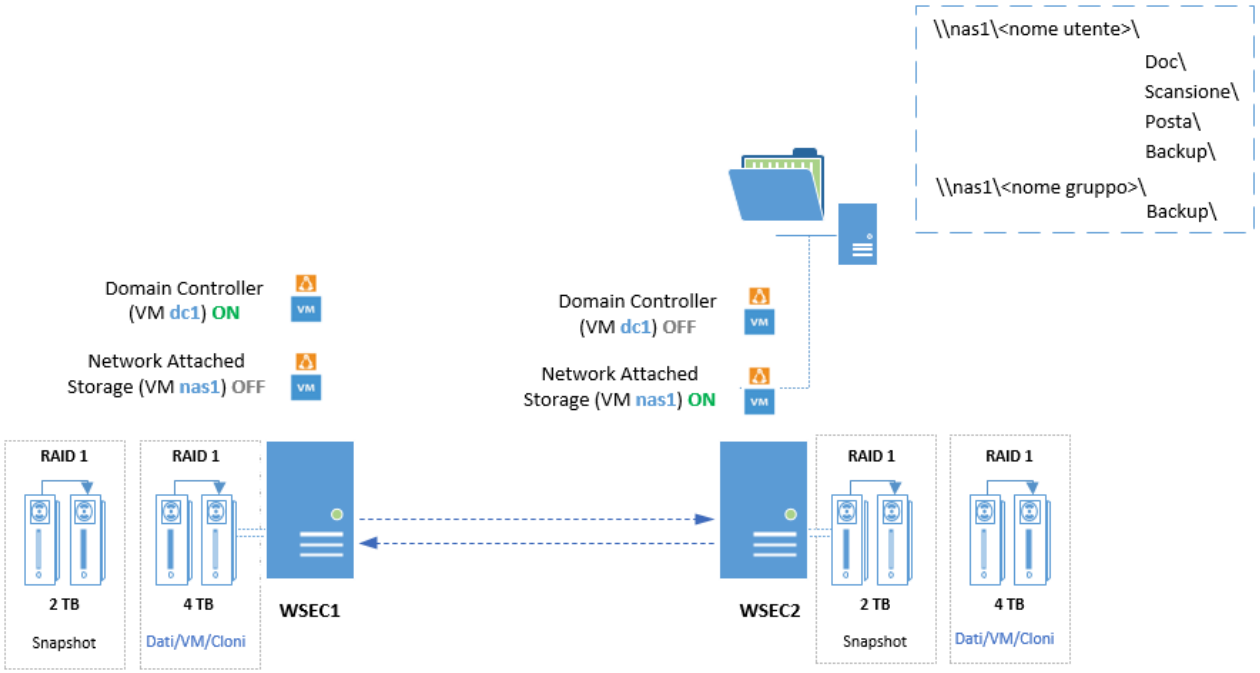


Figura 15 – Architettura Storage

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.

Alta affidabilità e Backup
Il filesystem organizzato in questo modo consente una gestione agevole degli 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. Gli snapshot riguardano un intero volume del filesystem e sono al tempo stesso efficienti in termini di velocità di esecuzione ed occupazione di spazio. Ulteriore vantaggio rappresentato da questa tipologia di filesystem di nuova generazione è la possibilità di creare un sistema ridondante, utilizzando una macchina secondaria sulla quale replicare il filesystem e prevedere un invio temporizzato degli snapshot. Rilevando soltanto le differenze a livello di blocchi del filesystem, gli snapshot risultando molto contenute rispetto ad un tradizionale sistema di backup incrementale/differenziale e ciò consente una replica agevole verso sistemi secondari.

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/Azienda e dati ritenuti sensibili.

Prevenzione
Gli storage non hanno soltanto la classica funzione di archiviazione dei dati, ma sono a tutti gli 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.
Sulla base di alcune politiche implementate nel servizio, rilevando un possibile inizio di attività da parte dell'applicazione malevola, il sistema rende automaticamente inaccessibili le aree dati personali e centralizzate. Pertanto, si confina in maniera ottimale un eventuale tentativo di criptazione dei dati.

Rimedio
Come ben sappiamo, la prevenzione è solo una delle armi in possesso degli operatori di tecnologia che può in qualche modo mitigare attività malevole. Spesso da sola non è in grado di proteggere l'integrità e la disponibilità dei dati, pertanto, si rende necessario disporre di soluzioni di backup che consentano un ripristino dei dati in maniera efficace ed agevole. 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.

13.5 Formazione al dipendente

Un fattore fondamentale nell'ottica della prevenzione di eventi dannosi, quali esfiltrazione di dati, furti di identità, corruzione e/o perdita dati, è la formazione del personale.
In un contesto di gruppo dell'Ente, il fattore umano è spesso determinante per valorizzare quanto messo a disposizione dall'infrastruttura tecnologica.
L'attività formativa è la diretta conseguenza dell'implementazione di una piattaforma tecnologica che si pone come obiettivo quello di massimizzare la sicurezza e rendere al tempo stesso agevole il lavoro dell'utente, in linea con le nuove normative a cui principalmente le P.A. devo adeguarsi.
Tale attività viene erogata secondo un flusso di lavoro ben determinato che parte da un'infarinatura sui concetti base della sicurezza informatica e del corretto utilizzo della PDL - postazione di lavoro – fino a toccare temi più specifici relativamente alla privacy ed alla protezione delle informazioni.
Nello specifico si cerca di sensibilizzare l'utente sui temi cardine della **sicurezza delle informazioni**:

- Riservatezza
- Integrità
- Disponibilità

Viene data particolare enfasi alla presenza del **dominio** che consente la centralizzazione degli accessi e la corretta gestione dei singoli profili utente.

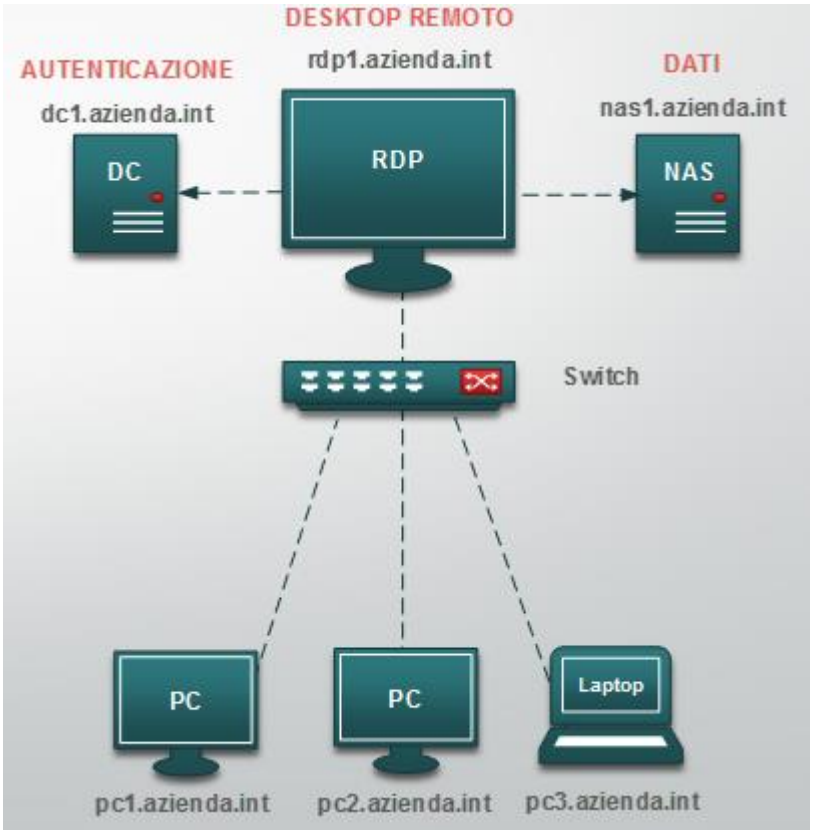


Figura 16 – Architettura di rete

In particolare, viene approfondita una modalità di lavoro improntata sulla centralizzazione dei dati e degli accessi, che evita un utilizzo della PDL nella classica modalità "casalinga" ed educa l'utente al concetto di separazione dei dati dalle applicazioni. Si approfondisce l'utilizzo del desktop virtualizzato che fa cadere il concetto classico di PDL legata all'hardware fisico: infatti attraverso tale tecnologia, l'utente dispone di un proprio desktop virtuale accessibile da postazioni fisiche differenti presenti nella rete locale. Diventa, inoltre, un sistema altamente fruibile per il lavoro in "smart working", in quanto, grazie alla separazione tra hardware della singola postazione profilo utente, che risiede su un sistema centralizzato, l'utente può collegarsi, attraverso VPN, al proprio profilo direttamente dal computer di casa o da altri sistemi autorizzati, accedendo in maniera trasparente al proprio profilo come se fosse fisicamente dinanzi alla sua postazione, senza la necessità di avere il computer dell'ufficio acceso. Approfondito il tema della centralizzazione attraverso il dominio, l'accesso flessibile al proprio profilo, l'accesso remoto sicuro tramite VPN, si fa leva in seguito sulla corretta gestione del dato, dalla creazione alla registrazione. Si dà particolare rilevanza all'utilizzo delle partizioni crittografate che consentono l'archiviazione di dati ritenuti particolarmente importanti e/o sensibili, alle modalità di trasferimento dei dati in rete, evitando il più possibile l'utilizzo di pendrive e/o dispositivi personali esterni all'Ente ed alla corretta gestione dei dati di backup.

14. 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 così 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.

15. 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
- Martorana Marco (2018), *GDPR e Decreto Legislativo 101/2018*, CEDAM
- Montanile Flavia- Montanile Massimo (2021), *Un modello per la sicurezza dei dati personali nell'era digitale*, Tab Edizioni
- Perego Monica (2017), *Privacy & Audit*, IPSOA
- 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"
- Soffientini Marco (2018), *Privacy- Protezione e trattamento dei dati*, IPSOA

16. 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
- https://www.comunedipisticci.it/index.php/privacy.html

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