GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

Regolamento Privacy Unione Europea (2016/679) relativo al trattamento dei dati personali dei cittadini della Comunità Europea

Renato Narcisi – NetSense S.r.l.

Contesto normativo di riferimento

1995	Direttiva U.E. 94/46/CE
Dicembre 1995	Legge 675/96 che recepisce la direttiva
1999	D.P.R. 318/1999 (misure minime di sicurezza da adottare per il trattamento dei dati personali
01-01-2004	Va in vigore il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) altrimenti detto “Testo unico sulla privacy”
2004	Provvedimento sulla videosorveglianza
27-11-2008	Viene definito il ruolo degli Amministratori di Sistema
08-04-2010	Secondo provvedimento sulla videosorveglianza che sostituisce quello del 2004
04-05-2016	Viene pubblicato sulla G.U. Dell’U.E. Il General Data Protection Regulation (GDPR) – Regolamento UE 2016/679 o Regolamento Generale sulla Protezione dei Dati (RGPD)
2016-2018	Linee Guida Gruppo Articolo 29
25-05-2018	Il GDPR trova piena attuazione e nasce il Comitato europeo per la protezione dei dati
19-09-2018	Entra in vigore il decreto di attuazione del RGPD, D.Lgs. 101/2018

Era davvero necessaria?

ERRORE TIPICO: obiettare che non si ha nulla da nascondere.

E se i dati che non nascondiamo passassero di mano in mano e fossero male interpretati?

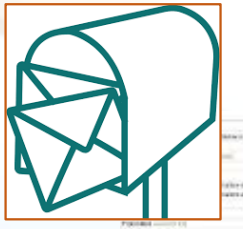
ESEMPIO: CARD NOMINATIVE DEI SUPERMERCATI

minimarket familiare → catene supermercati → fondi di investimenti

RISULTATO:
Miei comportamenti si potrebbero riflettere nelle richieste di mutui/servizi assicurativi
Non è fantascienza: In UK è successo proprio questo alle catene di PUB

Negligenti con le nostre mail?

Mia mail



tutti i documenti che sono transitati negli anni dalla mail:

- CI / CF
- estratti conto bancari (IBAN / ecc)
- conti telefonici e numeri di SIM

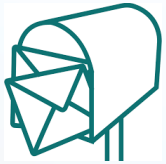
POTENZIALE FURTO DELLA MIA IDENTITA', CLONAZIONI SIM, ALTRO

- **ricatti**
- **furti di account più importanti**
- **ecc.**

Errore tipico che genera vulnerabilità

Secondo Esempio :
REGISTRAZIONE NEI VARI SITI UTILIZZANDO SEMPRE LA STESSA MAIL

Mia mail



renato.narcisi@netsenseweb.com
password123

1 iscrizione a vari siti

renato.narcisi@netsenseweb.com
password123

renato.narcisi@netsenseweb.com
differentePassword

renato.narcisi@netsenseweb.com
altraPassword

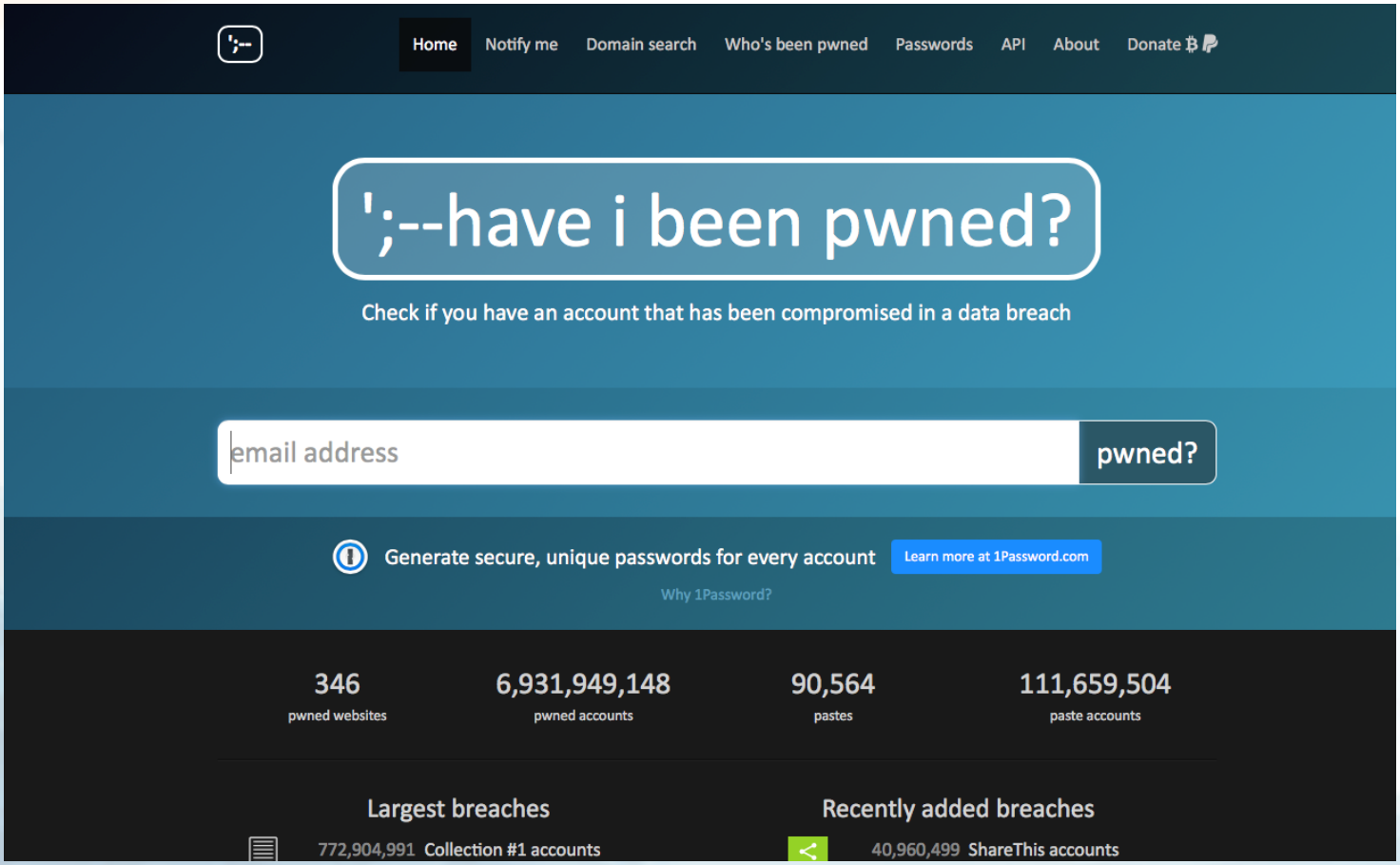
2 siti brecciati

3

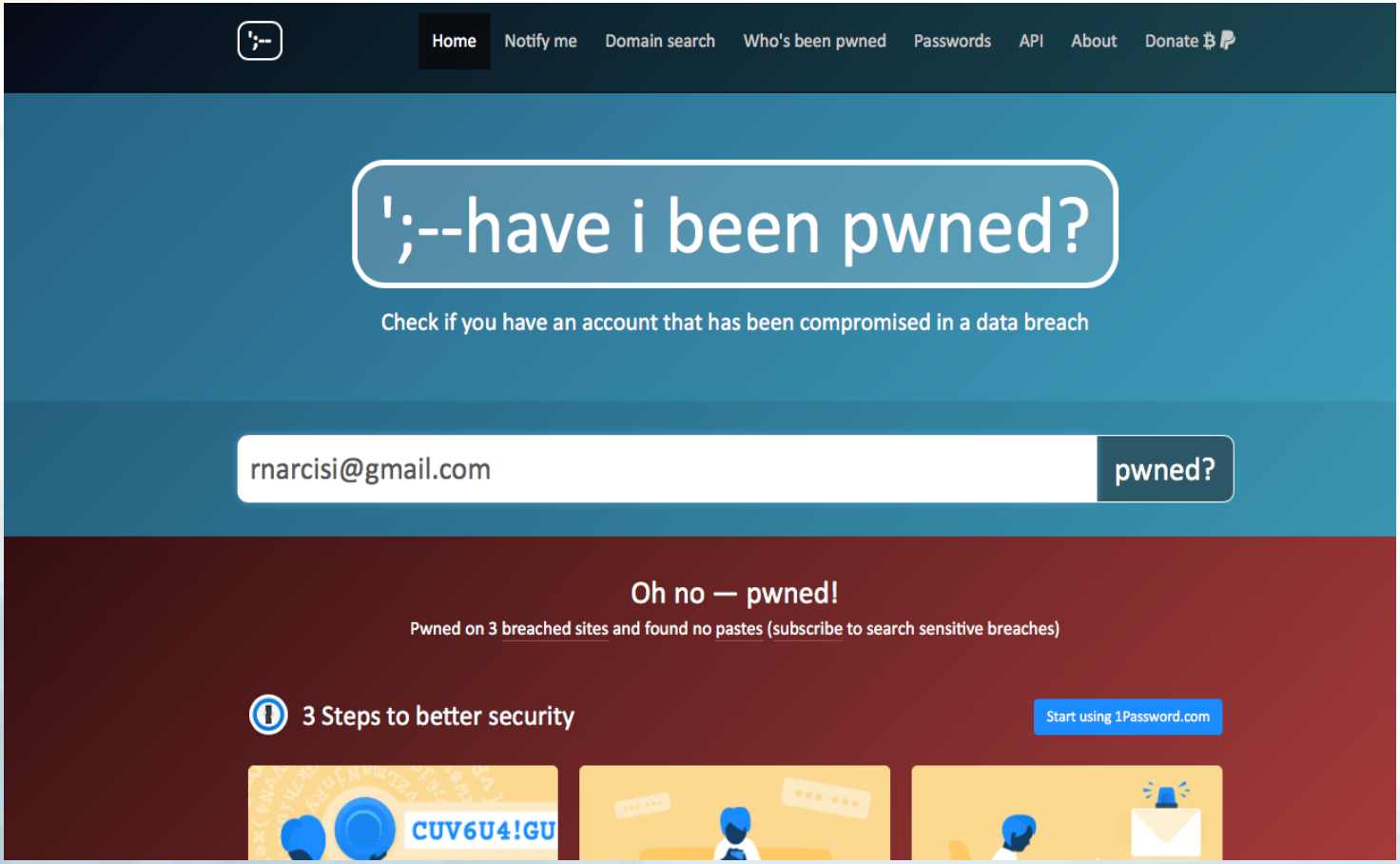
BINGO!!! (si fa per dire)
una delle tre credenziali corrisponde
sono entrati nella mia mail…..

renato.narcisi@netsenseweb.com / differentePassword
renato.narcisi@netsenseweb.com / password123
renato.narcisi@netsenseweb.com / altraPassword

E‘ capitato a me? https://haveibeenpwned.com



https://haveibeenpwned.com



COSA FARE?

- Cambiare password nella propria mail.

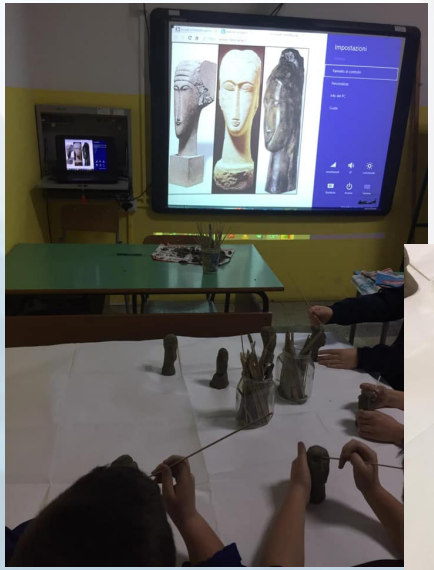
- Utilizzare una mail SOLO per le cose importanti e una seconda per le altre

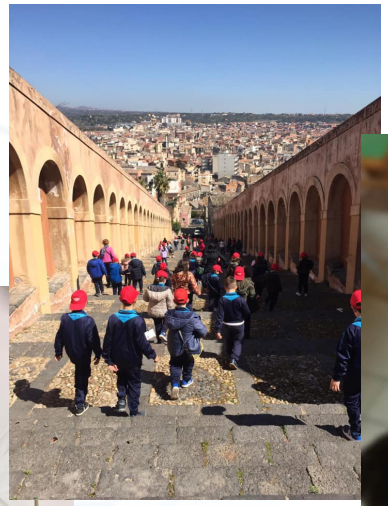
MA SOPRATTUTTO:
Imparare che la password è importante quanto le chiavi di un oggetto materiale.

La responsabilità di furti di dati / perdita di privacy /ecc. ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

MISURE DI CAUTELA : FOTO / VIDEO

Realizzarli senza primi piani (foto di gruppo) oppure sfumate / oscurate





MISURE DI CAUTELA : FOTO / VIDEO (caso genitori)

NOTA PRIVACY

LINEE GUIDA DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LE FOTO ED I VIDEO RIPRESI DURANTE LE RECITE ED ALTRE INIZIATIVE SCOLASTICHE POSSONO ESSERE UTILIZZATI SOLO PER FINI PERSONALI E DESTINATI AD UN AMBITO FAMILIARE O AMICALE.

LA DIFFUSIONE DI TALI FOTO E VIDEO ATTRAVERSO CANALI SOCIALI (FACEBOOK / ECC.), WEB O QUALSIASI ALTRO MEZZO DI COMUNICAZIONE VIOLA LE NORMATIVE VIGENTI IN MATERIA.

MISURE CAUTELA : PASSWORD

CHIARO RIFERIMENTO: (Gestionali e Registro Elettronico)

Perché rispettare le prescrizioni del Codice nella scelta delle password?

Se qualcuno accede ad un computer o ad un servizio WEB potrà impossessarsi di dati personali e aziendali.

La responsabilità di questa sottrazione ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

Il 90% dei furti di identità sono riconducibili ad un uso non responsabile delle password

La password

Suggerimenti per creare una password sicura (tratto dal sito della polizia postale):

- Creare una password di minimo dieci caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati: ! $? # = * + - . , ; :
- Includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad esempio il numero “0” per la lettera “O” o il carattere “$” per la lettera “S”).
- Creare un acronimo univoco (ad esempio "PDRM" per "Piazza Delle Repubbliche Marinare").

Includere sostituzioni fonetiche o grafiche (ad esempio “6 arrivato” per “Sei arrivato” o “Arrivo + tardi” per “Arrivo più tardi”).

Da evitare:

- Non utilizzare le stesse password per più account.
- Non usare una password già utilizzata in un esempio di come si sceglie una buona password.
- Non utilizzare una password contenente dati personali (nome, data di nascita, ecc.).
- Non usare parole o acronimi che si possono trovare nel dizionario.
- Non usare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234).
- Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.
- Non usare ripetizioni di caratteri (aa11).

Suggerimenti per tenere al sicuro la password:

- Non comunicare a nessuno la password (inclusi partner, compagni di appartamento, colleghi, ecc.).
- Non lasciare la password scritta in posti facilmente raggiungibili da altri.
- Non inviare mai la password per email.
- Verificare periodicamente la password corrente e cambiarla con una nuova.

La password - Le linee guida del NIST

Password complesse?
Dalla ricerca del NIST è emerso che gli utenti, quando venivano costretti a scegliere dei simboli o dei numeri, si affidavano quasi sempre agli stessi: i più usati sono i numeri 1,2 e 3 e il punto esclamativo.

Gli hacker, conoscendo questa tendenza, sono spesso riusciti a rubare password, anche complesse.

CONSIGLIO: UTILIZZARE APP O SOFTWARE PORTACHIAVE

APP o Software portachiave

Sono software nei quali memorizzare tutte le proprie password.

- saranno crittografate
- accessibili solo da noi attraverso una masterpassword
- la masterpassword è protetta attraverso una "autenticazione a due vie"
- altro (in base al tipo di software scelto)

- **Consiglio: LastPass, sia Free che Premium (30 Euro /anno)**

FACEBOOK / ALTRI SOCIAL NETWORK

Facebook ricorda che utilizzando il social network l'utente accorda all'azienda di Zuckerberg "*licenza non esclusiva, trasferibile, che può essere concessa come sottolicenza, libera da royalty e valida in tutto il mondo, che consente l'utilizzo dei contenuti (...) pubblicati su Facebook o in connessione con Facebook*".

In altre parole, **Facebook si dichiara libera di utilizzare le foto e gli altri contenuti conferiti dall'utente ovunque lo ritenga opportuno e senza versare un centesimo in termini di royalty**. I contenuti, foto comprese, restano quindi di proprietà dell'utente ma Facebook non dovrà versare alcun corrispettivo economico se vorrà riutilizzarle. Eventuali società con cui Facebook abbia stretto un accordo, potranno a loro volta - sulla base di un'apposita licenza - riutilizzare lo stesso materiale.

CONCLUSIONE : NO PUBBLICAZIONE FOTO SU SOCIAL NETWORK

solo informazioni o foto anonimizzate

POSSIBILI MISURE TECNICHE DA ADOTTARE – RETE DATI

B) MISURE TECNICHE – RETE DATI (rete WIFI, rete aule e laboratori e rete segreteria)

FIGURA COINVOLTA: AMMINISTRATORE DI RETE

- verificare la separazione fisica (o con VLAN) delle tre rete
- autorizzare l'uso della rete a personale autorizzato con l'uso di credenziali personali (user e password individuali!)
- mantenere tracciati di navigazione anonimi (quale PC dall'interno ha generato un certo traffico verso Internet)
- mantenere altri tracciati (DHCP, accessi in rete, ecc.)
- rispettare le indicazioni AGID (circolare 2/2017(su DPCM 01/08/2015 relativo a misure minime sicurezza ICT

Esigenza funzionale: su più linee Internet, implementare meccanismi di failover (spostare le varie reti sulle linee di uscita più performanti)

POSSIBILI MIS. TECNICHE DA ADOTTARE – PC AULE E LAB

C) MISURE TECNICHE – PC AULE E LABORATORI

FIGURA COINVOLTA: AMMINISTRATORE DI SISTEMA

Problema: spesso documenti riservati (es. relazioni attività con soggetti BES o password di registro informatico) vengono dimenticati nei PC ad uso “promiscuo”.

Problema2 : nelle scuole esiste normalmente un parco macchine esteso (tanti PC)

Soluzione che mette d’accordo esigenze tecniche (basso costo manutenzione) e GDPR:

- UTILIZZO SOFTWARE DI CONGELAMENTO DELLA CONFIGURAZIONE SU TUTTI I PC

(reboot and restore RX / deep freeze / ecc.)

La password di congelamento e scongelamento: all’amministratore di sistema

POSSIBILI MIS. TECNICHE DA ADOTTARE – SEGRETERIA

D) MISURE TECNICHE – PC E SISTEMI SEGRETERIA

FIGURA COINVOLTA: AMMINISTRATORE DI SISTEMA

Obiettivo1: nessuno deve leggere dati da Hard Disk, anche sottratti dalla segreteria

Obiettivo2: nessun dato deve perdersi, anche a seguito di danno o furto

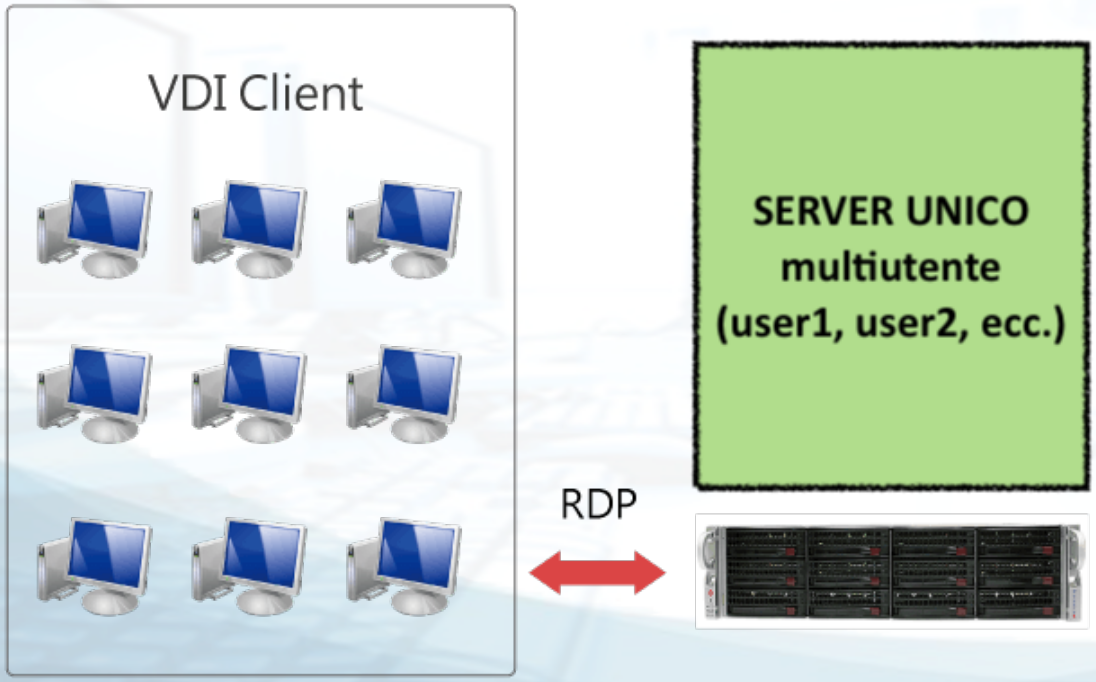
Soluzione 1 :

- UTILIZZO SOFTWARE FREE DI CRITTOGRAFIA PER GLI HARD DISK (BitLocker / File Vault)
- UTILIZZO DI SISTEMI FREE DI SINCRONIZZAZIONE DEI FILE PROPRI (owncloud / nextcloud) Attenzione: no dropbox, gdrive, eccetera.
- UTILIZZO DI SISTEMI DI BACKUP AUTOMATICI DELL'INTERO SISTEMA (ACRONIS ecc.)

POSSIBILI MIS. TECNICHE DA ADOTTARE – SEGRETERIA

Soluzione avanzata che mette d'accordo basso costo manutenzione e GDPR:

- segreteria in un'unica macchina server e postazioni di segretr. veri e propri terminali



Data Breach (art. 33, C85, C87, C88)

ATTENZIONE alle **chiavette USB** e agli **Hard Disk portatili**

L’enorme diffusione di questi dispositivi, nonché la loro praticità e semplicità di utilizzo può comportare problemi anche gravi ai dati aziendali contenuti.

Nella stragrande maggioranza dei casi, i dati contenuti in questi dispositivi non sono protetti. Lo smarrimento, quindi, dovrebbe portare alla notificazione di data breach al Garante sulla Privacy.

Una soluzione semplice e poco costosa potrebbe essere quella di usare dei software di crittografia sui dispositivi USB forniti dall’azienda.

I trattamento dei dati cartacei

ATTENZIONE alla carta riciclata!

ATTENZIONE alle stampe che si lasciano!

Se la stampante è condivisa con altri utenti o è fuori dal campo visivo evitare di lasciare le stampe per troppo tempo, perché degli utenti non autorizzati potrebbero visualizzarle o asportarle.

I trattamento dei dati cartacei

Per eliminare dati sensibili cartacei utilizzare il distruggi documenti.

Il livello di sicurezza di un distruggi documenti è dettato dalla norma DIN 66399:

Livello di sicurezza 1: Documenti di carattere generale devono essere invalidati o resi illeggibili.
Livello di sicurezza 2: Documenti interni che devono essere invalidati o resi illeggibili.
Livello di sicurezza 3: **Supporti dati con dati sensibili,** riservati e personali che richiedono una maggiore protezione.
Livello di sicurezza 4: Supporti dati con dati particolarmente sensibili e riservati nonché dati personali che richiedono una maggiore protezione.
Livello di sicurezza 5: Supporti dati con informazioni strettamente segrete di rilevanza per l'esistenza di una persona, azienda o istituzione.
Livello di sicurezza 6: Supporti dati con documenti strettamente segreti, quando è necessario.
Livello di sicurezza 7: Per dati strettamente segreti, per cui necessario adottare le misure di prevenzione di massima sicurezza.

Il GDPR e i servizi in CLOUD

SI CONOSCE QUALI SIANO LE MISURE DI SICUREZZA ADOTTATE DAL FORNITORE PER PROTEGGERE I DATI?

Il Titolare del trattamento **ha sempre l'obbligo di indicare le misure di sicurezza e verificare che siano rispettate dai propri fornitori**. Pertanto, è necessario chiedere dettagliate informazioni al fornitore del servizio su questo punto.

DOVE SI TROVANO FISICAMENTE I SERVER DOVE RISIEDONO I DATI?

In Italia: il trattamento dei dati non richiede nessun adempimento;

In un paese della Comunità Europea:

vale il trattato di Schengen, ribadito dal nuovo Regolamento Europeo, che permette la libera circolazione dei dati, ma si deve comunicare agli interessati che i loro dati usciranno dall'Italia;

Il GDPR e i servizi in CLOUD

In un paese extraeuropeo:
la soluzione è sconsigliata. Per scegliere questa soluzione è necessario che **siano assicurate dal fornitore misure di sicurezza pari o superiori a quelle che si avrebbero nei paesi europei.**

Per prima cosa bisogna vedere se il paese extraeuropeo è nella lista dei paesi considerati affidabili, quindi bisogna **verificare se vengono adottate le misure previste dalla Commissione Europea.**

Verificato che sia tutto in regola, **rimangono due ulteriori obblighi**:

1. comunicare agli interessati che i loro dati usciranno dai confini europei;
2. provvedere alla notifica al Garante.

Il GDPR e i servizi in CLOUD

È STATO VALUTATO L'IMPATTO AZIENDALE CHE SI AVREBBE SE I DATI SUL CLOUD ANDASSERO PERSI O DISTRUTTI?

I dati non sono da noi. Se il fornitore o uno della filiera fallisse? Se fosse attaccato da un pirata informatico? Se avesse dei problemi legati ad un evento fisico (terremoto, incendio, alluvione, ...). I dati delle aziende hanno un valore elevatissimo ed è meglio **predisporre adeguate misure di backup** con varie tipologie di frequenza (per maggiori garanzie temporali) e vari punti di stoccaggio (per delocalizzare sul territorio il rischio).

ESISTONO GARANZIE DI RISERVATEZZA PER I NOSTRI DATI NEL CASO IN CUI UN CONCORRENTE CONDIVIDA GLI STESSI SERVIZI CLOUD?

Chi offre un servizio alla mia azienda in cloud, offrirà lo stesso servizio anche ai miei concorrenti. **Quali sono le logiche a garanzia della sicurezza dei miei dati aziendali**? Chi e come gestisce i criteri di accesso e le politiche di password? Vi è possibilità di accedere facilmente alla mia password?

Il GDPR e i servizi in CLOUD

LA TECNOLOGIA UTILIZZATA DAL FORNITORE DI CLOUD È DI TIPO "PROPRIETARIO"? I DATI POSSONO ESSERE ESPORTATI FACILMENTE?

Nell'ipotesi in cui un giorno si voglia cambiare fornitore del servizio, i dati caricati fino a quel momento sono facilmente esportabili? Il fornitore garantisce il rispetto del diritto alla portabilità dei dati previsto dal GDPR?

NEL CASO IN CUI SI ACCERTI UNA VIOLAZIONE O LA PERDITA DEI DATI, IL FORNITORE GARANTISCE UN PRONTO RISARCIMENTO DEL DANNO?

Non è più un tema da sottovalutare. Con il nuovo GDPR, ogni violazione dei dati (data breach) deve essere segnalata al Garante e in alcuni casi anche agli interessati. Questo significa almeno due cose: la prima che **devo essere certo che il mio fornitore mi comunichi un data breach in tempi veloci e certi** per adempiere alle richieste del Garante, la seconda che **abbia la capacità economica o assicurativa di rispondere alle richieste di risarcimento.**

Ransomware cos'è?

Il ransomware è un programma informatico dannoso che infetta un dispositivo (PC, Tablet, Smartphone, Smart TV), bloccando l'accesso ai contenuti (foto, video, file) e chiedendo un riscatto (ransom) per «liberarli».

La richiesta di pagamento con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato.
L'utente ha pochi giorni per pagare, poi il blocco dei file diventa definitivo.

Ci sono 2 tipi principali di ransomware:
Cryptor: criptano i file contenuti nel dispositivo rendendoli illeggibili;
Blocker: bloccano l'accesso al dispositivo infettato.

Ransomware come si diffonde?

Il ransomware si diffonde soprattutto attraverso messaggi inviati via e-mail, sms o chat o che appaiono su pagine web e social network, che sembrano provenire da soggetti conosciuti e sicuri (corrieri espressi, gestori di servizi (acqua, luce, gas), operatori telefonici, soggetti istituzionali ecc.

Chi li riceve è indotto ingannevolmente ad aprire allegati o a cliccare link o banner collegati a software dannosi.

Il dispositivo infettato può a sua volta «contagiarne» altri, perché il ransomware, impossessandosi della rubrica dei contatti, può utilizzarla per spedire automaticamente messaggi contenenti file dannosi.

Ransomware come difendersi?

La prima difesa dai ransomware è **evitare di aprire messaggi provenienti da soggetti sconosciuti** o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere da cui non si aspettano consegne, ecc.) e non cliccare su collegamenti a siti sospetti.

E' utile installare un **antivirus con estensione per malware** sui propri dispositivi e mantenere aggiornato il sistema operativo.

E' fondamentale **effettuare backup periodici dei contenuti**, così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, i dati in esso contenuti non verranno persi.

Ransomware come liberarsene?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in liste di «pagatori», potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.
Oppure si può formattare il dispositivo, ovviamente se si ha a disposizione un backup. E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia Postale, anche per aiutare a prevenire ulteriori truffe.

Grazie per l’attenzione

Per qualsiasi informazione contattateci a:
info@netsenseweb.com
095.8996123 / 095.334673