Cybersicurezza
Business continuity

GDPR General Data Protection Regulation

innovare
futuro semplice

CyberSicurezza

La sicurezza informatica (in inglese information security) è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici.

Un sinonimo spesso usato è cybersecurity, termine che ne rappresenta una sottoclasse essendo quell'ambito della sicurezza informatica che dipende solo dalla tecnologia.

Con esso si enfatizzano spesso qualità di resilienza, robustezza e reattività che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance (attacchi cyber).

Nella sicurezza informatica sono coinvolti elementi tecnici, organizzativi, giuridici e umani.

Per valutare la sicurezza è solitamente necessario individuare le minacce, le vulnerabilità e i rischi associati agli asset informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore a una determinata soglia di tollerabilità (es. economico, politico-sociale, di reputazione, ecc...) a un'organizzazione.

Oltre alle tre fondamentali proprietà (riservatezza, integrità, disponibilità) possono essere considerate anche: autenticità, non ripudiabilità, responsabilità, affidabilità.

LA STAMPA

Un attacco hacker ha bloccato la città di Atlanta

Per cinque giorni, un ransomware ha colpito i computer di 8mila dipendenti pubblici

Durato cinque giorni e terminato giovedì 29 marzo, L'attacco ha colpito i sistemi informatici della corte di giustizia, dell'amministrazione comunale e dei centri per l'impiego. 8mila dipendenti pubblici **non hanno potuto accendere i computer e per lavorare hanno dovuto utilizzare carta e penna.**

Gli Hacker obbligano a tornare a carta e penna.

Circa un anno fa 8000 dipendenti pubblici di Atlanta (Stati Uniti) si sono visti bloccare i computer dai Cyber Criminali e sono stati costretti a lavorare per 5 giorni in stile vecchia scuola: carta e penna.

Tanto per fare un inciso: stiamo parlando dei grandi, tecnologici, all'avanguardia, Stati uniti. Non abbiamo detto l'ultimo dei paesi in via di sviluppo a livello tecnologico!

Cosa li ha colpiti? Un Cryptolocker.

Un Cryptolocker è, a grandi linee, un tipo di virus che limita l'accesso ai tuoi dati.

Ti chiude fuori dal tuo stesso computer.

Questo tipo di malware è conosciuto come Ransomware. Ransom in inglese vuol dire riscatto, ed è quello che gli hacker chiedono per sbloccare l'accesso.

In poche parole vi rapiscono il computer!

380.000 carte di credito rubate in un colpo solo!

Quello di cui parliamo ora è una delle altre possibili minacce, il Data Breach. **Un Data Breach è un incidente di sicurezza in cui dei dati riservati vengono rubati da un soggetto non autorizzato.**

L'incidente accaduto a **British Airways nel settembre 2018** è stato considerato il primo grande Data Breach dell'era post GDPR.

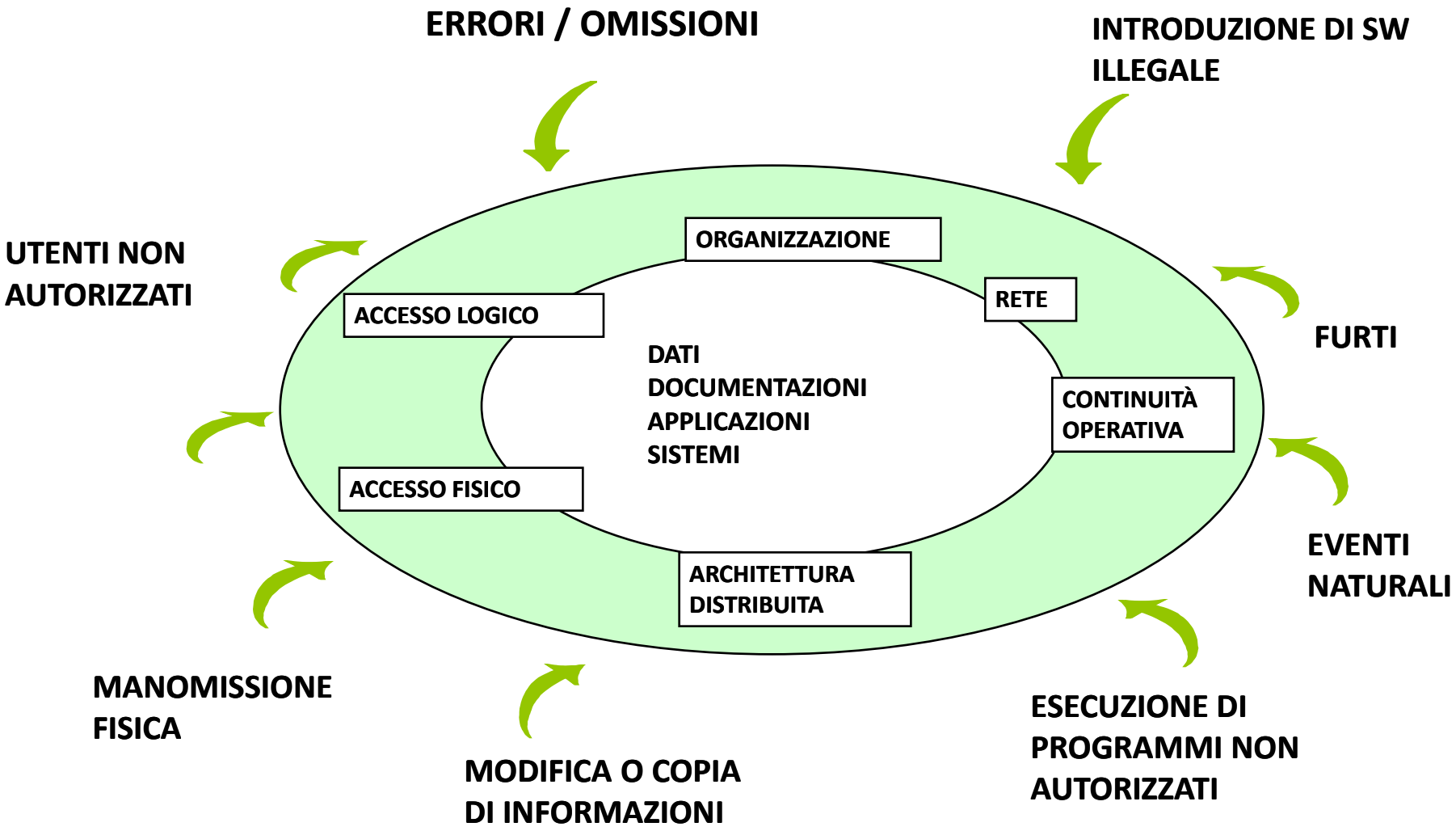
La compagnia aerea si è vista sottrarre le **informazioni relative alle carte di credito di 380.000 Clienti!**

Di questi giorni invece la notizia che vede attribuire proprio a British Airways una **multa per questo evento di circa 204 Milioni di Euro**.

Potranno fare ricorso e appellarsi ma il fatto non è tanto cosa comporterà per loro.

Questa multa diventa sintomatica perché è l'esempio di quanto siano gravi questo tipo di attacchi e dei danni, diretti e indiretti, che possono creare.

Ma COSA ACCADE quando avviene una violazione di dati?



Business Continuity

La Business Continuity nacque verso la fine degli anni '70 negli Stati Uniti d'America come conseguenza dell'avvento dell'Information Technology nelle aziende. I manager si resero conto che in caso di malfunzionamento dei sistemi IT, non era più possibile tornare a processi manuali. Pertanto iniziarono a riflettere sulla continuità dei processi IT, attraverso le prime attività di Disaster Recovery. Una delle difficoltà iniziali dei tecnici chiamati a fare queste riflessioni fu quella di giustificare investimenti significativi per preparare l'organizzazione a reagire a eventi distruttivi con bassa probabilità di accadimento. Si instaurò così verso la metà degli anni '80 la prima metodologia di Business Impact Analysis, che venne originariamente applicata al solo ambito informatico.

La disciplina iniziò quindi a evolversi e a essere implementata anche in altri Paesi anglosassoni (principalmente nel Regno Unito e in Australia). Negli anni '90 le organizzazioni incominciarono inoltre ad allargare la riflessione anche alle risorse umane, agli asset fondamentali e ai processi aziendali nel loro complesso. In quegli stessi anni il *British Standards Institution* lanciò un primo standard per la sicurezza informatica, che negli anni è stato modificato fino a diventare l'attuale Norma ISO/IEC 27001:2013) che tra i principi fondamentali enunciava la necessità di continuità operativa, definita ai tempi ancora in termini di disponibilità dei dati.

Approvato il14 aprile 2016
dal Parlamento Europeo e pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016

Efficace dal **25 maggio 2018**

G.D.P.R. 2016/679
PROTEZIONE DEI DATI E PRIVACY

UNA NUOVA RICCHEZZA: I DATI

DIGITALIZZAZIONE:
aumento dei dati,
facilità di archiviazione e trasmissione

RISERVATEZZA
(**art. 7 Carta di Nizza**)
Rispetto della vita privata e della vita familiare
Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

TUTELA DEI DATI
(**art. 8 Carta di Nizza**):
Protezione dei dati di carattere personale
1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

G.D.P.R. 2016/679
14. MISURE DI SICUREZZA

Considerando 83

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe

valutare i rischi inerenti al trattamento

e

attuare misure per **limitare tali rischi**

G.D.P.R. 2016/679
14. MISURE DI SICUREZZA

Sicurezza del trattamento (art. 32)

Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, dell'**oggetto**, del **contesto** e delle **finalità del trattamento**, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**

↓

il **titolare** del trattamento e il **responsabile** del trattamento **mettono in atto misure tecniche e organizzative adeguate** per **garantire** un **livello di sicurezza adeguato al rischio**

14. MISURE DI SICUREZZA

Sicurezza del trattamento (art. 32)

Le misure comprendono

- la **pseudonimizzazione** e la **cifratura** dei dati personali
- la **capacità di assicurare** su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi** di trattamento
- la **capacità di ripristinare** tempestivamente la **disponibilità** e l'**accesso** dei **dati personali** in caso **di incidente fisico o tec**nico
- una **procedura per testare**, **verificare** e **valutare** regolarmente l'**efficacia delle misure tecniche** e **organizzative** al fine di **garantire la sicurezza del trattamento**

14. MISURE DI SICUREZZA

Sicurezza del trattamento (art. 32)

17. IL NUOVO SISTEMA SANZIONATORIO

fino a 10 milioni di euro,
o per le imprese, fino al 2 % del fatturato

↓

per la violazione degli:

• obblighi del titolare del trattamento e del responsabile del trattamento connessi:
- al consenso dei minori;
- ai trattamenti senza identificazione dell'interessato;
- ai principi di *accountability*, Privacy by design e by default, al Joint Controller, ai responsabili del trattamento, alla tenuta di un registro del trattamento;
- al trasferimento dei dati all'estero;

• obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

• obblighi dell'organismo di controllo a norma dell'articolo 41.4.

fino a 20 milioni di euro,
o per le imprese, fino al 4 % del fatturato

↓

per la violazione:

• dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

• dei diritti degli interessati a norma degli articoli da 12 a 22;

• dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

• di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (artt. da 85 a 91);

• ovvero per 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 o il negato accesso.

Grazie per la vostra attenzione!

Rag. Mario Desantis

innovare
futuro semplice

FEDERPRIVACY