UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2021-14/

COME E QUANDO SI VERIFICA LA VIOLAZIONE DELLA SICUREZZA DEI DATI (DATA BREACH)

di Massimiliano Mancini (massimiliano.mancini-privacy@hotmail.com)[a]

ABSTRACT: *A quali condizioni e con quali modalità si verificano le violazioni della sicurezza dei dati personali, da quelle finalizzate alle truffe finanziarie a quelli accidentali, tra gli atti criminali informatici e gli errori umani che spesso si sommano, nell'analisi dei principali casi di data breach nella vita quotidiana dei privati e delle aziende.*

KEYWORDS: #databreach #violazionedatipersonali #privacy #GDPR #malware #phishing #hacking #pretexting #ransomware #hacking #ramscraping #trattamentoillecitodatipersonali #hacker #accessoillecito #accessoillecitoaisistemiinformatici #MassimilianoMancini #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana.

INDICE

IL DATA BREACH

È una violazione della sicurezza dei dati che comporta, per ragioni accidentali o per comportamenti illeciti [art.4 p.12 GDPR[1]]:

- la distruzione;
- la perdita;
- la modifica;
- la divulgazione non autorizzata;
- l'accesso ai dati personali trasmessi, conservati o comunque trattati
- il blocco della disponibilità dei dati.

La violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali, ossia qualsiasi informazione riguardante persone fisiche identificate o identificabili, definite dalla normativa come "interessati" [art.4 p.1 GDPR[2]].

Tipici casi di data breach[3]:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;

---

[a] *Segretario Generale UPLI, criminologo, già comandante dirigente di Polizia Locale e Provinciale, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.*

[1] Reg. UE/2016/679 GDPR, art.4 p.12 "*1. Ai fini del presente regolamento s'intende per: [1] «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*".

[2] Reg. UE/2016/679 GDPR, art.4 p.12 "*1. Ai fini del presente regolamento s'intende per: …omissis… [12] La «violazione dei dati personali»: 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;*".

[3] Casi esposti sul sito del Garante per la protezione dei dati personali: https://servizi.gpdp.it/databreach/s/self-assessment.

- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ransomware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

LE TIPOLOGIE DI VIOLAZIONI DEI DATI NEL DETTAGLIO

Le principali violazioni alla sicurezza dei dati che possono dar luogo a data breach sono:

- HACKING: in questi casi l'accesso abusivo è conseguenza di un comportamento doloso di criminali che accedono abusivamente ai sistemi informatici. Gli hacker possono rubare le credenziali di accesso ai sistemi con diversi sistemi: possono trovarle scritte in chiaro accanto il terminale, nelle rubriche, oppure si utilizzano dei software per la generazione automatica di password, impresa semplice se le password sono . Effettuato l'accesso, gli hacker possono poi raccogliere tutte le informazioni che vogliono, lanciare altri attacchi ai sistemi aziendali.

- MALWARE: sono uno strumento tipico dei cyber criminali che possono essere utilizzati per numerose attività illecite, dalla diffusione di virus distruttivi, all'apertura di backdoors che permettono accessi illeciti dall'esterno, al furto di dati personali. Un esempio di malware è il cosiddetto RAM Scraper, che scansiona la memoria dei dispositivi digitali per raccogliere informazioni sensibili, utilizzati, tra l'altro, per scandagliare i POS per prelevare i dati delle carte di credito. Un'altra forma di software malevolo sono i cosiddetti ransomware, che bloccano i dispositivi elettronici e interi sistemi aziendali che gli hacker sbloccheranno solo dietro pagamento di un riscatto (dall'inglese "ransom").

- ERRORE UMANO: è uno dei casi più frequenti e sebbene meno temuto. L'errore di un impiegato che sbaglia ad inviare una mail, l'errata condivisione di singoli file o di intere directory, lasciare fogli stampati con informazioni personali nella stampante di rete, può determinare colposamente gravi violazioni delle informazioni oppure favorire comportamenti dolosi, ad esempio condividendo le password di acceso ai sistemi informatici o alle email.

- SOCIAL ENGINEERING: sono le attività illecite come il phishing, che è l'invio di email che sembrano all'apparenza identiche a quelle di aziende di credito, come ad esempio le Poste o istituti bancari, che richiedendo agli utenti di ripristinare i dati del proprio account, o altre volte fingendo di essere gestori di email, inviano i destinatari su siti contraffatti che acquisiscono così le informazioni personali e i loro dati di accesso che consentono di accedere alle caselle email o, addirittura, ai conti correnti e alle carte prepagate. Il pretexting è un'attività simile, ma condotta al telefono.

- ACCESSI ILLECITI DEI DIPENDENTI: nelle aziende, spesso alcuni utenti hanno la possibilità di accedere ai dati dei propri colleghi e sottoposti, perché magari hanno un account con accesso privilegiato o superiore o per errate politiche di privacy policies (regole di sicurezza per la protezione dei dati personali). Questo può causare data breach accidentali o volontari.

- AZIONI FISICHE: le violazioni dei dati personali possono avvenire anche offline, come nel caso delle clonazioni delle carte di credito che può avvenire in un bancomat o in POS manipolati da criminali.

L'INCIDENZA DEI VARI CASI

Verizone Communications, l'azienda statunitense leader nelle connessioni a banda larga e nelle telecomunicazioni, nel suo Rapporto sulla sicurezza globale del 2020 [2020 Data Breach Investigations Report[4]], ha studiato e quantificato la ripartizione delle cause dei data breach che possono anche sommarsi:

1. hacking: 45% ;
2. errore umano: 22%;
3. social engineering: 22%;
4. malware: 17%;
5. accessi illeciti dei dipendenti: 8%;
6. azioni fisiche: 6%.

[4] Fonte dati: https://enterprise.verizon.com/en-gb/resources/reports/dbir/.