DATA BREACH

COSA SONO E COME GESTIRLI

AGID CERT-PA

Le pillole di sicurezza

Chi siamo

Il CERT-PA è una struttura che opera all'interno dell'Agenzia per l'Italia Digitale (AGID) ed è preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni.

Contattaci

Se sei una PA accreditata puoi contattarci:
AGID CERT-PA

Email: cert-pa@cert-pa.it

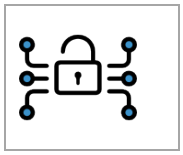
Web: www.cert-pa.it

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA

INDICE

I NOSTRI SERVIZI

ANALISI E INDIRIZZO



Supporto alla definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica

SERVIZI PROATTIVI

Raccolta e elaborazione di dati significativi ai fini della sicurezza cibernetica, emanazione di bollettini e segnalazioni di sicurezza, implementazione e gestione di basi dati informative

SERVIZI REATTIVI

Gestione degli allarmi di sicurezza e supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA

FORMAZIONE E COMUNICAZIONE

Promozione della cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni

COS'È UN DATA BREACH?

Un Data Breach è un incidente di sicurezza che ha come conseguenza la diffusione, la distruzione, la perdita o la modifica non autorizzate di dati confidenziali come indirizzi, numeri di telefono o e-mail, username e password, dati bancari o numeri di carte di credito, PIN e così via. Tali violazioni possono avvenire durante la conservazione, la trasmissione o, più in generale, qualunque trattamento effettuato sui dati stessi.

COS'È IL GDPR?

Il regolamento UE n. 2016/679, detto anche GDPR (in inglese General Data Protection Regulation, in italiano regolamento generale sulla protezione dei dati) è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, riconosciuta come diritto fondamentale dell'individuo, adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno. Essendo un regolamento è immediatamente operativo in tutti i paesi membri a partire dal 25 maggio 2018.

Il testo ha come oggetto la protezione dei dati personali (intesi come qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica) dei residenti nel territorio della UE nei confronti di trattamenti ovunque e comunque effettuati anche da soggetti, cosiddetti Titolari, anche con sede legale fuori dall'Unione Europea. L'obiettivo è quello di semplificare, armonizzare e unificare il contesto normativo sulla privacy per garantire la libera circolazione dei dati personali tra Stati membri. In Italia, in particolare, ha abrogato il codice per la protezione dei dati personali (d. lgs. n. 196/2003). Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico.

Nell'ambito del Regolamento, un **dato personale** è definito come qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).

Inoltre, un **trattamento** è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

CHE FIGURE SONO PREVISTE DAL GDPR?

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro. Nel caso dell'Italia il Garante della Privacy

Interessato: una persona fisica identificata o identificabile; 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

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro

organismo che tratta dati personali per conto del titolare del trattamento Interessato

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento

Data Protection Officer (DPO) persona fisica, nominata dal titolare o dal responsabile del trattamento, ha competenze specifiche in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi allo scopo di osservare, valutare e gestire il trattamento dei dati personali in ottemperanza alle normative. E' inoltre punto di contatto nei confronti delle autorità.

PERCHE AVVENGONO I DATA BREACH?

Un Data Breach può avvenire per motivi volontari o involontari. Ad esempio:

- **perdita accidentale**: data breach causato ad esempio da smarrimento di una chiavetta USB con contenuti riservati;
- **furto**: data breach causato ad esempio da furto di un notebook con all'interno dati confidenziali/riservati;
- **infedeltà aziendale**: data breach causato ad esempio da un dipendente/persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia da distribuire in ambiente pubblico;
- **accesso abusivo**: data breach causato ad esempio da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

COSA FARE PER PREVENIRE I DATA BREACH?

La prevenzione dei data breach passa attraverso la predisposizione di opportune contromisure. In linea di massima, il punto di partenza è sempre quello di fare un'analisi del Rischio. Partendo da ciò che si fa e dal perché lo si fa, cioè di fatto mission e funzioni, si passa a analizzare come lo si fa, e quindi processi e servizi, e cosa occorre per farlo, cioè gli asset. I dati sono tra questi ultimi. Fatto questo, si passa a analizzare le minacce agli asset, ad esempio incendi, terremoti, malware, hacker, furti ecc, e le vulnerabilità che permettono a queste minacce di operare. I Rischi così individuati possono essere mitigati attraverso opportune contromisure. Nel seguito vedremo alcune di esse:

1. **obblighi legali** – la privacy e la sicurezza dei dati sono affrontate in leggi specifiche, come ad esempio il GDPR, ma anche in leggi e regolamenti specifici per un determinato ambito come il caso dei dati sanitari o dei dati giudiziari. Seguire le prescrizioni relative e gli aggiornamenti evita di esporsi a problemi giudiziari o multe. Inoltre, in caso di violazione

dei dati, il rispetto delle normative è la prima cosa che viene controllata.

2. **Policy di sicurezza dei dati** – è il documento principale che deve essere prodotto e a cui deve sottostare l'ente nel suo complesso. Esso dettaglia le best practice, gli standard e le procedure che devono essere seguiti per massimizzare la sicurezza dei dati. Deve riguardare la conservazione dei dati, sia fisici che digitali, il loro trasporto, le modalità di accesso (CRUD – Create, Read, Update, Delete), le responsabilità e così via
3. **Policy per l'utilizzo degli apparati aziendali** – in questo documento vengono affrontate tutte le problematiche relative all'utilizzo degli strumenti che un ente mette a disposizione dei suoi dipendenti e consulenti. E' lecito portare a casa un computer portatile? E possibile usarlo a fini privati? Che complessità devono avere le credenziali di accesso? Cosa deve essere fatto quando un computer, portato temporaneamente all'esterno dell'ente vi rientra? Deve essere definita una procedura di quarantena? E' possibile scaricare software? Cosa fare quando un dipendente lascia l'ente?
4. **Autorizzazione degli utenti** – gli utenti devono ricevere solo i privilegi strettamente necessari per le operazioni che devono compiere. Inoltre i privilegi non dovrebbero mai essere attribuiti direttamente agli utenti ma dovrebbero seguire paradigmi come RBAC (Role Based Access Control), cioè gli utenti dovrebbero, sulla base dei loro ruoli aziendali, essere aggregati in gruppi e i privilegi dovrebbero essere attribuiti a questi ultimi. Anche i gruppi dovrebbero essere strutturati in modo da ricevere solo i privilegi strettamente necessari
5. **Automatizzazione** – è stato valutato che l'errore umano è il primo responsabile dei data breaches ed è normalmente il prodotto di una bassa cultura della sicurezza, di una gestione inaccurata, negligente e incontrollata dei dati, dell'utilizzo ad esempio di password deboli e così via. Automatizzare i processi laddove possibile permette di far lavorare le persone in modo controllato e standardizzato. Inoltre, l'adozione di controlli automatici permette di prevenire e contrastare l'errore umano prima ancora che si verifichi il problema come, ad esempio, il controllo automatizzato della complessità delle password o l'uso di configurazioni dei sistemi operativi che impediscano l'installazione di software non approvato dall'ente.
6. **Promozione di consapevolezza della sicurezza** – le persone sono la prima linea di difesa se opportunamente educate e formate
7. **Uso della criptazione laddove possibile** – criptare i dati, stazionari e in movimento, con meccanismi di complessità adeguata è un ottimo modo per affrontare il problema dell'integrità e dell'accesso ai dati
8. **Tracciamento e Monitoraggio** – l'accesso ai dati e tutte le funzioni eseguite su essi devono essere tracciati in tempo reale e i log prodotti devono essere conservati con tutta la cura possibile per il tempo richiesto dalla legge e dai regolamenti interni. Oltre alle verifiche in tempo reale devono essere fatti periodicamente Audit da parte di consulenti esterni.
9. **Backup dei dati** – il backup dei dati permette il ripristino nel caso di eventi distruttivi. La frequenza dei backup, i tempi di conservazione dei backup, la scelta dei supporti dei backup e la loro modalità di conservazione devono tutti essere scelti in modo compatibile all'importanza dei dati e all'analisi del rischio effettuata in precedenza. Attenzione al fatto, ovviamente, che la qualità di un backup dipende dalla qualità del dato di partenza: se quest'ultimo era già corrotto anche il backup presenterà lo stesso problema

10. **Gestione delle patch** – l'adeguamento di software e sistemi operativi via via che vengono individuate nuove vulnerabilità deve essere fatto con la massima priorità possibile, soprattutto nel caso di patch di sicurezza ma non essere precipitoso in tutti gli altri casi. Prima di installare una patch devono sempre essere effettuati i backup e le patch devono sempre essere provate in un ambiente di test prima dell'installazione in ambiente di produzione.

COSA È UN DATA BREACH RESPONSE PLAN?

Nel momento in cui si verifica un incidente, o data breach, è importante muoversi in maniera coordinata e precisa, sulla base di responsabilità chiare e preventivamente definite, in modo da evitare di agire in modo potenzialmente nocivo in preda al panico. Un Data Breach Response Plan è un insieme di procedure e risorse che vengono messe in atto in occasione di un incidente allo scopo di:

1. Rispondere all'emergenza e evitare ulteriori danni. In questa fase occorrerà raccogliere le informazioni sull'incidente, documentare tutto insieme a data e ora di accadimento, agire per priorità sulla base dell'analisi del rischio, comunicare con tutti gli Stakeholder diffondendo le informazioni necessarie, mettere in sicurezza le aree coinvolte e allertare se necessario le autorità
2. Investigare le cause, preservando le evidenze in caso di un'ulteriore prosecuzione giudiziaria.
3. Ripristinare i sistemi compromessi

Una volta creato il Piano, esso andrà periodicamente verificato tramite opportuno audit.

COS'È UNA DATA BREACH POLICY?

La Data Breach Policy è un documento in cui l'ente, sulla base della propria mission e dei dati trattati, rende nota la procedura da seguire per assicurare un approccio efficace e consistente alla gestione dei data breach e agli incidenti di sicurezza. L'obiettivo della policy deve essere quello di minimizzare il rischio associato con il breach e delineare le azioni da compiere per ridurre le perdite e ripristinare velocemente la normale operatività. Essa deve dichiarare prima di tutto a chi è applicabile (ad esempio, se l'ente è un'università, allo staff, agli studenti, ai consulenti e ai fornitori).

Tra gli argomenti che devono sicuramente comparire ci sono: 1) i ruoli e le responsabilità, eventualmente con le indicazioni dell'orario di lavoro delle varie figure coinvolte e delle modalità di contatto (telefono, e-mail ecc.) 2) le informazioni da raccogliere per dettagliare il breach (data e ora, nome di chi compila il rapporto, natura dell'informazione coinvolta e la sua sensibilità, descrizione dell'evento, impatto su cose e persone, estensione) 3) procedure disciplinari o impatto giudiziario, quando applicabile, nel caso di cattivo comportamento accertato 4) modalità di contenimento e ripristino 5) contromisure in essere 6) modalità di comunicazione verso l'interno dell'ente, le autorità, la stampa e eventuali terzi coinvolti) 7) modalità di revisione della policy (ogni quanto tempo deve essere effettuata e con quale iter) 8) template del report da compilare nel caso di data breach

COSA FARE IN CASO DI UN DATA BREACH?

Nel caso in cui ci si dovesse accorgere di essere stati vittima di un data breach la prima cosa da fare è quella di non farsi prendere dal panico e agire in modo scomposto ma, anzi, applicare subito le procedure previste dalla policy. Relativamente al punto 6 della domanda precedente e cioè all'aspetto della comunicazione, il GDPR prevede espressamente l'obbligo di notifica da parte del Titolare qualora si sia in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati. In particolare, l'art. 33 impone al titolare di notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza, e cioè nel momento in cui ha ragionevole certezza dell'avvenuto data breach. L'eventuale dolo da parte del Titolare verrà valutato a posteriori qualora emerga dall'indagine la carenza di contromisure appropriate. L'obbligo di notifica tempestiva impegna anche il responsabile nei confronti del Titolare, il quale verrà considerato a conoscenza nel momento in cui sarà avvenuta tale comunicazione. La notifica deve almeno (art. 33 GDPR):

a) 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;

b) 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;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) 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.

L'Autorità di controllo a cui fare la notifica (via PEC all'indirizzo: protocollo@pec.gpdp.it) del data breach ha carattere nazionale. Nel caso dell'Italia è il Garante per la protezione dei dati personali (Garante Privacy). Qualora un'ente operi in più paesi e sia quindi potenzialmente sotto la giurisdizione di più autorità il GDPR ha introdotto il **principio dello sportello unico** (*one stop shop*) che è l'autorità di controllo del paese dove si trova la sede principale e che coopererà con le altre in caso di data breach con impatto transfrontaliero. Qualora, invece, l'impatto sia locale, l'autorità di riferimento sarà quella del paese ove avviene il trattamento che è stato oggetto di data breach.

Oltre alla comunicazione della violazione all'autorità di controllo, il Titolare dovrà anche provvedere a dare comunicazione senza ingiustificato ritardo al diretto interessato qualora il data breach sia suscettibile di presentare un rischio elevato per i diritti e le libertà

delle persone fisiche.

DOVE TROVARE I RISULTATI DI UN DATA BREACH?

Nel caso di furto di dati personali e/o sensibili gli autori del fatto, se si esclude un utilizzo diretto, possono decidere o di metterli in vendita sul mercato nero (verosimilmente il cosiddetto Dark Web) o di pubblicarli in chiaro, a fine dimostrativi, su siti spesso usati a questo fine come https://ghostbin.com/ o https://pastebin.com/ magari annunciandone la presenza su social network come Twitter.

Un altro posto dove ad esempio cercare se la nostra account e-mail è stata hackerata è "Have I been pwned?" https://haveibeenpwned.com/

Qui di seguito alcuni articoli online sul prezzo dei dati personali sul mercato nero:

https://privacyaustralia.net/dark-web-personal-data/

https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-us-edition/

https://www.roccobalzama.it/dark-web-market-price-index-quanto-vale-la-nostra-identita-digitale-nel-dark-web/

COSA FA IL CERT-PA IN CASO DI DATA BREACH?

In relazione alla raccolta e all'elaborazione di dati significativi ai fini della sicurezza cibernetica e in conformità con le regole tecniche per la sicurezza informatica delle PA, CERT-PA eroga, per le sole amministrazioni accreditate, uno specifico servizio proattivo che prevede la notifica ai diretti interessati qualora venga rilevata l'esposizione di informazioni. Quest'ultima consiste nella diffusione non autorizzata di dati di varia natura che si riferiscono a realtà della Pubblica Amministrazione. In particolare, in quasi tutti i casi, viene rilevata la combinazione di accesso (di solito la coppia username/password) al servizio oggetto di data breach. Tali dati possono essere successivamente utilizzati da utenti malintenzionati ed è pertanto necessario analizzare prontamente le informazioni contenute dandone tempestiva notifica ai diretti interessati così da attivare, per tempo, le contromisure possibili a seconda del caso.

A partire dalla fine del 2017 il CERT-PA ha attivato uno specifico servizio che è oggi suddiviso nelle seguenti quattro fasi:

- il **monitoraggio**, demandato ad un software proprietario che è in grado di rilevare su più canali, per lo più OSINT, la presenza di informazioni inerenti un possibile "data breach" e quindi notificare agli analisti del CERT-PA i termini della pubblicazione delle stesse;

- il **recupero delle informazioni**, attività manuale che viene svolta direttamente dall'analista del CERT che

sceglie anche lo strumento\canale più idoneo a seconda della dimensione, natura, ubicazione o servizio che ospita i dati da scaricare;

- l'**elaborazione**, operazione automatizzata svolta da un software proprietario che si occupa di individuare se nel blocco di dati individuato vi sono informazioni che riguardano enti appartenenti alla constituency del CERT-PA. L'elaborazione implica anche l'estrazione e il salvataggio delle informazioni in relazione alla specifica PA rilevata nei dati esfiltrati;

- la **segnalazione**, che può essere automatizzata o manuale a seconda della necessità e rappresenta la fase conclusiva del ciclo di lavorazione dove l'utente specifico (Referente PA) viene informato dell'esposizione di informazioni della Struttura o Ente di appartenenza.

Il servizio appena descritto è fondamentale ai fini della sicurezza cibernetica dei singoli enti accreditati. Per tale ragione è stato progressivamente potenziato nel corso del tempo sia con l'obiettivo di ridurre i tempi di reazione che di gestire moli importanti di dati non strutturati e disomogenei.

Autore
Alessandro Sinibaldi, senior security expert CERT-PA
Graphic designer
Daniela De Blasis, visual designer, UX/UI designer at AgID

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA