UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

L'amministratore di sistema secondo il Provvedimento del Garante per la Protezione dei Dati Personali del 27.11.2008

Mara Beccaceci

BiMind S.r.l.

m.beccaceci@bimind.it

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Contesto storico

- Sapevi che il 61% delle violazioni riguarda le credenziali?
- Gli hacker riescono spesso ad ottenere l'accesso alle reti aziendali trafugando le credenziali degli utenti o quelle degli amministratori, causando così incidenti di sicurezza e falle di conformità

Chi è l'amministratore di sistema?

- Provvedimento Garante: «Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008, modificato con provvedimento del 25 giugno 2009
- **amministratore di sistema** «figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi».

- Non rientrano nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi *software*.
- Sono esclusi dall´ambito applicativo del provvedimento i Servizi svolti per ordinarie finalità amministrativo-contabili

Nomina: interna o esterna

- Persona fisica o giuridica
- Identificazione e censimento
- estremi identificativi degli amministratori di sistema e l´elenco delle funzioni loro attribuite
- Definizione ambito di operatività sistema amministrato
- 1 sistema può avere 1 o + amministratori
- 1 amministratore può amministrare 1 sistema o + sistemi
- Utenze privilegiate: accessi o poteri speciali ben oltre quelli garantiti ad un utente standard. Gli accessi privilegiati consentono alle organizzazioni di proteggere la propria infrastruttura e le proprie applicazioni e di operare con efficienza, mantenendo comunque la riservatezza dei dati sensibili e dell'infrastruttura critica. Gli accessi privilegiati possono essere associati a utenti sia umani che non umani, come le applicazioni e le identità di macchina.

Ruolo privacy dell'amministratore di sistema

- Dipendente dell'organizzazione: ruolo di autorizzato al trattamento
- Collaboratore esterno: ruolo di Responsabile del trattamento *ex* art. 28 GDPR

Obblighi del Titolare

- Prima della nomina:
- Valutazione requisiti soggettivi: **esperienza**, **capacità**, e **affidabilità,** in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza
- Dopo la nomina:
- Relazione almeno annuale per verificare la rispondenza dell´operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali
- Tra le verifiche,
- Log di accesso:

- Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell´evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Obblighi del Titolare – datore di lavoro

- Importante: i dipendenti devono conoscere il nominativo dell'amministratore del sistema che tratta i loro dati personali
- Es: smarcatempo digitale
- *«…Qualora l´attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l´identità degli amministratori di sistema nell´ambito delle proprie organizzazioni, secondo le caratteristiche dell´azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti..»*

Controlli del Garante

- Provvedimento del Garante del 2.12.2021
- Al **Responsabile esterno** (software house) perché *«…Nel corso dell'istruttoria è emerso altresì che, al momento della violazione, l'accesso al software XXXX da parte del radiologo era effettuato con un'utenza di tipo amministrativo (admin) e password non robusta (admin)…»*
- Al **Titolare** perché «*…si è resa responsabile della mancata adozione di misure tecniche e organizzative adeguate a garantire la riservatezza e l'integrità dei dati personali trattati mediante il software XXXXX, in violazione degli artt. 5, par.1, lett. f) e 32 del Regolamento…*»

Profili penali

- **accesso abusivo** ad un sistema informatico o telematico (art. 615 *ter* Codice penale);
- **danneggiamento** di sistemi informatici e telematici (art. 635 *bis* Codice penale);
- **danneggiamento** di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* Codice penale);
- **danneggiamento** di sistemi informatici o telematici (art. 635 *quater* Codice penale);
- **danneggiamento** di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* Codice penale);
- **frode informatica** (art. 640 *ter* Codice penale).
- Reati ai sensi della D.Lgs. 231/01

Quid juris: utenza privilegiata non umana

- **Esempi:**
- **Account di applicazione:** si tratta di un account privilegiato specifico del software applicativo, che viene tipicamente utilizzato per amministrare, configurare o gestire l'accesso al software applicativo stesso.
- **Account di servizio:** si tratta di un account che viene utilizzato da un'applicazione o da un servizio per interagire col sistema operativo. I servizi utilizzano questi account per accedere ed apportare modifiche al sistema operativo o alla configurazione
- **Chiave SSH:** (come descritto sopra). Le chiavi SSH vengono inoltre utilizzate dai processi automatizzati.
- **Segreto:** spesso utilizzato dal team DevOps come termine onnicomprensivo per designare le chiavi SSH, le chiavi API (Application Program Interface) e le altre credenziali utilizzate da tali team per garantire l'accesso privilegiato.

Sfugge alla normativa, dal momento in cui non c'è una persona fisica che la gestisce e costituisce una vulnerabilità per la sicurezza dei sistemi.

Conclusioni

- La nomina di amministratori di sistema contribuisce al **rispetto dei princìpi fondamentali** in materia di protezione dei dati personali che ogni organizzazione è tenuta ad osservare (**art. 5 GDPR)**;
- L'amministratore di sistema ha il compito di **sviluppare le misure** cosiddette **di "*privacy by design e privacy by default*"** (**art. 25 GDPR**), quali ambiti di operatività rispetto ai quali può svolgere un ruolo non secondario di progettazione e di innovazione dei processi organizzativi;
- La nomina di un amministratore di sistema rappresenta senza dubbio per il titolare del trattamento un elemento di "***accountability***" ai sensi dell'art. **24 GDPR**;
- La presenza di amministratori di sistema costituisce senza dubbio un'attuazione concreta dell'**adozione di misure di sicurezza adeguate al rischio** di cui all'**art. 32 GDPR**;