DISCIPLINARE TECNICO DESIGNAZIONE AMMINISTRATORI DI SISTEMA

Sommario

1. PREMESSA E OBIETTIVI

Il presente disciplinare tecnico descrive la procedura di designazione degli Amministratori di Sistema e le misure da applicare per garantire la sicurezza dei dati e delle informazioni trattate.

Ai fini del presente Disciplinare, per Amministratori di Sistema si intendono le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali o di sue componenti (Amministratori di Dominio e di Server), nonché ogni altra figura equiparabile dal punto di vista dei rischi relativi alla protezione dei dati (Amministratori di Base Dati, Amministratori di Reti e di Apparati di Sicurezza, Amministratori di Sistemi Software complessi[1])

2. AMBITO D'APPLICAZIONE

Il presente disciplinare si applica a tutti gli Amministratori di Sistema che operano sui servizi sistemistici, infrastrutturali e applicativi che afferiscono al sistema informatico dell'Ente. A causa della interconnettività e della interdipendenza fra le componenti di un sistema informativo, i problemi di sicurezza su una sola di esse propagano i loro effetti incidendo gravemente sulla sicurezza del sistema nel suo complesso. Per tale motivo, la presente disciplina è recepita da tutte le organizzazioni che utilizzano il sistema informativo dell'Ente.

3. PROCEDURA DI DESIGNAZIONE DEGLI AMMINISTRATORI DI SISTEMA

Le designazioni sono effettuate dal Direttore in quanto RTD.

Il Responsabile del Servizio gestione documentale, segreteria Organi, transizione digitale e comunicazione cura la tenuta dell'elenco

La lettera di designazione per i dipendenti dell'Ente è trasmessa per conoscenza anche alla struttura competente in materia di Gestione del Personale ai fini dell'aggiornamento del curriculum dei dipendenti.

3.1 Amministratore di Sistema interno

Per Amministratore di Sistema "interno" si intende il personale alle dirette dipendenze dell'Ente a cui sono attribuite funzioni di Amministratore di Sistema.

---

[1] Definizione da provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" pubblicato sulla G.U. n. 300 del 24-12-2008

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale deve, quindi, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza (cfr. par. 2 lett. a) del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

Tale valutazione è effettuata dal Direttore.

A ciascuna singola persona fisica cui siano attribuite funzioni di Amministratore di Sistema viene inviata una lettera di incarico, con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Qualora fosse necessario integrare le funzioni di un Amministratore di Sistema interno già designato, occorre effettuare una lettera di integrazione dell'incarico.

3.2 Amministratori di Sistema di società esterne

3.2.1 Amministratori di Sistema designati dall'Ente

Nei casi in cui il personale alle dipendenze di società esterne svolga funzioni di Amministratore di Sistema presso il Data Center dell'Ente, è il Direttore che effettua la designazione su richiesta del Responsabile del Servizio gestione documentale, segreteria Organi, transizione digitale e comunicazione.

La valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare deve essere effettuata dalla società esterna di appartenenza, a mezzo di formale attestazione.

La società deve essere preventivamente designata quale Responsabile del relativo trattamento.

A ciascuna singola persona fisica, cui siano attribuite funzioni di Amministratore di Sistema, deve essere inviata una lettera di incarico, con l'elencazione degli ambiti di operatività in funzione dei profili autorizzativi assegnati.

Qualora fosse necessario integrare le funzioni di un Amministratore di Sistema interno già designato, occorre effettuare una lettera di integrazione dell'incarico.

3.2.2 Amministratori di Sistema designati da un Fornitore

Nei casi non disciplinati dal paragrafo precedente (ad esempio nei casi di fruizione di applicativi con modalità SaaS) la designazione degli Amministratori di Sistema è effettuata direttamente dai Fornitori, già nominati Responsabili del trattamento per i servizi affidati, i quali hanno l'obbligo di

conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'attività di Amministratori di Sistema.

Tale onere deve essere espressamente indicato nella designazione del Fornitore quale Responsabile del trattamento dei dati personali, ai sensi e per gli effetti di cui all'art. 28 del Regolamento UE 2016/679.

3.2.3 Amministratori di Sistema delle "postazioni di lavoro"

Tutti gli utenti che possiedono privilegi di amministrazione di postazione/i di lavoro, devono essere designati Amministratori di Sistema. La richiesta segue la procedura di cui al par. 3.2.1., integrata con precise e circostanziate motivazioni. Il Responsabile del Servizio gestione documentale, segreteria Organi, transizione digitale e comunicazione valuta se le esigenze poste alla base della richiesta possono essere esaudite anche senza la concessione dei privilegi di amministrazione della postazione di lavoro.

4. REGISTRO DIGITALE DEGLI AMMINISTRATORI DI SISTEMA

La norma dispone che sia mantenuto costantemente e tempestivamente aggiornato un elenco nominativo degli Amministratori di Sistema e che per ciascuno degli amministratori designati sia specificato l'ambito di operatività in funzione dei profili autorizzativi assegnati.

Il Registro degli Amministratori di Sistema contiene le seguenti macro categorie:

- Amministratori di Dominio: si tratta degli amministratori del dominio che consente all'accesso alle risorse e ai servizi informativi dell'Ente.
- Amministratori di Server: si tratta degli utenti che hanno diritti amministrativi su uno o più server; a titolo esemplificativo rientrano in questa categoria gli utenti appartenenti al gruppo "Administrators" di uno o più server Windows o gli utenti di uno o più server Linux che attraverso il comando "sudo" possono impersonare l'utente "root".
- Amministratori di Base Dati: si tratta degli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di "Data Definition Language".
- Amministratori di Apparati di Rete: si tratta degli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni.
- Amministratori di Apparati di Sicurezza: si tratta degli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus.

- Amministratori di Postazioni di Lavoro individuale: si tratta degli utenti che hanno privilegi di amministrazione della PdL.
- Amministratori di Sistemi Software complessi: si tratta degli utenti con privilegi di amministrazione di software applicativi o infrastrutturali che contengono diverse componenti hardware e software che interagiscono tra loro; esempi di sistemi software complessi sono i sistemi ERP, i sistemi di data warehouse, i sistemi di posta elettronica e i sistemi middleware.

L'identità degli Amministratori di Sistema la cui attività riguarda procedure che determinano il trattamento di dati personali di lavoratori dipendenti, deve essere condivisa dal Titolare del trattamento (Datore di Lavoro) con il contesto organizzativo di riferimento (es. inserendo i nominativi di tali soggetti nelle informative rivolte ai dipendenti, oppure attraverso la pubblicazione sui canali di comunicazione interna come la intranet aziendale, regolamenti aziendali e disciplinari tecnici, ecc.).

Il Responsabile del Servizio gestione documentale, segreteria Organi, transizione digitale e comunicazione crea e mantiene aggiornato il Registro degli Amministratori di Sistema, individuando gli strumenti tecnologici più idonei per la gestione, la conservazione e l'aggiornamento.

Le funzioni di amministrazione di sistema effettuate dai soggetti indicati al par. 3.2.2 non comportano obblighi di inserimento nel Registro degli Amministratori di Sistema.

5. SISTEMA DI ACCESS LOG

La normativa dispone che sia tenuta traccia degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo 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 di tempo, non inferiore a sei mesi.

1) A tale scopo è predisposto un sistema centralizzato di raccolta dei log dei sistemi, che garantisce le caratteristiche di completezza e inalterabilità richieste. Il sistema centralizzato di gestione dei log (log management) raccoglie i log di tutti gli accessi logici degli utenti (Amministratori di Sistema e non) dei sistemi sui quali siano stati designati Amministratori di Sistema e per i quali la tracciatura degli accessi sia tecnicamente possibile. Tale sistema è utilizzato inoltre per raccogliere e gestire i log di sicurezza di tutti i differenti sistemi che fanno parte del sistema informatico dell'Ente.

Tale funzione è svolta dal Responsabile del Servizio gestione documentale, segreteria Organi, transizione digitale e comunicazione. Ogni qualvolta venga attivato un sistema su cui è necessario

autorizzare le funzioni di Amministratore di Sistema, occorre concordare con la suddetta struttura le modalità di integrazione ai fini della raccolta dei log. Allo stesso modo, una volta che il sistema viene dismesso, deve esserne comunicata la dismissione.

6. VERIFICA ANNUALE DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA

La normativa dispone che l´operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Titolari del trattamento o dei Responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Il Direttore verifica annualmente la corretta designazione degli Amministratori di Sistema e la sussistenza dei requisiti di capacità e di affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Inoltre, i log di cui al precedente paragrafo sono analizzati al fine di verificare elementi di anomalia che possano far emergere criticità in termini di riservatezza, integrità e disponibilità delle informazioni.

7. INVENTARIO DEI DISPOSITIVI E DEL SOFTWARE AUTORIZZATI

7.1 Inventario dei dispositivi autorizzati

Al fine di prevenire e rilevare attacchi che utilizzano dispositivi non gestiti dall'Ente connessi alla rete interna, occorre che tutti i dispositivi presenti sulla rete interna siano gestiti in maniera attiva, mantenendo un inventario aggiornato di tutte le categorie di dispositivi autorizzati.

Tale registro costituisce strumento di ausilio all'Ente nella comprensione delle relazioni tra le componenti censite e la loro configurazione e rappresenta un componente fondamentale nei processi di change management.

Si tratta di una misura fondamentale e strategica per il buon governo dell'infrastruttura e, al fine di garantire un elevato livello qualitativo del sistema, è fondamentale assicurare un costante aggiornamento delle informazioni in esso contenute.

7.2 Inventario del software autorizzato

Alcune categorie di attacchi, sfruttando una o più vulnerabilità, prevedono l'installazione di software malevolo sulle macchine di un'organizzazione, che in questo modo possono diventare punto di raccolta di informazioni sensibili o punto di partenza per effettuare movimenti laterali verso altri

obiettivi all'interno della rete dell'organizzazione. Le organizzazioni che non hanno un inventario del software autorizzato hanno più difficoltà nell'individuare i sistemi che sono stati compromessi.

A tal fine occorre che tutto il software presente sulla rete interna sia gestito in maniera attiva, mantenendo un inventario aggiornato del software autorizzato.

8. USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORI

L'uso non corretto dei privilegi amministrativi è uno dei metodi principali usato dagli attaccanti per espandersi all'interno di un'organizzazione attaccata. Una prima tecnica è quella di far eseguire un codice malevolo ad utenti che hanno privilegi amministrativi, aumentando notevolmente l'efficacia dell'attacco. Una seconda tecnica è quella di elevare i privilegi indovinando o carpendo la password di un utente amministratore. Se i privilegi amministrativi sono largamente distribuiti o se le stesse password sono utilizzate su più sistemi, l'attaccante può ottenere più facilmente l'accesso completo ai sistemi target.

Per tali motivi è importante che i privilegi amministrativi vengano utilizzati solo quando serve e che le credenziali degli Amministratori di Sistema siano protette in maniera particolare. Gli Amministratori di Sistema sono perciò tenuti ad osservare le seguenti misure:

- prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso;
- tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa;
- generare un 'allerta quando viene aggiunta una utenza amministrativa;
- generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa;
- utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi. Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri);
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
- tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona;

- le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l’imputabilità di chi ne fa uso;
- evitare l’uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio);
- conservare le credenziali amministrative in modo da garantire disponibilità e riservatezza;
- se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette;
- le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative: non scadono dopo un periodo di inutilizzo, non vengono bloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche di modifica manuale delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato;
- le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l’accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all’ambito per cui sono state create;
- le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via email: in tali casi, è necessario convocare l’utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio di informazioni sicuro;
- le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati.

8.1 Sospensione dei privilegi

Nel caso in cui sia accertato che il comportamento di un Amministratore di Sistema doloso o gravemente negligente ed in palese contrasto con le policy di sicurezza dell’Ente sia causa diretta o indiretta di incidente di sicurezza, i privilegi informatici ad esso assegnati sono sospesi fintantoché le cause e le responsabilità effettive dell’incidente non siano state appurate a conclusione del procedimento per l'accertamento di una eventuale responsabilità disciplinare.