Capital Security Srls

Come predisporre correttamente un bando, un contratto o una nomina per Amministratore di Sistema

Aspetti contrattuali, giuridici, economici, tecnologici, organizzativi, di sicurezza e conformità al GDPR ed al Provvedimento del Garante per la protezione dei dati personali del 27/11/2008 e alla Circolare AGID 2/2017

Corso online tenuto in data 28/11/2022

Relatore: Dott. Giancarlo Favero - Direttore

Capital Security Srls
Via Montenapoleone 8 – 20121 Milano
Via Scarlatti, 7 – 20124 Milano

www.capitalsecurity.it

Comunicazioni di Servizio

- L’evento sarà registrato
- Per richiedere gli attestati di partecipazione mandare una mail ad

amministrazione@capitalsecurity.it

specificando Istituto di appartenenza (compresa la città) ed elenco dei partecipanti (nome e cognome)

Capital Security Srls
Via Montenapoleone, 8
Milano

La radice (e la soluzione) del problema:

AMMINISTRATORE DI SISTEMA

- AMMINISTRATORE DI **SISTEMI**, poiché in una Scuola ci sono centinaia di sistemi, completamente differenti
- **AMMINISTRATORI** DI SISTEMI, poiché essendoci centinaia di sistemi completamente differenti, potremmo avere più di un amministratore di sistema

Capital Security Srls
Via Montenapoleone, 8
Milano

Capiamo bene che cos'è un «Sistema»: Esempi di sistemi

- PC, PC Portatile, server, database server, server di videosorveglianza, telecamere, stampanti, sistemi per la rilevazione delle presenze

- Firewall, router, switch, access point Wi-FI, controller di access point Wi-Fi, piattaforme di monitoraggio e system management

- Registro elettronico, segreteria digitale, protocollo informatico, sito web, posta elettronica, Gsuite for Education, Microsoft Teams, tutte le piattaforme in cloud utilizzate, tutti i programmi in locale installati

IN UNA SCUOLA CI SONO CENTINAIA DI SISTEMI, COMPLETAMENTE DIFFERENTI

Capital Security Srls
Via Montenapoleone, 8
Milano

Vediamo come si possono classificare i vari sistemi

- Sistemi in cloud vs sistemi installati in locale («on premises»)
- Sistemi applicativi vs. sistemi operativi
- Sistemi per le (tele) comunicazioni: router, firewall, switch
- Sistemi fisici tangibili (es. un PC o una stampante) vs. sistemi software (es. registro elettronico)
- Sistemi mission critical (es. un firewall) vs. sistemi non mission critical (es. un PC della didattica)
- Sistemi facili da amministrare vs. sistemi difficili da amministrare

Capital Security Srls
Via Montenapoleone, 8
Milano

Alcuni punti chiave da tenere presenti

- I sistemi migliori sono quelli che non devono essere amministrati
- I sistemi in cloud sono di norma molto semplici da amministrare
- Il Piano Triennale per l'Informatica nella Pubblica Amministrazione, il principio di efficienza, efficacia ed economicità e l'AGID dicono «CLOUD FIRST»
- «CLOUD FIRST» significa …. «CLOUD FIRST»!!!
- Significa che l'acquisto di un server deve essere giustificato, e prima devono essere valutare le opzioni in cloud (es. Microsoft Azure, Google Workspace, Microsoft Office 365, AWS – Amazon Web Services etc.)
- Significa che deve essere fatta o richiesta una valutazione comparativa, anche da un punto di vista economico, dell'opzione «in locale» vs. l'opzione in cloud

Capital Security Srls
Via Montenapoleone, 8
Milano

Alcuni punti chiave da tenere presenti

- Spesso le opzioni «in locale» si portano dietro dei costi e dei rischi non indifferenti: vediamo il caso di un server
- Bisogna avere lo spazio fisico, l'armadio rack, un locale dedicato etc.: alcune Scuole hanno subito il **FURTO DEL SERVER**
- Costi aggiuntivi: costo dell'antivirus sul server, costo del backup, costo del NAS dove fare il backup, costo del gruppo di continuità
- Costi aggiuntivi: costi dell'aggiornamento del sistema operativo, costo delle analisi di vulnerabilità, costo dell'installazione degli aggiornamenti di sicurezza
- Tutti questi costi ed i rischi connessi, che possono arrivare a migliaia di euro, si azzerano o si riducono notevolmente se si sceglie l'opzione in cloud

Capital Security Srls
Via Montenapoleone, 8
Milano

Chi è l «Amministratore di Sistema» ?

- «Amministratore di sistema» è chi effettua operazioni su un sistema hardware e/o software con profilo di «administrator» o equivalente («admin», «root», «supervisor» etc.)
- Può essere un soggetto interno o esterno alla Scuola
- In ogni caso, anche in caso di affidamento ad una ditta esterna, l'AdS deve essere riconducibile ad una persona fisica ben identificata
- Es.: il router con indirizzo 192.168.1.1 è amministrato dal Sig. Mario Rossi che utilizza l'account «admin» per effettuare le operazioni di amministrazione di sistema

Capital Security Srls
Via Montenapoleone, 8
Milano

Tipologie/fasi di amministrazione di sistema

Vi sono varie tipologie di amministrazione di sistema, che corrispondono al ciclo di vita del sistema

- Operazioni di AdS «una tantum», che tipicamente vengono effettuate in fase di prima installazione e configurazione del sistema: es. Vodafone o subcontractor o altra ditta che installa e configura il Wi-Fi e la rete cablata

- Operazioni di «ordinaria amministrazione» su un sistema già installato e configurato: verifica delle performance, verifica che il backup funzioni, verifica del livello di occupazione dello spazio su disco, etc.

- Operazioni di «pronto intervento» su un sistema già funzionante ed in esercizio: es. guasto o malfunzionamento su un sistema mission critical, come il Firewall o il router per l'accesso ad internet, guasto del server della Segreteria, guasto del sistema di rilevazione delle presenze, indisponibilità del Registro elettronico e della Segreteria digitale

Capital Security Srls
Via Montenapoleone, 8
Milano

Tipologie/fasi di amministrazione di sistema

Vi sono varie tipologie di amministrazione di sistema, che corrispondono al ciclo di vita del sistema, e che richiedono tempi di intervento e di risoluzione del problema completamente differenti

- Operazioni di AdS «una tantum», che tipicamente vengono effettuate in fase di prima installazione e configurazione del sistema: es. Vodafone o subcontractor o altra ditta che installa e configura il Wi-Fi e la rete cablata: tempi di intervento che coincidono con i tempi di installazione e rilascio al collaudo del sistema

- Operazioni di «ordinaria amministrazione» su un sistema già installato e configurato: verifica delle performance, verifica che il backup funzioni, verifica del livello di occupazione dello spazio su disco, etc.: tempi di intervento che possono essere pianificati, ed essere comunque dell'ordine di giorni o settimane

- Operazioni di «pronto intervento» su un sistema già funzionante ed in esercizio: es. guasto o malfunzionamento su un sistema mission critical, come il Firewall o il router per l'accesso ad internet, guasto del server della Segreteria, guasto del sistema di rilevazione delle presenze, indisponibilità del Registro elettronico e della Segreteria digitale: tempi di intervento e risoluzione che devono essere praticamente immediati o molto contenuti

Capital Security Srls
Via Montenapoleone, 8
Milano

Introduciamo un concetto importante: i livelli di servizio

- Livelli di Servizio, detti anche SLA, che significa Service Level Agreement
- Gli SLA sono i tempi entro i quali l'AdS (sia interno che esterno) deve intervenire e risolvere il problema
- I tempi di intervento e di risoluzione del problema devono essere ovviamente commisuranti a quanto mission critical è il sistema, e possono variare da qualche ora a qualche giorno
- Il mancato rispetto degli SLA deve comportare il pagamento di penali, che devono essere esplicitate
- Ovviamente ci deve essere qualcuno che controlla i livelli di servizio: SLM – Service Level Monitorin

Capital Security Srls
Via Montenapoleone, 8
Milano

Chi è l «Amministratore di Sistema» ?

- Qualcuno deve «valutare» l'Amministratore di Sistema: 4.1. Valutazione delle caratteristiche soggettive.
- L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacita' e dell'affidabilita' 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.
- L'amministratore di sistema può vedere tutto e modificare, cancellare, falsificare i dati, quindi può compiere una serie di reati ed abusi non indifferente (es. trasmissione «Report» di Milena Gabanelli)

Capital Security Srls
Via Montenapoleone, 8
Milano

Bisogna controllare l’operato degli AdS

- 4.4. Verifica delle attivita'.
- L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attivita' di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Capital Security Srls
Via Montenapoleone, 8
Milano

Bisogna controllare l’operato degli AdS

- 4.5. Registrazione degli accessi.
- Devono essere adottati sistemi idonei alla registrazione 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, inalterabilita' e possibilita' di verifica della loro integrita' 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.

Capital Security Srls
Via Montenapoleone, 8
Milano

Errori frequenti:

1. Non specificare chiaramente i sistemi che dovranno essere amministrati
2. Non prevedere l'obbligo di fornite all'Ente la mappa dei sistemi
3. Non prevedere l'obbligo di fornire all'ente l'inventario dei sistemi installati e/o configurati
4. Non prevedere l'obbligo di fornire all'Ente l'elenco delle password di sistema di ciascun sistema
5. Non prevedere il livelli di servizio, cioè gli SLA
6. Non prevedere penali in caso di mancato rispetto degli SLA

Capital Security Srls
Via Montenapoleone, 8
Milano

Errori frequenti:

7. Non essere in grado di passare immediatamente da un AdS (sia interno che estero) ad un altro
8. Non richiedere la dichiarazione di aver verificato l'idoneità e l'affidabilità degli ADS
9. Non verificare la completezza e la correttezza della documentazione fornita
10. Diventare «ostaggio» del fornitore
11. Non richiedere il salvataggio delle configurazioni dei sistemi
12. Non verificare (o far verificare) l'operato degli AdS

Capital Security Srls
Via Montenapoleone, 8
Milano

Clausole/contenuti che non devono mai mancare:

1. Specificare chiaramente i sistemi o le tipologie di sistemi
2. Richiedere esplicitamente la mappa del sistema informativo
3. Richiedere la consegna delle password di administrator
4. Prevedere esplicitamente gli SLA
5. Prevedere le penali in caso di mancato rispetto degli SLA
6. Richiedere l'elenco nominativo individuale degli AdS e dei sistemi amministrati
7. Richiedere la dichiarazione sulla idoneità ed affidabilità degli AdS

Capital Security Srls
Via Montenapoleone, 8
Milano

Clausole/contenuti che non devono mai mancare:

8. Richiedere la dichiarazione di conformità dei sistemi e degli interventi effettuati al GDPR

9. Richiedere esplicitamente l'elenco dei sub-responsabili del trattamento dei dati

10. Verificare se i sistemi hanno attivato un meccanismo di logging (tracciatura) degli accessi con profilo di administrator

Capital Security Srls
Via Montenapoleone, 8
Milano

Grazie per l'attenzione

Relatore Dott. Giancarlo Favero

Tel. 02-94750267 Cell. 335-5950674

mail giancarlo.favero@capitalsecurity.it

amministrazione@capitalsecurity.it

www.capitalsecurity.it

Capital Security Srls
Via Montenapoleone, 8
Milano