POLITECNICO
MILANO 1863

Area Servizi ICT
Yuri CORIO

CODAU: GdL «MISURE MINIME DI SICUREZZA ICT PER LE PA»

Agenda

- Inquadramento normativo
- Panoramica Misure Minime Sicurezza
- Gruppo di lavoro CODAU
- Chiarimenti forniti da AgID

MMS-PA - Inquadramento generale 1/2

- Le misure minime di sicurezza ICT per le pubbliche amministrazioni costituiscono una parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

- Sono state emesse in attuazione alla direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici e costituiscono un'anticipazione urgente della regolamentazione completa in corso di emanazione

- Consistono in un insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica ed organizzativa, predisposto da AgID per fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento

MMS-PA - Inquadramento generale 2/2

- Il documento con le MMS-PA è stato finalizzato nell'aprile del 2016 al termine di un processo di sviluppo che ha compreso anche una estesa consultazione con alcune Pubbliche Amministrazioni di riferimento e con i componenti del Nucleo Sicurezza Cibernetica (NSC). AgID e CERT-PA nel settembre 2016 hanno pubblicato il documento sui rispettivi siti web.

- Ogni PA dovrà individuare al suo interno eventuali sottoinsieme tecnici e/o organizzativi caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi

MMS-PA: ABSC (AgID Basic Security Controls)

- I controlli individuati da AgID sono basati sui 20 CIS Critical Security Control (CCSC) pubblicati dal Center for Internet Security (CIS) noti anche come «SANS 20»
- I CCSC sono largamente diffusi ed utilizzati, e pongono una particolare attenzione ai costi che l'implementazione di una misura minima richiede rispetto ai benefici che è in grado di offrire
- Nell'identificazione dei ABSC si fa riferimento alla versione 6 dei CCSC di ottobre 2015
- L'insieme dei controlli individuati da AgID è più vicino alla versione 5.1 dei CCSC, che presenta caratteristiche ancora attuali nel contesto della PA italiana
- Le MMS-PA pongono l'accento sugli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino

ABSC: 8 classi di controlli (1/3)

ABSC 1: Inventario dei dispositivi autorizzati e non autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC 2: Inventario dei software autorizzati e non autorizzati

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC 3: Proteggere le configurazioni hardware e software sui dispositivi mobili, laptop, workstation e server

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC: 8 classi di controlli (2/3)

ABSC 4: Valutazione e correzione continua delle vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC 5: Uso appropriato dei privilegi di amministrazione

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC 8: Difese contro i malware

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC: 8 classi di controlli (3/3)

ABSC 10: Copie di sicurezza

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC 13: Protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC: livelli di sicurezza

Livello ***minimo***: livello sotto al quale nessuna PA può scendere

=> controlli strettamente obbligatori ai quali ogni PA, indipendentemente dalla sua natura e dimensione, deve essere conforme in termini tecnologici, organizzativi e procedurali.

Livello ***standard***: base di riferimento per la maggior parte delle PA

=> controlli che costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione

Livello ***alto***: obiettivo a cui tendere per tutte le PA

=> controlli adeguati alle organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati

MMS-PA: Circolare AgID ed allegati 1/2

Circolare AgID del 18/04/17 n. 2/2017:

- Ha l'obiettivo di indicare alle PA le misure minime per la sicurezza ICT da adottare al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri
- Individua i destinatari della circolare, ovvero i soggetti di cui all'art. 2, comma 2 del C.A.D.
- Individua il responsabile dell'attuazione delle misure minime, ovvero il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., o in sua assenza, il dirigente allo scopo designato
- L'allegato 1 contiene le MMS-PA
- L'allegato 2 contiene il modulo di implementazione delle MMS-PA, da compilare con una descrizione sintetica delle modalità di implementazione delle MMS-PA

MMS-PA: Circolare AgID ed allegati 2/2

- Il modulo di implementazione deve essere firmato digitalmente dal responsabile dell'attuazione delle MMS-PA e dal rappresentante legale della struttura e conservato dalla PA stessa, salvo inviarlo al CERT-PA in caso di incidenti

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati	

- La circolare stabilisce il termine ultimo entro il quale la PA dovranno attuare gli adempimenti indicati => **31.12.2017**

Gruppo di lavoro CODAU MMS-PA

In considerazione delle peculiarità che caratterizzano gli Atenei e delle possibili criticità di applicazione di quanto richiesto da AgID, è stato costituito un gruppo di lavoro in ambito CODAU con l'obiettivo di raccogliere quesiti e proposte da sottoporre all'attenzione di AgID

- ***27/04 ⇨ costituzione gruppo di lavoro CODAU***
  - 9 università (Bicocca, Insubria, Milano, Pavia, PoliMI, PoliTO, Trento, Verona)
  - 30 componenti (dirigenti, esperti di networking & security, gestione sistemi / data center, gestione client, gestione database
- ***03/05 ⇨ avvio lavori e predisposizione documentazione condivisa***
  - Documento excel con la mappatura delle Misure Minime raggruppate per ABSC e filtrabili per livello di applicazione
  - Documento word per raccogliere i quesiti da sottoporre ad AgID
  - Folder di lavoro con la documentazione di riferimento indicata da AgID

Gruppo di lavoro CODAU MMS-PA

- **30/05 ⇨ *condivisione quesiti con referenti ICT degli Atenei***
- ***13/06 ⇨ incontro con AgID (dott. Terranova)***
  - Presentazione dei quesiti individuati
  - Raccolta osservazioni e chiarimenti
- ***22/06 ⇨ condivisione con GDL dei contenuti dell'incontro con AgID***
- ***12/07 ⇨ documento di sintesi dei contenuti dell'incontro con AgID***

Incontro con AgID: ambito di applicazione MMS-PA

Gli atenei non gestiscono direttamente tutte le risorse che possono essere attive in rete (es. notebook e smartphone degli studenti). L'accesso alla rete di tali dispositivi non è ad oggi soggetto ad approvazione mentre lo è l'utente che accede alla rete. Come ci si può regolare per rispondere ai requisiti AgID?

Il perimetro da considerare per la definizione dell'ambito di interesse e la valutazione delle corrispondenti misure minime non è definito in termini assoluti; è infatti necessaria un'analisi della specifica realtà in esame che consideri le sue peculiarità ed il contesto di riferimento nel quale è inserita per individuare una partizione ("segregazione stratificata") dei sistemi e della rete, articolandone opportunamente i domini di sicurezza. In tale stratificazione la parte centrale ("core") costituisce la zona di massima criticità, per la quale va assolutamente garantito il rispetto di tutte le misure di sicurezza necessarie per impedirne la compromissione, sia da parte di azioni esterne che interne.

Incontro con AgID: Responsabilità attuazione MMS-PA (1/2)

Circolare AgID Art. 3. - Attuazione delle misure minime

Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle misure minime di cui all'art. 1.

Incontro con AgID: Responsabilità attuazione MMS-PA (2/2)

In mancanza del responsabile designato ai sensi dell'Art.17 del CAD e dell'incarico esplicito ad un dirigente, chi ha la responsabilità dell'attuazione delle misure minime?

La responsabilità complessiva per l'Ateneo è in capo al rappresentante legale ovvero al Rettore. Tuttavia, stante l'articolazione organizzativa degli Atenei, in essi sono tipicamente presenti strutture dotate di ampia autonomia, che si estende anche alla definizione, implementazione ed erogazione di servizi. In considerazione di ciò, la responsabilità di applicazione delle misure minime va, per tali strutture, ascritta al Responsabile della struttura stessa, tipicamente il Direttore di Dipartimento. In taluni casi, legati all'utilizzo di dispositivi e postazioni sotto il totale controllo dei singoli utenti (es. docenti e ricercatori) la responsabilità diretta potrebbe essere ascritta ad essi.

Incontro con AgID: ABSC 1

[1.1.1]
Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
[1.4.1]
Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

Differenza tra inventario del punto 1.1.1 e 1.4.1 e set minimo di informazioni contenute in entrambi.

L'inventario del punto 1.1.1 include tutte le risorse attive sulla rete. L'inventario del punto 1.4.1 include le risorse attive e autorizzate.
L'inventario deve contenere almeno l'indirizzo IP, informazione che potrebbe costituire un dato personale, con specifici vincoli di trattamento, laddove consentisse l'identificazione della singola persona.
L'inventario delle risorse attive deve essere dettagliato in funzione della distanza dal "core" identificato come zona di massima criticità per la sicurezza delle informazioni.

Incontro con AgID: ABSC 2

[2.1.1]
Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.

Cosa si intende per «software»?

L'obiettivo è conoscere il software attivo sulla rete, in rapporto al contesto considerato.

In particolare è necessario:

- *redigere un inventario dei software installati su tutti i dispositivi di proprietà dell'ente*
- *impedire che gli utenti possano modificare le configurazioni standard evitando di fornire loro credenziali amministrative;*

Incontro con AgID: ABSC 2

- *stabilire e descrivere tutti i casi in cui sono ammesse deroghe (mobile smartphone e notebook di proprietà dell'Ente ma usati soprattutto al di fuori della rete di Ateneo). Nel caso di utenti amministratori è necessario predisporre procedure e modalità di utilizzo dei dispostivi conformi al livello di sicurezza dell'ente.*

Le eccezioni non devono in ogni caso violare le policy definite dal GARR:

https://www.garr.it/it/regole-di-utilizzo-della-rete-aup

Incontro con AgID: ABSC 3

[3.1.1]
Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.

Cosa si intende per «configurazione sicura standard»?

Ci si propone di identificare una configurazione ottimale rispetto ai fabbisogni ed al livello di sicurezza da garantire.

È necessario individuare policy, procedure e configurazioni sicure differenziate per tipo di dispositivo connesso e per contesto di utilizzo e prevedere in particolare le necessarie verifiche di funzionalità per l'aggiornamento dei pacchetti software autorizzati (ad es. la retrocompatibilità degli stessi)

Incontro con AgID: ABSC 4

[4.1.1]

Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.

E' necessario dotarsi di un software che internamente permetta di verificare le vulnerabilità dei sistemi e degli applicativi. (es. Nessus installato su una macchina interna)

Incontro con AgID: ABSC 4

[4.5.1]

Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.

Il termine "automaticamente" fa riferimento alla necessità che gli aggiornamenti siano gestiti da amministratori di sistema, evitando che possa/debba farsene carico l'utente finale.

Il rilascio deve essere testato in opportuni ambienti di prova.

Le eccezioni devono essere documentate.

Incontro con AgID: ABSC 4

[4.8.1]

Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).

Il modello del piano di gestione dei rischi deve essere adatto al contesto e gestibile.

Il piano deve prendere in considerazione anche i servizi dell'Ente erogati direttamente o indirettamente tramite fornitori.

Incontro con AgID: ABSC 4

In particolare la contrattualistica di acquisizione di moduli sw e/o di servizi dovrà esplicitamente prevedere da parte del fornitore il rispetto delle misure minime di sicurezza sia con riferimento ai moduli applicativi che alle componenti di sistema che costituiscono l'environment necessario alla loro esecuzione (Web/Application/Database server, CMS, sistema operativo, …).

Gli aspetti contrattuali andranno adattati alle situazioni specifiche, con prevedibili differenze nel caso di installazione on premise rispetto all'erogazione dei servizi in hosting o in cloud.

Incontro con AgID: ABSC 5

[5.1.1]

Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

Gli utenti finali non possono essere amministratori dei loro dispositivi?

È necessario:

- *definire e rispettare il workflow di gestione del ciclo di vita ed autorizzazione delle utenze amministrative.*
- *impedire (limitare il più possibile) gli attacchi che potrebbero sfruttare gli elevati privilegi associati a queste utenze (i principali attacchi, quelli con elevato costo di ripristino, fanno uso dei privilegi di amministratore).*

Incontro con AgID: ABSC 5

[5.2.1]

Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.

E' necessario identificare gli amministratori di sistema in modo chiaro, come richiesto dal GDPR, definendo contestualmente i registri dei trattamenti e l'analisi di rischio privacy sui dati trattati.

Incontro con AgID: ABSC 8

[8.9.3]

Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

Come definire quali sono le tipologie "strettamente necessarie" soprattutto nell'ambito della ricerca?

Ciò che non è possibile controllare o gestire deve essere confinato per evitare che possa arrecare danni, soprattutto ai servizi presenti all'interno della zona identificata come core.

Incontro con AgID: ABSC 13

[13.1.1]

Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica

Rispetto al GDPR la richiesta ha una valenza più ampia, comprendendo nel perimetro anche informazioni per le quali valgano requisiti di riservatezza pur non riguardando dati personali (es tutela diritti copyright, NDA, ecc).

Q & A

Grazie per l’attenzione