UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA

Corso di Laurea triennale in Ingegneria Informatica e dell'Automazione

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

MINIMAL ICT SECURITY MEASURES FOR PUBLIC ADMINISTRATIONS

Relatore:
Prof. Ennio Gambi

Correlatore:
Dott. Silvio Fabi

Tesi di Laurea di:
Davide Di Massimo

A.A. 2019 / 2020

Sommario

PREMESSA

Il preoccupante aumento degli eventi cibernetici e, in particolare, quelli a carico della pubblica amministrazione ha spinto il Presidente del Consiglio dei ministri ad emanare, il 1° agosto 2015, una direttiva. Quest'ultima, in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, il quale raccordi le capacità di risposta delle singole amministrazioni con l'obiettivo di assicurare la capacità dell'infrastruttura informatica nazionale di far fronte ad incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi, mira a sollecitare tutte le amministrazioni e gli organi delegati a dotarsi di standard minimi di prevenzione e reazione in risposta ad eventi cibernetici.

Al fine di agevolare tale processo l'Agenzia per l'Italia digitale (AgID) si è occupata di redigere indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

AGENZIA PER L'ITALIA DIGITALE

L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio, che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

L'AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese, e di sostenere l'innovazione digitale e promuovere la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali.

La struttura incorpora ed eredita le competenze precedentemente assegnate all'Agenzia per la diffusione delle tecnologie per l'innovazione, DigitPA e il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri.
Secondo lo Statuto approvato a Febbraio 2014, le finalità dell'Agenzia per l'Italia digitale sono:

- Assicurare il coordinamento informatico delle amministrazioni statale, regionale e locale, con la finalità di progettare e monitorare l'evoluzione strategica del sistema informativo della pubblica amministrazione, favorendo l'adozione di infrastrutture e standard che riducano i costi sostenuti dalle singole amministrazioni e migliorino i servizi erogati;
- Accreditare i soggetti certificatori in ambito digitale (certificato digitale, SPID, conservazione sostitutiva, ecc.);
- Perseguire l'ottimizzazione della spesa in materia informatica delle pubbliche amministrazioni attraverso il monitoraggio della relativa spesa corrente e il supporto alle amministrazioni pubbliche nazionali e locali nel raggiungimento di obiettivi di standardizzazione e revisione dei processi interni e di ottimizzazione della spesa informatica complessiva;
- Svolgere i compiti necessari per l'adempimento degli obblighi internazionali assunti dallo Stato nelle materie di competenza;
- Promuovere l'innovazione digitale nel Paese e contribuire alla creazione di nuove conoscenze ed alla diffusione di nuove opportunità di sviluppo economico, culturale e sociale collaborando con le istituzioni e gli organismi europei, nazionali e regionali aventi finalità analoghe, anche attraverso la stipula di accordi strategici;
- Emanare linee guida, regolamenti e standard;
- Promuovere iniziative di alfabetizzazione informatica per i cittadini.

ABSC – AGID BASIC SECURITY CONTROLS

Per la stesura delle linee guida, l'AgID ha scelto di prendere come base l'insieme dei controlli noti come CIS 20, i quali sono stati definiti dal Center for Internet Security (CIS). Questa scelta trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che tali controlli nascono con una particolare sensibilità verso i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro è in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. È comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le amministrazioni pubbliche.

In realtà nel definire gli AgID Basic Security Control (ABSC) si è partiti dal confronto tra le versioni 6.0 e 5.1 dei CSC (attualmente alla versione 7.1), che può essere assunto quale indicatore dell'evoluzione della minaccia cibernetica nel corso degli ultimi anni. È infatti evidente l'aumento di importanza delle misure relative agli amministratori di sistema, che balzano dal 12° al 5° posto, mentre la sicurezza applicativa scivola dal 6° al 18° posto e gli accessi wireless dal 7° al 15° a causa della diffusione delle contromisure atte a contrastare le vulnerabilità tipiche di tali ambiti.
Per facilitare il confronto con la definizione originale, si è deciso di fare riferimento, nell'identificazione degli ABSC, alla versione 6 dei CSC. Tuttavia, l'insieme dei controlli definiti è più vicino a quello della versione 5.1, poiché, nonostante molti di quelli che nel passaggio alla nuova versione sono stati eliminati, probabilmente perché non più attuali nella realtà statunitense, si ritengono ancora importanti nel contesto della pubblica amministrazione italiana.
Occorre inoltre osservare che i CSC sono stati concepiti essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime cinque classi si è deciso di aggiungere quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfiltrazione.

Ciascun CSC è costituito da una famiglia di misure di dettaglio più fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realtà locale. Nonostante ciò, si è ritenuto che anche al secondo livello ci fosse una granularità ancora eccessiva, in particolar modo sotto il profilo implementativo, che avrebbe costretto soprattutto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione. Per tale ragione è stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente. Pertanto, un ABSC è identificato da un identificatore gerarchico a tre livelli x, y, z, dove x e y sono i numeri che identificano il CSC concettualmente corrispondente e z individua ciascuno dei controlli di livello 3 in cui questo è stato raffinato.

Al primo livello, che corrisponde ad una famiglia di controlli destinati al perseguimento del medesimo obiettivo, è associata una tabella che li contiene tutti:

- Nella prima colonna, "ABSC_ID", sviluppata gerarchicamente su tre livelli, viene definito l'identificatore univoco di ciascuno di essi;
- Nella seconda colonna, "Descrizione", si specifica il controllo attraverso una definizione sintetica;
- Nella terza colonna, "FNSC" (Framework nazionale di sicurezza cibernetica), viene indicato l'identificatore della Subcategory del Framework Core del Framework nazionale per la Cyber Security, proposto con il 2015 Italian Cyber Security Report del CIS «La Sapienza», presentato il 4 febbraio 2016, al quale il controllo è riconducibile.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le ultime tre colonne sono booleane e costituiscono i tre livelli di attuazione che dovrebbero essere implementati per ottenere un determinato livello di sicurezza:

- Minimo (quarta colonna): è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
- Standard (quinta colonna): è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.
- Alto (sesta colonna): deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto, ogni amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, 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.

ABSC 1 (CSC 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_ID			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazioni del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X

		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	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.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X
	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

ABSC 2 (CSC 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 il software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione.

ABSC_ID			Descrizione	FNSC	Min.	Std.	Alto
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'installazione di software non compreso nell'elenco.	ID.AM-2	X	X	X
	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	ID.AM-2		X	X
		2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	ID.AM-2		X	X
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X

	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	ID.AM-2		X	X
		3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ID.AM-2			X
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	ID.AM-2			X

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI 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_ID			Descrizione	FNSC	Min.	Std.	Alto
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X

		2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	PR.IP-1		X	X
		3	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	PR.IP-2 RC.IM-1			X
	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	PR.IP-1	X	X	X
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	PR.IP-3		X	X
	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	PR.DS-2 PR.IP-2		X	X

	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X
	5	1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	PR.DS-6		X	X
		2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	PR.DS-6			X
		3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	PR.IP-3			X
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	PR.IP-3			X
	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	PR.IP-3			X
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	PR.IP-3			X

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

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

ABSC_ID			Descrizione	FNSC	Min.	Std.	Alto
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.	ID.RA-1 DE.CM-8	X	X	X
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	ID.RA-1 DE.CM-8		X	X
		3	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	DE.CM-8			X
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	DE.CM-8		X	X
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	DE.CM-8		X	X
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	DE.CM-8		X	X

	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	DE.CM-8		X	X
		2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	DE.CM-8		X	X
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	DE.CM-8	X	X	X
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	ID.RA-2		X	X
	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	X
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	ID.RA-1 DE.CM-8		X	X
	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	PR.IP-12 RS.MI-3	X	X	X

		2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	PR.IP-12 RS.MI-3		X	X
	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.).	ID.RA-4 ID.RA-5 PR.IP-12	X	X	X
		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X
	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	PR.IP-12 RS.MI-3		X	X
	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	PR.DS-7		X	X

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

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

ABSC_ID			Descrizione	FNSC	Min.	Std.	Alto
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.	PR.AC-4 PR.PT-3	X	X	X

		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PR.AC-4 PR.PT-3	X	X	X
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	PR.AC-4 PR.PT-3		X	X
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	ID.AM-3 DE.AE-1			X
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ID.AM-6 PR.AT-2 DE.CM-3	X	X	X
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	DE.CM-3			X
	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	PR.IP-1	X	X	X
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	PR.PT-1 DE.AE-1 DE.AE-5 DE.CM-1		X	X

	6	1	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.	PR.AC-1 PR.AT-2			X
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	PR.AC-1 PR.AT-2	X	X	X
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	PR.AC-1 PR.AT-2		X	X
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	PR.AC-1 PR.AT-2	X	X	X
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	PR.AC-1		X	X
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	PR.AC-1 PR.AT-2		X	X
	8	1	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	PR.AC-1 PR.AT-2 DE.CM-7		X	X

	9	1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	PR.AT-2 PR.PT-2 PR.PT-3 PR.PT-4		X	X
	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	X
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	ID.AM-6	X	X	X
		3	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.	ID.AM-6 PR.AT-2	X	X	X
		4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	ID.AM-6 PR.AT-2	X	X	X
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AT-2	X	X	X

ABSC 8 (CSC 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_ID			Descrizione	FNSC	Min.	Std.	Alto
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	DE.CM-4 DE.CM-5	X	X	X
		2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	DE.AE-3 DE.CM-1 RS.CO-1 RS.MI-1		X	X
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	PR.IP-3 DE.DP-1		X	X
		2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	PR.IP-3 PR.MA-1 PR.MA-2 DE.CM-4		X	X
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	PR.DS-7 DE.CM-4			X
	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	PR.AC-3 DE.AE-1 DE.CM-7			X

	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	PR.IP-1 RS.MI-1 RS.MI-2		X	X
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	PR.IP-1 RS.MI-1 RS.MI-2			X
	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	DE.CM-1 DE.CM-4		X	X
		2	Installare sistemi di analisi avanzata del software sospetto.	DE.CM-4			X
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	DE.CM-1 DE.CM-4		X	X
	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X
		4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X	X	X

	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X
		2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X
		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).	DE.CM-1 DE.CM-4	X	X	X
	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	DE.CM-1 DE.CM-4		X	X
	11	1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	ID.AM-6 DE.CM-4 RS.CO-5		X	X

ABSC 10 (CSC 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_ID			Descrizione	FNSC	Min.	Std.	Alto
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
		2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono	PR.IP-4			X

			riguardare il sistema operativo, le applicazioni software e la parte dati.				
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

ABSC 13 (CSC 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_ID			Descrizione	FNSC	Min.	Std.	Alto
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	ID.AM-5	X	X	X

	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	ID.AM-5 PR.DS-5		X	X
	3	1	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	ID.AM-3 PR.AC-5 PR.DS-1 DE.AE-1			X
	4	1	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	ID.AM-3 DE.CM-1			X
	5	1	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	PR.PT-2			X
		2	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	ID.AM-1 PR.PT-2			X
	6	1	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	ID.AM-3 DE.CM-1			X
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	ID.AM-3 DE.CM-1			X

	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	ID.AM-3 PR.DS-5 DE.CM-1			X
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.AM-3 PR.DS-5 DE.CM-1	X	X	X
	9	1	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	PR.AC-4 PR.DS-5			X

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA ICT

L'obiettivo dell'elaborato è stato fornire un "Modulo di implementazione delle misure minime di sicurezza per le pubbliche amministrazioni", che consiste in una tabella per ogni ABSC e uno spazio dedicato alla descrizione della modalità di implementazione delle singole misure, al fine di avere un esempio e una base di partenza per l'adeguamento di una pubblica amministrazione alla normativa. Il seguente modulo fornisce un ausilio alla prevenzione e al contrasto di eventuali attacchi cibernetici, ma anche per attività di verifica, controllo e aggiornamento nel tempo, necessari per assicurarne l'efficacia.

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	L'inventario è composto da un foglio Excel, riportando almeno l'indirizzo IP, il MAC Address.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Aggiornamento del foglio Excel di inventario descritto nel punto 1.1.1.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Il foglio Excel dell'inventario viene creato e aggiornato riportando, indirizzo IP, MAC Address, Hostname, Switch e porta al quale è collegato, Rete, Vlan, Utenti ecc.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	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'installazione di software non compreso nell'elenco.	Ad ogni utente viene consegnata una postazione già completa di tutto il software necessario al suo utilizzo. L'utente non ha i permessi di amministratore per poter installare ulteriori software.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Vedere punto 2.1.1.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Gli amministratori disattivano tutto ciò che non è necessario all'utente finale (ad esempio: disattivazione di servizi non necessari, disattivazione di porte di rete non utilizzate), seguendo delle linee guida sulla creazione di configurazioni standard precedentemente redatte. Inclusa l'installazione dei software base necessari.

3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Implementato seguendo le linee guida al punto 3.1.1.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Tramite l'utilizzo di appositi software viene creata un'immagine del sistema operativo con la sua configurazione standard, in modo da poterlo ripristinare in caso di problemi. O si ripercorrono le linee guida al punto 3.1.1.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	L'immagine del sistema operativo viene memorizzata su supporti USB.
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Le operazioni remote vengono effettuate tramite collegamenti SSH, SFTP, VPN, Remote Desktop Protocol.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a	Utilizzo di software come "OpenVAS" per la vulnerabilità dei sistemi e "OWASP ZAP" per la vulnerabilità per le applicazioni web.

				ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Controllo periodico degli aggiornamenti dei software al punto 4.1.1.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti sono automatizzati con la sola eccezione delle macchine server per il quale è previsto un controllo manuale della compatibilità degli aggiornamenti.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	L’aggiornamento è implementato utilizzando procedure off-line con l’ausilio di supporti removibili.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	In seguito ad aggiornamenti saranno eseguite nuove analisi con i software al punto 4.1.1 per la verifica della risoluzione delle vulnerabilità, se queste ultime non possono essere risolte, come in caso di macchine obsolete che non possono essere dismesse, verranno messe in pratica delle contromisure (ad esempio: disconnessione dalla rete, riduzione dei privilegi, lasciare attivi solo i servizi strettamente necessari).

4	8	1	M	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.).	In caso di vulnerabilità o compromissione del sistema verrà ripristinata la configurazione originale dell'apparato. I server esposti sono configurati in una DMZ protetta da un Firewall con filtri ad hoc.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, applicare le patch per le vulnerabilità a partire da quelle più critiche.	Se sono presenti vulnerabilità verranno classificate in diversi livelli di rischio: ALTO: si procederà ad un ripristino della configurazione iniziale. BASSO: si procederà ad una rimozione delle minacce con successiva analisi del sistema per la verifica.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	I privilegi di amministrazione sono concessi ai soli amministratori di sistemi e vengono concessi temporaneamente ad altri utenti solo su richiesta con giusta motivazione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi,	L'accesso ai dispositivi da parte di qualsiasi utente viene registrato dal sistema. Solo gli amministratori di

				registrando ogni accesso effettuato.	sistemi sono autorizzati ad accedere con privilegi di amministrazione dietro reale necessità.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Utilizzo di un registro adeguatamente memorizzato e criptato con tutte le credenziali amministrative e gli utenti associate.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Ad ogni nuovo dispositivo vengono modificate le credenziali di default con quelle previste per l'utente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Per le utenze amministrative vengono utilizzate credenziali a 8 caratteri con l'obbligo di caratteri alfanumerici e caratteri speciali.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Ogni 4 mesi viene richiesto il cambiamento della password alle utenze amministrative.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non possono essere riutilizzate le ultime 3 password.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori,	Gli amministratori di sistemi hanno credenziali per utenze privilegiate e

				alle quali debbono corrispondere credenziali diverse.	credenziali diverse dalle precedenti per utenze standard.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Nel registro delle credenziali ognuna di esse è associata ad una singola persona autorizzata al suo utilizzo.
5	10	3	M	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.	Le utenze amministrative anonime sono utilizzate solo in caso di emergenza.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono memorizzate su supporti adeguati e criptati.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali per l'autenticazione.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus	In tutti i sistemi connessi alla rete sono installati antivirus e antimalware con aggiornamenti automatici.

				locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i dispositivi è attivo il firewall locale.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'utilizzo di dispositivi esterni a quelli necessari per le attività aziendali deve essere approvato e controllato dagli amministratori di sistemi.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili viene disattivata.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'esecuzione automatica dei contenuti dinamici presenti nei file viene disattivata.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il programma di posta installato viene impostato per disattivare tale funzionalità.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Il programma di posta installato viene impostato per disattivare tale funzionalità.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	In ogni sistema l'antivirus è configurato per eseguire una scansione automatica ad ogni connessione di supporti removibili.

8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	I messaggi di posta vengono filtrati da filtri antispam offerti dal client di posta.
8	9	2	M	Filtrare il contenuto del traffico web.	Il contenuto del traffico web viene filtrato dal Firewall.
8	9	3	M	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).	Il programma di posta installato viene impostato per disattivare tale funzionalità.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Dove possibile sono impostati backup automatici giornalieri. Nel caso non sia possibile implementare backup automatici, le copie vengono eseguite manualmente almeno una volta alla settimana. I backup vengono inviati ad un server dedicato.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della	I backup vengono cifrati prima del loro invio al server di backup.

				trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Per i backup automatici il server si occupa di gestire la connessione con la macchina da cui effettuare il backup. Per i backup manuali l'utente deve prima effettuare una connessione manuale al server per poter eseguire il backup.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	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	I dati sono trattati tutti come particolarmente riservati e pertanto cifrati tutti allo stesso modo.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Tramite il firewall vengono limitati servizi e porte a disposizione della navigazione in Internet.

Il modulo deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., o in sua assenza dal Dirigente allo scopo designato, e dal Responsabile Legale della struttura.
Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CSIRT (Computer Security Incident Response Team) (ex CERT-PA) insieme con la segnalazione dell'incidente stesso.

CSIRT - COMPUTER SECURITY INCIDENT RESPONSE TEAM

Il CSIRT italiano è l'istituito presso il **Dipartimento delle Informazioni per la Sicurezza (DIS)** della **Presidenza del Consiglio dei Ministri** ed è composto da un team di esperti in cyber security, che agisce in chiave di prevenzione e tempestiva individuazione delle minacce, di ricezione di notifiche e supporto nella gestione degli incidenti segnalati da soggetti pubblici e privati nazionali.
I compiti di questa istituzione includono:

- Il monitoraggio degli incidenti a livello nazionale;
- L'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- L'intervento in caso di incidente;
- L'analisi dinamica dei rischi e degli incidenti;
- La sensibilizzazione situazionale;
- La partecipazione alla rete dei CSIRT.

Il CSIRT stabilisce relazioni di cooperazione oltre che con le pubbliche amministrazioni anche con il settore privato e con segnalazioni volontarie, in modo da favorire la più ampia diffusione possibile di una consapevole cultura nel campo della cyber security.

CONCLUSIONI

Negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia cibernetica, in particolare per quella che grava sulla pubblica amministrazione e sull'istruzione, che divengono bersaglio di categorie di attaccanti molto pericolose. Questi settori operano spesso con budget ridotti, misure minime di sicurezza, tecnologie obsolete e un ristretto staff IT e sono pertanto vulnerabili ad un'ampia gamma di attacchi (ad esempio: Ransomware).

Le misure preventive devono essere affiancate da efficaci strumenti di rilevazione, in grado di accorciare i tempi tra l'inizio dell'attacco e il momento in cui viene rilevato, in modo da limitare il più possibile i danni.
In quest'ottica diviene dunque fondamentale l'individuazione delle anomalie dei sistemi, per il quale si pone particolare attenzione agli inventari nelle prime due classi di misure (ABSC1, ABSC2), così come per la protezione della configurazione, sulla quale si concentra la terza classe (ABSC3).
La quarta classe (ABSC4), dedicata all'analisi delle vulnerabilità, ha un duplice scopo: conoscere le vulnerabilità dei sistemi, che sono l'elemento fondamentale della scalata ai privilegi la quale permette il successo di un attacco, e permettere, tramite la continua analisi dei sistemi stessi, un più facile rilevamento di alterazioni eventualmente avvenute e quindi sventare un attacco in corso. Il passaggio dal 12° al 5° posto dei CIS 20 motiva l'importanza della quinta classe (ABSC5), rivolta alla gestione degli utenti, in particolare gli amministratori.
La sesta classe (ABSC8) è incentrata sul fatto che i maggiori attacchi prevedono in alcune fasi l'installazione di codice malevolo, la cui individuazione può impedire la riuscita dell'attacco o evidenziarne la presenza.
La settima classe (ABSC10) pone l'attenzione sulle copie di sicurezza, unico strumento in grado di garantire un ripristino dei sistemi dopo un incidente.
Considerando che la sottrazione delle informazioni è l'obiettivo principale degli attacchi più gravi, l'AgID ha scelto come ultima classe (ABSC13) la protezione dei dati.

I vari metodi di implementazione presenti nel modulo sono stati individuati, testati e messi in pratica durante un tirocinio formativo presso l'azienda NBS S.r.l. di San Benedetto del Tronto (AP), sfruttando il reale contesto di privati e pubbliche amministrazioni di interesse sanitario in cui opera.
Evidenziando come l'utilizzo di questo modulo sia efficace per una più facile configurazione e manutenzione di tutto il sistema.
In conclusione, l'utilizzo del "Modulo di implementazione delle misure minime di sicurezza ICT" per le pubbliche amministrazioni, ma anche per tutti i privati che decidano di redigerlo per la loro

attività, può diminuire considerevolmente la vulnerabilità del sistema ad attacchi informatici ed essere d'aiuto per una migliore gestione ed aggiornamento dei sistemi stessi.

Al contempo, il costante monitoraggio della piattaforma CSIRT diviene un buon alleato per le pubbliche amministrazioni nell'aggiornamento sulle ultime vulnerabilità, il che consente di tenere costantemente e tempestivamente sicuro l'intero sistema, e può risultare un valido appoggio a livello nazionale per la risoluzione di attacchi.

BIBLIOGRAFIA

https://www.agid.gov.it/it/agenzia/chi-siamo

https://www.assiteca.it/2020/01/sicurezza-informatica-i-rischi-cyber-da-affrontare-nel-2020/

https://www.cisecurity.org/controls/cis-controls-list/

https://csirt.gov.it/chi-siamo

https://it.wikipedia.org/wiki/Agenzia_per_l%27Italia_digitale

RINGRAZIAMENTI

A conclusione di questo elaborato, desidero ringraziare tutte le persone che hanno contribuito alla mia crescita personale e professionale.

Ringrazio il mio relatore, il Professor Gambi, per i suoi insegnamenti, il suo supporto e per l'opportunità di accrescere il mio curriculum con esperienze internazionali a contatto con importanti aziende del settore tecnologico.

Ringrazio il mio correlatore, il Dottor Fabi, per la sua disponibilità e pazienza nel trasmettermi le sue conoscenze, necessarie per la scrittura di questa tesi e per l'ambito lavorativo.

Ringrazio di cuore la mia famiglia, per avermi sostenuto moralmente ed economicamente in questo percorso, spronandomi sempre ad andare avanti, negli studi come nella vita.

Infine, un ringraziamento particolare va a Maria Grazia, per il supporto e la vicinanza dimostratami in questi anni, incitandomi a non mollare, ripetendomi che sarei arrivato anche io a questo traguardo.