“Misure Minime di Sicurezza ICT per le pubbliche amministrazioni”

Modello semplificato di implementazione per i referenti informatici

su richiesta dei Direttori di Dipartimento

VANNO COMPILATE SOLO LE RIGHE EVIDENZIATE IN VERDE SEGUENDO LA DESCRIZIONE DELLE MODALITA’ DI IMPLEMENTAZIONE

Nome struttura:

Area di appartenenza:

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	Si tratta dell’inventario IPAdmin gestito da Infosapienza per i nodi registrati della rete informatica. Verificare che i responsabili dei nodi siano effettivamente assegnati ai nodi loro corrispondenti e sanare con InfoSapienza eventuali anomalie.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Gli inventari di cui al punto 1.1.1 vengono aggiornati quando nuove risorse attive vengono collegate in rete
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	Vedi punti 1.1.1 e 1.3.1

				IP.	

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.	Predisporre un documento in cui indicare la lista del software usato nel dipartimento, a partire dai sistemi operativi, al software installato sulle postazioni di lavoro ad uso del personale tecnico amministrativo, il software distribuito da CINFO in modalità campus, quello ad uso del personale tecnico amm. e quello in uso nelle biblioteche/laboratori. Occorre condividere un documento all'interno delle struttura in cui inserire il software utilizzato sulle postazione di lavoro, sui server e nei pc di laboratorio (sistema operativi e software installati) presenti all'interno della struttura.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Si effettuano verifiche periodiche sui nodi di competenza

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.	Scrivere un documento che indichi - le configurazioni che effettuate sui sistemi operativi - inserire gli aggiornamenti del sistema operativo in modalità automatica - attivare firewall locale e dell'antivirus (installare AV Kapsersky) - modalità in cui si effettua il backup
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi 3.1.1

3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Vedi 3.1.1
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini dei OS Microsoft (licenze campus) vengono fornite e distribuite da CINFO. Le immagini dei sistemi operativi Linux e relative ISO di appliance vengono reperite direttamente dai siti ufficiali di distribuzioni
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).	Descrivere se viene effettuata assistenza remota da voi o da ditte esterne. In caso affermativo descrivere quali (es. Desktop remoto, SSH, Teamviewer)

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 ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Installare su tutti i pc e server interni di proprietà del dipartimento la soluzione AV Kaspersky fornita da CINFO reperibile su https://campus.uniroma1.it Per la ricerca di vulnerabilità sulle applicazioni si consiglia l'utilizzo delle seguenti soluzioni facilmente reperibili su internet - nessus home version - openvas software opensource
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	vedi 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 limitatamente alle postazione di lavoro. In ambito server (appliance) vengono installate automaticamente solo patch critiche e di sicurezza (security updates)
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.	All'interno dei laboratori informatici e di ricerca non esistono sistemi air-gapped

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.	
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.).	Predisporre un documento in cui elencare quali apparati sono esposti a maggior rischio rispetto ad altri, indicando quali ad alto, quali a medio e quali a basso rischio. Per rischio si intende il tipo di criticità che potrebbe influire sul funzionamento della struttura
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.	Vedi 4.8.1 e 4.1.1

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.	Sulle postazioni di lavoro in uso a laboratori o centri calcolo, laddove possibile, usare solo utenti non amministratori. Evitare di fornire privilegi amministrativi a personale che non abbia necessità operativa di modificare la configurazione
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Sulle postazione di lavoro in uso a laboratori o centri calcolo usare solo utenti non amministratori, e usare i privilegi amministrativi quando è necessario. Laddove possibile registrare gli accessi effettuati dalle utenze amministrative (si tratta di conservare i log file di sistema) amministra Su pc in uso ad utenti limitare l'uso di utenti non amministratori e usare l'account amministratore solo in caso di effettiva necessità. Sulle console di gestione delle stampanti limitare solo agli amministratori dell'accesso come amministratore, eventuale

					creare ulteriori utenti per la gestione con privilegi più bassi laddove il software lo consenta.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Redigere un documento in cui inventariare le utenze amministrative, a chi sono in possesso e su quali dispositivi
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 dispositivo collegato alla rete devono essere sostituite le credenziali di default. Cambiare sempre la password e le credenziali di default sulle stampanti
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).	Questa misura è rispettata dall'adozione della password policy di Sapienza (https://web.uniroma1.it/infosapienza/sites/default/files/passwordpolicy.pdf)
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Sostituire con frequenza periodica le password delle utenze con ruolo amministratore.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Evitare, laddove possibile, di riutilizzare le stesse password
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Gli amministratori di sistema devono usare due utenze una personale e una di tipo amministrativo che rigorosamente dovranno avere password diverse e di diversa complessità.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze amministrative devono essere registrate e riconducibili, in termini di responsabilità, ad una persona fisica
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 non personali (Administrator, admin, root, etc) devo essere usate solo in caso di necessità e/o emergenza. In caso di utilizzo occorre sempre poter risalire e assicurare l'imputabilità di chi ne fa uso.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Predisporre le utenze amministrative su un documento (foglio password) garantendone la riservatezza e consegnarlo al direttore di dipartimento.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Se vengono usati certificati digitali indicare come questi vengono conservati

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 locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Installare l'antivirus Kaspersky fornito da CINFO a tutte le strutture reperibile su https://campus.uniroma1.it
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i dispositivi deve essere attivato il firewall di Windows
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Vedi 8.1.1
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Vedi 8.1.1
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Vedi 8.1.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Vedi 8.1.1. L'interfaccia web di Google Mail non consente l'apertura automatica di messaggi di posta, ne consente la visualizzazione di anteprima , senza esecuzione di codice
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Vedi 8.1.1
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Vedi 8.1.1
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.	Vedi 8.1.1
8	9	2	M	Filtrare il contenuto del traffico web.	Vedi 8.1.1
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).	Vedi 8.1.1

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	Predisporre il salvataggio dei dati delle varie postazioni di lavoro,

				almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	delle configurazioni degli apparati. Potete usare software liberamente scaricabili da internet (es. syncback)oppure usare la piattaforma google GDrive a patto di cifrare il contenuto oppure fare archivi zip/rar con password.
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 trasmissione consente la remotizzazione del backup anche nel cloud.	Vedi 10.1.1
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.	vedi 10.1.1

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	Vedi 10.1.1
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Misura coperta dalla presenza del firewall perimetrale laddove presente. CINFO a seguito di segnalazione del GARR opera un blocco del traffico agenda sul protocollo o sulla porta

Il/La sottoscritto/a _____

matricola n. _____

indirizzo email _____

titolare/responsabile dei seguenti indirizzi IP:

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

7) _____

e titolare/amministratore/responsabile dei seguenti dispositivi:

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

7) _____

Dichiara di essere titolare/responsabile e amministratore delle suddette risorse, ed è, quindi, tenuto a prendere visione delle linee guida AgID inerenti le misure minime di sicurezza (rif. http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni)e a ottemperare alla loro implementazione, tramite la sottoscrizione del modello di implementazione

Luogo e data

_____

Firma

_____