UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

AGID - Misure minime di sicurezza ICT per le pubbliche amministrazioni

Struttura: ___Dipartimento di Scienze Biomediche, Metaboliche e Neuroscienze _____

ABSC	ABSC_ID	Liv		Descrizione	Modalità di implementazione (Suggerimento)	Note
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	1 1 1 M			Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	*Il registro viene implementato e aggiornato periodicamente e verificati tramite scanning degli indirizzi IP dei dispositivi attivi sulla rete per verificare che solamente gli apparati autorizzati transitino/registrazione su Phpipam abbiano accesso alla risorse di rete.*	Gestione della connettività cablata e wireless a cura del SI-RS
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	1 3 1 M			Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	*Ogni nuovo dispositivo del Personale Docente e TA viene registrato su richiesta dell'utilizzatore . In tale contesto vengono registrati tutti i dati relativi del dispositivo compresi i dati dell'utilizzatore su PHPIPAM.*	
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	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.	*Ad ogni dispositivo che si connette alla rete, viene destinato un univoco indirizzo IP, che viene configurato in automatio tramite DHCP bastao sul mac-address.*	
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	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.	*Il Consiglio di Dipartimento, autorizza un elenco di software che saranno installati sui computer sotto la gestione del referente informatico. Il referente, verifica, all'atto dell'attribuzione dell'indirizzo ip che tale elenco sia realmente rispettato. Per le postazioni utente che saranno sotto la supervisione del referente informatico sarà necessario inserire tali postazioni sotto il dominio UNIMORE, o in alternativa creare degli utenti locali (non amministratori di sistema), al fine di permettere l'installazione del software solamente al personale "amministratore di sistema".*	L'elenco dei software autorizzati sarà presente e consultabile sul sito Dipartimentale e sarà aggiornato ogni qualvolta saranno autorizzati nuovi software da parte del Consiglio di Dipaimento.
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	2 3 1 M			Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	*Sui dispositivi sarà installato del software quali fusioninventory o altri secondo le disposizioni del SIRS, che ai collega ad un sistema centralizzato quale ad esempio GLPI così da tenere traccia del software ce vengono installati sui vari calcolatori.*	E' in fase di attivazione il nuovo sistema di gestione del software autorizzato di Ateneo. tramite l'applicativo GLPI,unimore.it
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	3 1 1 M			Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	*I computer postazioni esclusivamente software compatibili alle normative del GDPR, pertanto saranno accettate esclusivamente le versoni dei vari sistemi operativi definite da UNIMORE come sicure.*	Condividere il documento con gli utenti della struttura.
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	3 2 1 M			Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	*I sistemi operativi non conformi alle direttivi non saranno registrati su phpipam e pertanto non utilizzeranno la rete.*	
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	3 2 2 M			Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	*Quando un computer viene compromesso, viene disconnesso fisicamente dalla rete e successivamente il referente informatico provvederà al suo completo ripristino, effettuando, solo se necessario, un accesso al disco tramite altro sistema operativo "pulito" per il salvataggio dei dati ove possibile e successivamente si procede alla sua formattazione.*	
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	3 3 1 M			Le immagini d'installazione devono essere memorizzate offline.	*Le immagini (fornite dal SIA) sono memorizzate in supporti di memorizzazione e messi a disposizione del Dipartimento e conservati dal referente informatico.*	
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	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).	*Al momento le configurazione e i relativi dati vengono memorizzati su dispositivi esterni personali. E' in progetto la creazione di server o l'utilizzo di spazi web di backup.*	
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	*Al momento non è presente alcun sistema automatico di controllo interno anche in considerazione della diversa collocazione dei Docenti su tutte le strutture di UniMORE, pertanto rimane solo il controllo verso l'esterno tramite le firewall gestite dal SIRS.*	
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	4 4 1 M			Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	*A seguito di segnazioni da parte dei SIRS si procede secondo le loro indicazioni*	
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	4 5 1 M			Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	*Al momento della registrazione del dispositivo, sia al sistema operativo che al software presenti vengono attivati gli aggiornamenti automatica.*	
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	*Tali dispositivi non sono sotto la gestione del Dipartimento e tali operazioni sono eseguite dalla Direttore tecnica*	L'inventario è mantenuto dalla DirezioneTecnica
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.	*Al momento non è presente alcun sistema automatico di controllo interno anche in considerazione della diversa collocazione dei Docenti su tutte le strutture di UniMORE, pertanto rimane solo il controllo verso l'esterno tramite le firewall gestite dal SIRS.*	Azione collegata al piano di gestione dei rischi
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	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.).		Azione collegata al piano di gestione dei rischi
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	4 9 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.		Azione collegata al piano di gestione dei rischi
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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 delle aule e dei laboratori vengono creati solo utenti non amministratori.*	Gestione delle identità utente e di dominio a cura del SIA, gruppo gestione identità
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 1 2 M			Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.		
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 2 1 M			Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	*Verrà effettuato un censimento delle utenze con relativi privilegi.*	Condividere il documento con gli utenti della struttura.
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 3 1 M			Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori conformi con quelli delle utenze amministrative in uso.	*Le credenziali di amministratore sono personali dell'amministratore della macchina e sono sotto la propria responsabilità. Visto che la maggior parte dei pc sono ad uso personale (Docenti e PTA), mentre solo le macchine sotto la responsabilità del Dipartimento (aule e laboratori comuni) sono sotto il controllo e la responsabilità del referente informatico.*	E' in via di preparazione un apposito modulo di assunzione di responsabilità che verrà letto e fatto firmare ad ognuno che vuole essere amministratore di sistema, in cui vengono descritte tutte le azioni che l'utente deve fare per rispettare le MMS.
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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).	*Nel caso di pc in dominio dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 7 3 M			Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 7 4 M			Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	*Nel caso di pc in dominio dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 10 1 M			Assicurare la completa distruzione tra utenze privilegiate e non privilegiate degli amministratori, alla quali debbono corrispondere credenziali diverse.	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 10 2 M			Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	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.	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 11 1 M			Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	5 11 2 M			Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	*Nel caso di pc in dominio Unimore questa procedura è automatizzata dal SIA e di posta di Unimore, nel caso invece di computer al di fuori del dominio, tale procedura è sotto la responsabilità dell'amministratore del pc.*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	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.	*Gli utenti del dipartimento di BMN hanno installato l'antivirus Kaspersky*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 1 2 M			Installare su tutti i dispositivi firewall ed IPS personali.	*Attivare un firewall su tutti i dispositivi.*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 3 1 M			Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	*vd. 8.1.1*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 7 1 M			Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	*vd. 8.1.1*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 7 2 M			Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	*vd. 8.1.1*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 7 3 M			Disattivare l'apertura automatica dei messaggi di posta elettronica.	*Email non consente l'apertura automatica dei messaggi, l'anteprima e l'esecuzione di codice.*	Gestione della posta elettronica e dell'antispam a cura del SI-RS, gruppo posta elettronica
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 7 4 M			Disattivare l'anteprima automatica dei contenuti dei file.	*vd. 8.1.1*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 8 1 M			Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	*vd. 8.1.1*	
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	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.	*vd. 8.1.1*	Gestione della posta elettronica e dell'antispam a cura del SI-RS, gruppo posta elettronica
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	8 9 2 M			Filtrare il contenuto del traffico web.	*vd. 8.1.1*	Gestione del filtraggio del traffico web a cura del SI-RS, gruppo rete.
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	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).	*Email blocca allegati pericolosi. Per il traffico web fare riferimento alle blacklist gestite dal SIRS, gruppo rete.*	Gestione della posta elettronica e dell'antispam a cura del SI-RS, gruppo posta elettronica. Gestione del filtraggio del traffico web a cura del SI-RS, gruppo rete.
ABSC 10 (CSC 10): COPIE DI SICUREZZA	10 1 1 M			Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	*nel caso dei dati di Dipartimento questo è gestito tramite il sistemadi Microsoft e il sistema automatizzato di Google*	
ABSC 10 (CSC 10): COPIE DI SICUREZZA	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.	I sistemi Microsoft e Google sono già GDPR compliant e implemnetano già nativamente la cifratura dei back-up dei dati dei propri clienti.	
ABSC 10 (CSC 10): COPIE DI SICUREZZA	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.	La geolocalizzazione delle copie di sicurezza è gestita interamente da Microsoft e Google	
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	13 1 1 M			Effettuare un'analisi dei dati per individuare quali con particolari requisiti di riservatezza (dati rilevanti) e segnalatemele quelli ai quali va applicata la protezione crittografica	sistemi Microsoft e Google sono già GDPR compliant e implemnetano già nativamente la cifratura dei back-up dei dati dei propri clienti.	
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	13 8 1 M			Bloccare il traffico da e verso url presenti in una blacklist	*Fare riferimento alle blacklist gestite dal SIRS, gruppo rete.*	Gestione del filtraggio del traffico web a cura del SI-RS, gruppo rete

Referente

Rubardo Ippazio Antonio

MICHELE ZOLI
07.05.2024
18:56:51
GMT+01:00