



UNIONE MICROPOLIS

Provincia di Pavia

DELIBERAZIONE DELLA GIUNTA DELL'UNIONE

N.43 del 30.12.2017

Oggetto: Approvazione misure minime di sicurezza. (Circolare n.2/2017 del 18.04.2017 dell'Agenzia per l'Italia digitale).

L'anno duemiladiciassette addì trenta del mese di dicembre alle ore 10.30 nella sede comunale di Cervesina, si è riunita la Giunta dell'Unione dei Comuni di Cervesina, Pancarana.

<i>Risultano</i>		Presenti	Assenti
1	Daniele Taramaschi - Presidente	si	
2	Maurizio Fusi - Assessore	si	
3	Daniela Sartori – Assessore	si	
4	Marco Bresciani – Assessore	si	
<i>Totali presenti/assenti</i>		4	

Partecipa all'adunanza il Segretario Dott. Giuseppe Pinto il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il Sig. Daniele Taramaschi – Presidente assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

<p>PARERI PREVENTIVI: Visto, si esprime parere favorevole in ordine alla regolarità tecnica e contabile sulla proposta della presente delibera, ai sensi dell'art.49 del T.U.E.L. 18.08.2000, n.267. Firmato per quanto di propria competenza dal:</p> <p>f.to Responsabile Servizio Finanziario Dott. Giuseppe Pinto</p>	<p>Verbale, fatto, letto e sottoscritto come segue:</p> <p>f.to IL PRESIDENTE Rag. Daniele Taramaschi</p> <p>f.to IL SEGRETARIO Dott. Giuseppe Pinto</p>
<p>CERTIFICATO DI PUBBLICAZIONE Si certifica che la presente delibera viene affissa all'Albo Pretorio del Comune per 15 giorni consecutivi, ai sensi dell'art. 124 del T.U.E.L. 267/2000, dal 12.03.2018.</p> <p>f.to IL SEGRETARIO DELL'UNIONE Dott. Giuseppe Pinto</p>	<p>PER COPIA CONFORME ALL'ORIGINALE, PER USO AMMINISTRATIVO.</p> <p>IL SEGRETARIO DELL'UNIONE Dott. Giuseppe Pinto</p>  

LA GIUNTA DELL'UNIONE

Visti i prescritti pareri favorevoli, inseriti nella deliberazione in frontespizio, espressi dai responsabili dei servizi interessati alla presente, ai sensi dell'art.49 del T.U.E.L. 18.08.2000 n. 267;

Visto il D.Lgs. 07.03.2005 n.82 rubricato "Codice dell'amministrazione digitale";

Visto l'art.14 bis del suddetto D.Lgs. che al comma 2 lett. a) tra le funzioni attribuite all'AGID prevede tra l'altro l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica;

Vista la circolare 18.04.2017 n.2/2017 emanata dall'Agenzia per l'Italia digitale dal seguente titolo "Sostituzione della circolare n.1/2017 del 17.03.2017 recante "Misure minime di sicurezza I.C.T. per le pubbliche amministrazioni. (direttiva del Presidente del Consiglio dei Ministri 01.08.2015)";

Visti in particolare gli artt. 1 e 4 il cui testo qui di seguito si riporta:

ART.1 – Scopo – comma 1

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza I.C.T. che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.

ART.4 – Modulo di implementazione delle MMS – PA

Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2 anch'esso parte integrante della presente circolare.

Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art.3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso;

Visti i moduli all'uopo predisposti per dare attuazione a quanto previsto dalla circolare avanti richiamata;

Dato atto che detta documentazione è allegata alla presente deliberazione per farne parte integrante e sostanziale;

Con voti unanimi

DELIBERA

- Di approvare le misure minime di sicurezza per questo ente previste nella documentazione che viene allegata a questa deliberazione per formarne parte integrante e sostanziale;
- Di trasmettere la presente deliberazione agli uffici interessati per gli atti di competenza;
- Di dichiarare la presente deliberazione immediatamente eseguibile, stante l'urgenza.

Unione Micropolis

Unione Micropolis (PV)
Arrivo
Prot. N. 0001595
del 28-12-2017 ore 11:20:00
Categoria 1 Classe 7 Fascicolo


Unione Comuni di Cervesina e Pancarana (PV)

Piazza Caduti per la Patria, 1 - Cervesina (PV)

- P.IVA 01951950185 - C.F. 95021580188

Email: unione@comune.cervesina.pv.it - PEC: unioneepapi@pec.it

MODULO IMPLEMENTAZIONE MISURE MINIME DI SICUREZZA

(In ottemperanza a quanto previsto dalla Circolare n.2/2017 del 18 aprile 2017, pubblicata in Gazzetta Ufficiale il 5 maggio 2017)

Data ultima revisione documento:

27 DICEMBRE 2017

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

ABSC_ID	livello	Descrizione	Modalità di implementazione
1 1 1 M	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4.	Inventario risorse attive vedi Allegato 1 ABSC_ID 1-1-1
1 1 2 S	S	Implementare ABSC 1.1 attraverso uno strumento automatico	NON IMPLEMENTATO
1 1 3 A	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NON IMPLEMENTATO
1 1 4 A	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	NON IMPLEMENTATO
1 2 1 S	S	Implementare il "logging" delle operazioni del server DHCP.	NON IMPLEMENTATO
1 2 2 S	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	NON IMPLEMENTATO
1 3 1 M	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Registro sostituzione dispositivi collegati alla rete locale vedi Allegato 2 ABSC_ID 1-3-1
1 3 2 S	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	NON IMPLEMENTATO
1 4 1 M	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Nell'inventario delle risorse attive (vedi 1.1.1) è presente l'indicazione dell'indirizzo IP assegnato oppure il range di indirizzo assegnato ad una categoria di dispositivi.
1 4 2 S	S	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.	NON IMPLEMENTATO
1 4 3 A	A	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.	NON IMPLEMENTATO
1 5 1 A	A	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.	NON IMPLEMENTATO

1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NON IMPLEMENTATO
---	---	---	---	--	------------------

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione
2 1 1 M	S	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.	Registro software autorizzati vedi Allegato 3 ABSC_ID 2-1-1
2 2 1 S	S	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.	NON IMPLEMENTATO
2 2 2 S	S	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).	NON IMPLEMENTATO
2 2 3 A	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	NON IMPLEMENTATO
2 3 1 M	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Gli utenti sono responsabilizzati circa il controllo costante dei software installati sui propri elaboratori. Il tecnico informatico incaricato effettua verifiche periodiche su quanto installato su elaboratori client e server, comparando il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco (2.1.1) viene segnalato per la rimozione oppure, se valutato necessario, per un inserimento nell'elenco.
2 3 2 S	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	NON IMPLEMENTATO

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

ABSC ID	ID	Livello	Descrizione	Modalità di implementazione
4	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.	Il tecnico informatico incaricato è dotato di applicativi per la scansione generale delle vulnerabilità. I sistemi in rete a fronte di significative modifiche (installazione di un sistema o nuovo software, aggiornamento, modifica della configurazione, etc..) verranno analizzati al fine di individuare vulnerabilità critiche.
4	1	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	NON IMPLEMENTATO
4	1	A	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).	NON IMPLEMENTATO
4	2	S	Correlare il log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NON IMPLEMENTATO
4	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	NON IMPLEMENTATO
4	2	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	NON IMPLEMENTATO
4	3	S	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.	NON IMPLEMENTATO
4	3	S	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.	NON IMPLEMENTATO
4	4	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il tecnico informatico incaricato utilizzerà sempre gli strumenti di scansione nella versione più aggiornata durante le procedure di ricerca vulnerabilità.
4	4	S	Registrarsi ad un servizio che fornisca tempestivamente le	NON IMPLEMENTATO

				informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	I sistemi e le applicazioni sono configurati per l'installazione automatica delle patch una volta approvate dal tecnico informatico incaricato.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Non ci sono dispositivi air-gapped che contengono dati. Tali dispositivi sono preposti a fini specifici e sono comunque mantenuti manualmente dal tecnico informatico incaricato. Gli apparati più vecchi che non permettono l'aggiornamento, verranno progressivamente sostituiti compatibilmente con le disponibilità economiche e criticità dell'apparato.
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.	NON IMPLEMENTATO
4	6	1	S	Verificare regolarmente che tutte le attività di scansione siano state eseguite secondo delle policy predefinite.	Il tecnico informatico incaricato si occuperà della risoluzione delle vulnerabilità individuate. Nel caso non siano state trovate o applicate le patch necessarie, oppure non sia possibile applicarle, le eventuali contromisure o le motivazioni della mancata risoluzione verranno documentate su apposito registro/rapporto conservato presso l'ente.
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.	NON IMPLEMENTATO
4	7	2	S	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.	Verranno analizzate le azioni suggerite dal report prodotto dello strumento di scansione utilizzato dal tecnico informatico, agendo in base alle priorità ivi indicate, alla criticità del dispositivo e alla sua localizzazione.
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.).	I sistemi e le applicazioni sono configurati per l'installazione automatica delle patch una volta approvate dal tecnico informatico incaricato. Vulnerabilità di altro tipo verranno risolte nel più breve tempo possibile una volta individuate. Se non è disponibile o possibile la risoluzione al momento del riscontro della vulnerabilità, essa verrà implementata non appena disponibile.
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.	

				In caso di impossibilità di eliminare la vulnerabilità, verrà valutata una soluzione alternativa compatibilmente con le disponibilità economiche e la criticità riscontrata.
4	9	1	S	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.
4	10	1	S	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.

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 amministratore di server e dispositivi di rete sono concessi solo al tecnico informatico incaricato in possesso di credenziali specifiche riservate. Le credenziali dei client sono in carico agli stessi operatori.
5 1 2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	E' attivato il log di sistema per registrare gli accessi come amministratore su PC, server e dispositivi di rete (NAS) preposti alla conservazione dei dati che dispongono di tale funzionalità. Gli apparati più vecchi che non permettono tale funzionalità, verranno progressivamente sostituiti compatibilmente con le disponibilità economiche e la criticità dell'apparato.
5 1 3	S	Asegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	NON IMPLEMENTATO
5 1 4	A	Registrazione delle azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	NON IMPLEMENTATO
5 2 1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Le utenze amministrative saranno catalogate e memorizzate in database cifrato open source certificato OSI
5 2 2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NON IMPLEMENTATO

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.	La credenziale di default dell'utenza amministrativa viene sempre sostituita da una specifica in fase di configurazione del dispositivo e prima della messa in funzione sulla rete locale	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.		NON IMPLEMENTATO
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.		NON IMPLEMENTATO
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.		NON IMPLEMENTATO
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	E' attivato il log di sistema per registrare gli accessi falliti come amministratore sui server e dispositivi di rete (NAS) preposti alla raccolta dei dati. Gli apparati più vecchi che non permettono queste funzionalità verranno progressivamente sostituiti compatibilmente con le disponibilità economiche e criticità dell'apparato.	
5	6	1	A	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.		NON IMPLEMENTATO
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).	Le password associate alle credenziali amministrative di server e NAS che già non soddisfano elevati requisiti di sicurezza verranno adeguate al prossimo cambio (alfanumeriche, lunghezza di almeno 14 caratteri maiuscoli, minuscoli, cifre e simboli). Gli apparati più vecchi che non supportano tale livello di complessità verranno progressivamente sostituiti compatibilmente con le disponibilità economiche e criticità dell'apparato.	
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.		NON IMPLEMENTATO
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La frequenza con cui le password delle credenziali amministrative vengono cambiate varia in base alla loro criticità, e non è comunque mai superiore ai sei mesi.	
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sui dispositivi server e NAS che supportano tale funzionalità ne è in previsione l'attivazione. Gli apparati più vecchi che non supportano tale gestione verranno	

				progressivamente sostituiti compatibilmente con le disponibilità economiche e criticità dell'apparato.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
5	8	1	S	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.
5	9	1	S	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.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
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.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

ABSC ID	Livello	Descrizione	Modalità di implementazione			
			8	1	2	3
8 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.	Su tutti i PC e server Windows è installato un antivirus con funzionalità antimalware e aggiornamento quotidiano.			
8 1	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC e server Windows è attivato il firewall di Windows.			
8 1	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.		NON IMPLEMENTATO		
8 2	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.			NON IMPLEMENTATO	
8 2	S	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.			NON IMPLEMENTATO	
8 2	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.			NON IMPLEMENTATO	
8 3	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è previsto l'uso di dispositivi esterni. Nel caso di necessità, viene chiesto al tecnico informatico incaricato di verificarne la possibilità di uso sicuro e limitato del dispositivo per le finalità dichiarate.		NON IMPLEMENTATO	
8 3	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.			NON IMPLEMENTATO	
8 4	S	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.			NON IMPLEMENTATO	
8 4	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.			NON IMPLEMENTATO	
8 5	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli			NON IMPLEMENTATO	

				host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	NON IMPLEMENTATO
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	NON IMPLEMENTATO
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' in previsione la disattivazione dell'esecuzione automatica.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'esecuzione automatica di contenuti dinamici dei file sono bloccati di default.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' in previsione di implementare il blocco dell'apertura automatica dei messaggi di posta elettronica inclusa la loro anteprima.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' in previsione di implementare il blocco dell'anteprima automatica dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Gli antivirus locali sono impostati per il controllo antivirus e antimalware automatico e in tempo reale di tutti i file, inclusi quelli presenti su dispositivi rimovibili al momento della connessione.
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.	Il fornitore del servizio esterno (Aruba s.r.l.) include tra i propri servizi il filtraggio antivirus e antispam
8	9	2	M	Filtrare il contenuto del traffico web.	Funzionalità di filtro sul traffico web sono implementati sia nell'antivirus locale che a nel firewall centralizzato
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).	Gli antivirus sono configurati per bloccare in modo preventivo file potenzialmente dannosi e non necessari provenienti dalla posta elettronica o esterni alla rete locale
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NON IMPLEMENTATO
8	11	1	S	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.	NON IMPLEMENTATO

ABSC 10 (CSC 10): COPIE DI SICUREZZA

				Modalità di implementazione
ABSC_ID	Livello	Descrizione		
10_1_1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Tutti database e i documenti presenti sui server comunali sono oggetto di backup giornaliero. I dati sui client sono oggetto di backup con cadenza almeno settimanale manualmente.	NON IMPLEMENTATO
10_1_2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	I backup locali sono salvati sia internamente ai server stessi che su NAS locali.	NON IMPLEMENTATO
10_1_3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	I backup locali sono salvati sia internamente ai server stessi che su NAS locali.	NON IMPLEMENTATO
10_2_1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Non viene effettuata alcuna cifratura.	NON IMPLEMENTATO
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.	Le credenziali utilizzate per l'accesso ai sistemi di copia sono specifiche. I dispositivi preposti allo scopo hanno partizioni non direttamente accessibili attraverso la rete informatica. Ogni utenza può accedere solo ai propri dati.	NON IMPLEMENTATO
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.	Le credenziali utilizzate per l'accesso ai sistemi di copia sono specifiche. I dispositivi preposti allo scopo hanno partizioni non direttamente accessibili attraverso la rete informatica. Ogni utenza può accedere solo ai propri dati.	NON IMPLEMENTATO

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

				Modalità di implementazione
ABSC_ID	Livello	Descrizione		
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	Gli unici database contenenti dati sensibili presenti in formato digitale sono quelli di stato civile, anagrafe, alre insieme al alcuni documenti attinenti all'attività di Polizia Locale. Questi vengono trattati secondo le vigenti normative in materia di privacy.	NON IMPLEMENTATO
13_2_1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul	NON IMPLEMENTATO
13_3_1	A			

			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.	
13	4	1	A 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.	NON IMPLEMENTATO
13	5	1	A 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.	NON IMPLEMENTATO
13	5	2	A 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.	NON IMPLEMENTATO
13	6	1	A 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.	NON IMPLEMENTATO
13	6	2	A Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	NON IMPLEMENTATO
13	7	1	A Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NON IMPLEMENTATO
13	8	1	M Bloccare il traffico da e verso url presenti in una blacklist.	Il firewall centralizzato implementa le funzionalità di blocco verso gli url tramite il loro inserimento in una blacklist
13	9	1	A 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.	

Allegato 1 - Inventario risorse attive - aggiornato al 27/12/2017

Codice identificativo	Descrizione dispositivo	MAC	IP	Anno	Collocazione
firewall	Firewall Zyxwell USG 210		192.168.1.1		
Ragioneria 1	PDL Ragioneria n.1		192.168.1.10		
Ragioneria 2	PDL Ragioneria n.2		192.168.1.15		
Sindaco	PDL Sindaco		192.168.1.18		
Anagrafe	PDL Anagrafe		192.168.1.26		
Polizia Locale	PDL Polizia Locale		192.168.1.25		
Tecnico	PDL Ufficio Tecnico		192.168.1.13		
Unione PC	PDL Unione				
Protocollo	PDL Protocollo		192.168.1.160		
Videosorveglianza	Server Videosorveglianza		192.168.1.120-128		
Centralino e IP Phone	Centralino telefonico e telefoni IP		192.168.1.200		
Multifuzione Ricoh	Multifunzione Ricoh		192.168.1.201		
Multifuzione Kyocera	Multifunzione Kyocera FS-4200DN		192.168.1.202		
Multifuzione canon	Multifunzione Canon LBP6780		192.168.1.245		
Server Halley	Server Halley applicativi comunali		192.168.1.246		
Concentratore Halley	Concentratore Halley		192.168.1.247		
NAS_01	Backup SRV/CEPAPI e PC Uffici		192.168.1.249		
NAS_02	Backup server Halley		192.168.1.251		
CERV/NAS	Backup SRV/CEPAPI e PC Uffici		192.168.1.252		
Server SRV/CEPAPI	Server comunale				

Allegato 2 - Registro sostituzione risorse attive - aggiornato al 27/12/2017

DATA	Codice identificativo - Descrizione	Operazione svolta	MAC	IP	Collocazione
------	-------------------------------------	-------------------	-----	----	--------------

Allegato 3 - Registro software autorizzati - aggiornato al 22/12/2017

Nome e descrizione	Produttore	Scadenza licenza	Versione	Collocazione
Windows 7 (sistema operativo)	Microsoft			pc comunali
Windows 10 (sistema operativo)	Microsoft			pc comunali
Linux (sistema operativo)	Canonical Ltd.			server comunale
Windows Server 2008	Microsoft			server comunale
Halley - demografico / stato civile / elettorale	Halley Informatica			pc comunali
Halley - contabilità / protocollo / albo pretorio	Halley Informatica			pc comunali
Software office automation Office	Microsoft			pc comunali
Software office automation Openoffice	Apache software foundation			pc comunali
Browser web Internet explorer	Microsoft			pc comunali
Browser web firefox	Mozilla Foundation			pc comunali
Browser web chrome	Google			pc comunali
Client posta elettronica (Outlook, Live Mail)	Microsoft			pc comunali
Client posta elettronica (Thunderbird)	Mozilla Foundation			pc comunali
Firma elettronica (Dike, ArubaSign, Digitalsign)	Infocert, Arubapec			pc comunali
Software antivirus				pc comunali
Acrobat reader	Adobe			pc comunali
Gestore file compressi (7 zip)	Igor Pavlov			pc comunali
Masterizzazione CD /DVD (CD Burner)	Impressum			pc comunali
Copia e backup (Syncback free)	2brightsparks			pc comunali
Riproduzione video (Videolan client)	Video-lan			pc comunali
PDF Creator	PdfForge			pc comunali
Anag AIRE	SOGEI			pc comunali
Software teleassistenza (Supremo - Teamviewer)	Teamviewer \ Nanosystem			pc comunali
Vecchi software comuni (SICI - TINN)				pc comunali
Desktop telematico	SOGEI			pc comunali
GICIA	CSI Piemonte			pc comunali
Software compilazione F24 online	SOGEI			pc comunali
Java runtime machine	Oracle			pc comunali
Keepass	Dominik Reichl			pc comunali

Allegato 4 ABSC ID 3-1-1- Configurazioni standard dispositivi attivi

Aggiornato al 22/12/2017

Server

Le operazioni di configurazione di un server iniziano dalla scelta dei sistemi operativi e del software che dovranno essere eseguiti su di esso.

- Individuare delle funzioni ai cui verrà dedicato il server
- Individuare i software che verranno eseguiti su di esso
- Individuare il sistema operativo (SO) più adatto per compatibilità, affidabilità, sicurezza, aderenza agli scopi.
- Individuare i locali in cui verrà mantenuto, garantendone la sicurezza fisica e l'isolamento elettrico
- Individuare la configurazione di rete più adeguata, in base alla finalità di utilizzo e sicurezza
- Il SO installato dovrà essere l'ultima versione disponibile, a meno di incompatibilità con il software che verrà eseguito su di esso. In ogni caso dovranno essere installate le ultime patch di sicurezza disponibili al momento dell'installazione per la versione del SO scelto.
- Gli applicativi software che verranno installati dovranno essere aggiornati con le ultime patch di sicurezza disponibili al momento dell'installazione.
- SO e applicativi software saranno configurati per l'applicazione automatica delle patch di sicurezza e degli aggiornamenti, che avverrà previa valutazione e autorizzazione del tecnico informatico incaricato.
- Viene effettuata una valutazione complessiva sulla sicurezza in relazione alle funzionalità a cui il server sarà adibito.
- Tutti i servizi e le funzionalità non necessarie saranno disattivate.
- Verrà installato il software antivirus autorizzato presso l'ente e configurato opportunamente in relazione agli applicativi eseguiti sul server.
- Firewall locale e firewall centralizzato verranno configurati opportunamente in relazione alle funzionalità attribuite al server.
- Verranno create particolari utenze preposte ad ottenere (previa autenticazione) i più elevati accessi amministrativi. Le password associate a queste utenze saranno di tipo robusto e di lunghezza non inferiore a 14 caratteri. Verranno inoltre individuati i titolari di tali credenziali. Altri modi di accesso diretto alle utenze amministrative verranno disabilitate.
- Impostare policy relative alla sostituzione programmata delle password relative a credenziali amministrative (aging), alla registrazioni degli accessi (log) e alla storicitizzazione delle password.
- Se necessario, verranno create le utenze per i client e gli operatori che avranno necessità di fruire dei servizi offerti dal server. Tali credenziali dovranno essere note al solo destinatario.
- Viene disabilitata la richiesta di accesso da parte di client non appartenenti alla rete dell'ente
- In caso di gestione remota, sarà resa possibile solo tramite connessioni cifrate.
- Se il server elaborerà basi di dati o archivi di documenti, verrà predisposta e implementata la politica di gestione delle copie locali e remote a seconda della tipologia dei dati trattati
- Archiviare le immagini ISO, gli applicativi, gli snapshot di sistema e quanto altro necessario al fine un ripristino del server offline. Tutto quanto necessario deve essere mantenuto aggiornato in caso modifiche o aggiornamenti sostanziali del sistema.
- Aggiornare l'inventario e il registro sostituzione dei dispositivi attivi.

Personal computer

Le operazioni di configurazione di un PC iniziano dalla scelta del sistema operativo e dei software che dovranno essere eseguiti su di esso.

- Individuare delle funzionalità a cui verrà predisposto l'elaboratore
- Individuare i software che verranno eseguiti su di esso
- Individuare il sistema operativo (SO) più adatto per compatibilità, affidabilità, sicurezza, aderenza agli scopi.
- Individuare i locali in cui verrà installato ed utilizzato
- Individuare la configurazione di rete più adeguata, in base alla finalità di utilizzo e sicurezza
- Il SO Installato dovrà essere l'ultima versione disponibile, a meno di incompatibilità con il software che verrà eseguito su di esso. In ogni caso dovranno essere installate le ultime patch di sicurezza disponibili al momento dell'installazione per la versione del SO scelto.
- Eventuali automatismi nella gestione delle anteprime o esecuzione automatica devono essere disabilitati.
- Gli applicativi software che verranno installati dovranno essere aggiornati con le ultime patch di sicurezza disponibili al momento dell'installazione.
- Gli applicativi che verranno installati dovranno essere preventivamente stati autorizzati e quindi risultare presenti nella lista dei software autorizzati.
- SO e applicativi software saranno configurati per l'applicazione automatica delle patch di sicurezza e degli aggiornamenti, che avverrà previa valutazione e autorizzazione del tecnico informatico incaricato.
- Eventuale contenuto attivo (macro, script, etc..) deve essere disabilitato preventivamente ed eseguibile solo previo autorizzazione dell'operatore
- I client per la posta elettronica dovranno avere l'anteprima disabilitata.
- Viene effettuata una valutazione complessiva sulla sicurezza in relazione alle funzionalità a cui il PC sarà adibito.
- Verrà installato il software antivirus autorizzato presso l'ente e configurato opportunamente in relazione agli applicativi installati, con particolare attenzione verso l'abilitazione del filtraggio dei contenuti web, il controllo degli allegati di posta elettronica e la scansione in tempo reale di tutti i file compresi quelli su dispositivi rimovibili.
- Firewall locale e firewall centralizzato verranno configurati opportunamente in relazione alle funzionalità attribuite all'elaboratore
- Verranno create le utenze gli operatori che avranno necessità di fruire dei servizi offerti dall'elaboratore. Tali credenziali dovranno essere note al solo destinatario.
- In caso di gestione remota, sarà resa possibile solo tramite connessioni cificate.
- Se sono presenti basi di dati o archivi di documenti locali, verrà predisposta e implementata la politica di gestione delle copie locali a seconda della tipologia dei dati trattati
- Sono archiviate le immagini ISO, gli applicativi, gli snapshot di sistema e quanto altro necessario al fine di un ripristino dell'elaboratore in modalità offline.
- Aggiornare l'inventario e il registro sostituzione dei dispositivi attivi.

Altri dispositivi di rete

Prima di collegare un nuovo dispositivo attivo alla rete locale, verrà sempre effettuata la seguente procedura:

- Verifica generale del dispositivo, e valutazione dell'impatto nella rete locale, soprattutto in termini di sicurezza
- Analisi della configurazione da attribuire e del luogo di esercizio, in relazione alle funzionalità svolte dal dispositivo
- Aggiornamento del software di sistema all'ultima versione disponibile
- Sostituzione della password di gestione amministrativa di default e se possibile dell'intera credenziale, inserendo una password robusta di almeno 14 caratteri e policy di log accessi, aging e storcizzazione della password
- Se necessario, creare gli account per gli utenti che avranno accesso ai servizi offerti dal dispositivo, introducendo se possibile policy di aging e storcizzazione password
- Se necessario, implementare politiche di backup dati e configurazione
- In caso di gestione remota, saranno abilitate solo tramite connessioni cifrate (se il dispositivo lo consente)
- Individuare i parametri di rete adeguati alla destinazione d'uso del dispositivo
- Aggiornare l'inventario e il registro sostituzione dei dispositivi attivi.

Ricorrente

Procedura HA - Hw Hardware N. 4626 del 27-12-2017
"Misure minime di sicurezza ICT per le pubbliche amministrazioni"

Inserito da: Armignacca Federico

Descrizione

Si chiedono chiarimenti per la compilazione del modulo di implementazione relativo alle misure minime di sicurezza ICT per le pubbliche amministrazioni come da circolare del 18 aprile 2017 n. 2/2017, con particolare riferimento ai servizi offerti da Halley Informatica

Argomento: Procedura

Versione:

Tipo ricorrente: Consulenza

Tipo testo ricorrente: Testo ricorrente

Destinatari:

Web: Sì

Data ultima modifica: 29-12-2017

Effettuata dall'operatore: Armignacca Federico

Dati I.I.

I.I. collegata 0 Stato I.I. Versione aggiornamento in cui è inclusa

Ricorrenza

Da telefonate: 0 Da problemi: 20 Totale: 20

Testo del ricorrente

Chiarimenti

Per facilitare l'utente nella redazione del modulo, nella tabella sottostante si riportano tutti i casi in cui i servizi erogati da Halley informatica soddisfano le misure di sicurezza ICT.

Per consentire una lettura più agevole del documento si riportano di seguito alcuni chiarimenti in merito al significato delle colonne.

- La colonna "ABSC_ID" fa riferimento all'identificatore gerarchico del controllo;
- La colonna "Livello" si riferisce al livello di attuazione. Ne sono previsti tre:
 - o il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. Nella tabella è indicato con "M" ("Minimo");
 - o i livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi: è indicato con la lettera "S" il livello "Standard" e può essere assunto come base di riferimento nella maggior parte dei casi e con la lettera "A" il livello "Alto" che può essere visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.
- La colonna "Descrizione" riporta una definizione sintetica del controllo.
- L'ultima colonna "Modalità di implementazione" è stata compilata con l'indicazione del servizio Halley con cui viene rispettato l'adempimento.

Una volta compilato, il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e non è necessario che sia inviato ad alcun ente e solo in caso di incidente informatico deve essere trasmesso al CERT-PA unitamente alla segnalazione dell'incidente stesso.

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione
---------	---------	-------------	-----------------------------

2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Mantengono un inventario del software installato tramite la Dashboard Halley, le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud White Box Ced Remoto Antivirus Web Protection Content Filtering
2	3	3	A	Installare strumenti automatici d'inventario del software che registrano anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Registrano le versioni del sistema operativo e le applicazioni installate, le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud White Box Ced Remoto Antivirus Web Protection Content Filtering I servizi White Box e Ced Remoto, invece, registrano anche il livello di patch.

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.	Utilizzano le configurazioni standard per la protezione dei sistemi operativi le Workstation ed i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Disaster Recovery Cloud White Box Ced Remoto
3	1	2	S	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	Hanno implementato l'hardening per eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate i Server che hanno attivo uno dei seguenti servizi: Black Box

				eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	Full Service Server Continuity Cloud
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Hanno una configurazione standard definita i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Hanno una configurazione standard definita i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud White Box
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).	Ricevono dati nelle nostre dashboard in modo sicuro, I Server e le Workstation che hanno attivo uno dei seguenti servizi (per i server tramite tunnel crittografato ssh mentre per le workstation tramite protocollo https): Black Box Full Service Server Continuity Disaster Recovery Cloud White Box Ced Remoto Antivirus Web Protection Contenten Filter

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione
4	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscono a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	1	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto

4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Hanno attivo il log delle scansioni vulnerabilità le Workstation con attivo il servizio di: White Box Ced Remoto
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Registrano le attività dei sistemi di scanning delle vulnerabilità le Workstation con attivo il servizio di: White Box Ced Remoto
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Vengono regolarmente aggiornati con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Sono in grado di riconoscere le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Installano le patch critiche ed importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto
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.	La nostra Dashboard riceve un alert se una patch critica ed importante dei prodotti Microsoft fallisce durante un'installazione per le Workstation con attivo il servizio di: White Box Ced Remoto
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.	Eseguono una scansione delle vulnerabilità ed installano le patch critiche e importanti dei prodotti Microsoft le Workstation con attivo il servizio di: White Box Ced Remoto

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.	Limitano gli accessi ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi i Server e le Workstation che hanno attivo uno dei seguenti servizi:

					Black Box Full Service Server Continuity Cloud Storage dati non Halley Servizio Firewall Timbrature Sicure
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Registrano gli accessi effettuati i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Cloud
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.	Vengono sostituite le password standard di amministratore con password complesse i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halley
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tracciano i log di tentativi di accesso e le registrano sulla nostra Dashboard i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Hanno password amministrative complesse i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halley
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Vengono sostituite con sufficiente frequenza le password dei Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity
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 credenziali amministrative anonime vengono utilizzate per provvedere alla manutenzione ordinaria e/o straordinaria dei Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Conservano le credenziali amministrative in modo da garantirne disponibilità e riservatezza i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity Servizio Firewall Timbrature Sicure Storage dati non Halle Disaster recovery
---	----	---	---	--	---

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.	Bloccano l'esecuzione di malware e sono mantenuti sempre aggiornati i Server e le Workstation che hanno attivo uno dei seguenti servizi: Servizio Antivirus
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Hanno sempre il firewall di sistema i Server e le Workstation che hanno attivo uno dei seguenti servizi: Black Box Full Service Server Continuity White Box Ced Remoto
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Il servizio antivirus è gestito centralmente tramite la nostra Dashboard e non è consentito agli utenti di alterarne la configurazione per i Server e le Workstation che hanno attivo il servizio: Servizio Antivirus
8	2	2	S	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.	Per i Server e le Workstation che hanno attivo il Servizio Antivirus è possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo e la corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Viene effettuata un' analisi dei potenziali malware in un'infrastruttura dedicata, basata sul cloud i Server e le Workstation che hanno attivo il servizio:

					Servizio Antivirus
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Usano strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Bloccano siti con cattiva reputazione i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Eseguono una scansione anti-malware dei supporti rimuovibili al momento della loro connessione i Server e le Workstation che hanno attivo il servizio: Servizio Antivirus
8	9	2	M	Filtrare il contenuto del traffico web.	Filtrano il contenuto del traffico web i Server e le Workstation che hanno attivo il servizio: Servizio Web Protection

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID				Livello	Descrizione	Modalità di implementazione
10	1	1	M		<p>Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.</p>	<p>Effettuano una copia locale quotidiana mantenendo uno storico di 60 giorni e dove previsto la stessa copia viene ridondata su storage i Server che hanno attivo uno dei seguenti servizi: Black Box Full Service Cloud</p> <p>Effettuano una sincronia del database in tempo reale mantenendo i dati sempre aggiornati tra server di produzione e server Continuity i Server che hanno attivo il servizio: Server Continuity</p> <p>Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni i Server che hanno attivo il servizio: Disaster Recovery</p> <p>Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema.</p> <p>Copiano giornalmente le cartelle condivise scelte dal</p>

					<p>cliente mantenendo uno storico di 60 giorni le Workstation che hanno attivo il servizio: Servizio Storage</p> <p>Oltre a copiare giornalmente le cartelle condivise scelte dal cliente mantenendo uno storico di 60 giorni effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni delle cartelle scelte per il Disaster recovery le Workstation che hanno attivo il servizio: Disaster recovery dati non halley</p>
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	<p>Viene verificata periodicamente l'utilizzabilità delle copie mediante ripristino di prova sulle Workstation e i Server che hanno attivo uno dei seguenti servizi:</p> <p>Black Box Full Service Server Continuity Disaster Recovery Cloud</p>
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.	<p>Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni i Server che hanno attivo il servizio: Disaster Recovery</p> <p>Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema</p>
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.	<p>Effettuano una copia a Roma e Trento crittografando i dati e mantenendo uno storico di 60 giorni rendendoli inaccessibili dal sistema i Server che hanno attivo il servizio: Disaster Recovery</p> <p>Tutte queste copie mantengono le informazioni strettamente necessarie per il completo ripristino del sistema</p>

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	<p>Bloccano il traffico da e verso url presenti in una blacklist o in categorie concordate le Workstation e i Server che hanno attivo il servizio: Content Filtering</p>
----	---	---	---	--	--

Per maggiori informazioni e specifiche tecniche sui singoli servizi offerti da Halley Informatica si rimanda al sito www.halleysistemistica.it

Qualsiasi altra informazione sulla normativa è reperibile al seguente link:

<http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni>

