ORDINE DEGLI INGEGNERI
PROVINCIA DI UDINE

COPIA

ATTUAZIONE DELLE MISURE MINIME DI SICUREZZA ICT PER LE P.A.

Documento rispondente alle richieste presenti in:

AGENZIA PER L'ITALIA DIGITALE CIRCOLARE 18 aprile 2017, n. 2/2017.
Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 ° agosto 2015)».

Udine, 29 dicembre 2017

Il responsabile legale della struttura
Ing. Stefano Guatti

Il responsabile digitale della struttura
Ing. Fabio Zorzini

Ordine degli Ingegneri della Provincia di Udine
Via di Toppo, 5 / 33100 Udine / Tel. 0432.505305 / Fax. 0432.503941
segreteria@ordineingegneri.ud.it / www.ordineingegneri.ud.it

INTRODUZIONE

Il presente documento riporta le modalità con cui ciascuna misura di sicurezza I.C.T. è implementata presso la pubblica amministrazione dell'Ordine degli Ingegneri della Provincia di Udine.
Le misure sono sinteticamente riportate utilizzando come riferimento il modulo di implementazione di cui all'allegato 2 della circolare "AGENZIA PER L'ITALIA DIGITALE CIRCOLARE 18 aprile 2017, n. 2/2017 - Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 ° agosto 2015)»".
In accordo con le richieste normative, considerate le dimensioni della struttura della specifica pubblica amministrazione, si ritiene adeguata l'applicazione delle misure con riferimento al livello minimo.

SOMMARIO

1. 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	Utilizzo del software Ocs inventory e salvataggio dell'inventario su file excel per ogni dispositivo.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Utilizzo del software Ocs inventory.
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.	Utilizzo del software Ocs inventory.

2. 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.	Utilizzo dei software Ocs inventory e Kaspersky small office.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Utilizzo del software Kaspersky small office.

3. 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.	Utilizzo del software Kaspersky small office e regolare aggiornamento del Sistema operative tramite Windows update.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Utilizzo del software: Kaspersky small office, Office 365, Acrobat Reader.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Utilizzo dei DVD di ripristino standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Attualmente si utilizzano DVD di ripristino standard, in futuro verrà implementato un Nas di backup con file img.

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).	Attualmente si evitano tutte le operazioni di amministrazione remota, in futuro verrà implementato un Firewall.

4. 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.	Utilizzo del software Ocs inventory.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Utilizzo regolare di Windows update.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Utilizzo regolare di Windows update.
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.	Utilizzo di Windows update al momento della connessione alla rete.
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.	Utilizzo dei software Ocs inventory e Kaspersky small office.
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.).	Attualmente si considerano tutti i rischi (vulnerabilità e impatti) di pari livello di gravità, in futuro verrà implementato un Firewall per consentire una più appropriata scala di priorità.
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.	Utilizzo regolare di Windows update.

5. 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.	Attualmente si considerano tutti gli utenti con competenze adeguate per gestire i privilegi di amministrazione, in futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Attualmente si considerano tutti gli utenti con competenze adeguate per gestire i privilegi di amministrazione, gli accessi sono coincidenti con gli orari lavorativi dei dipendenti della p.a.. In futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Attualmente le utenze amministrative coincidono con i dipendenti della p.a. (autorizzati). In futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
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.	Attualmente non è previsto l'utilizzo di nuovi dispositivi connessi alla rete. In futuro, se necessario, saranno implementati controlli tramite il sistema Windows Active directory.
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).	A partire dal 2018 le utenze amministrative utilizzeranno credenziali di elevata robustezza.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	A partire dal 2018 le utenze utilizzeranno amministrative sostituiranno le credenziali con sufficiente frequenza. In futuro, se necessario, sarà implementato un sistema di password aging mediante il sistema Windows di Active directory.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	A partire dal 2018 le utenze utilizzeranno amministrative sostituiranno le credenziali con altre non utilizzate recentemente in modo manuale. In futuro, se necessario, sarà implementato un sistema di password history mediante il sistema Windows di Active directory.

5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Attualmente si considerano tutti gli utenti con competenze adeguate per gestire i privilegi di amministrazione, in futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Attualmente le utenze amministrative coincidono con i dipendenti della p.a.. In futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
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.	Attualmente si considerano tutti gli utenti con competenze adeguate per gestire i privilegi di amministrazione, in futuro, se necessario, saranno implementati utenti con meno privilegi tramite il sistema Windows Active directory.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate su supporto cartaceo.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non è previsto l'utilizzo di chiavi digitali.

6. 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.	Utilizzo del software Kaspersky small office.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Utilizzo del software Kaspersky small office.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Attualmente non è previsto l'utilizzo di dispositivi che siano esterni a quelli necessari per le attività aziendali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Opzioni disabilitata nel sistema operativo Windows (controllo periodico da parte delle utenze amministrative).
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Opzione disabilitata tramite nel software Office (controllo periodico da parte delle utenze amministrative).

8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Utilizzo del software Kaspersky small office (controllo periodico da parte delle utenze amministrative).
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Opzione disabilitata tramite Esplora risorse (controllo periodico da parte delle utenze amministrative).
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Utilizzo del software Kaspersky small office.
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.	Utilizzo del software Kaspersky small office.
8	9	2	M	Filtrare il contenuto del traffico web.	Kaspersky small office
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).	Kaspersky small office firewall

7. ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Attualmente il ripristino del sistema avviene tramite DVD di installazione e recupero dati da cloud. In futuro verrà implementato il sistema Windows server backup.
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.	Attualmente i dati sono su cloud. In futuro verrà implementato il sistema Windows server backup.
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.	Attualmente i dati sono su cloud. In futuro verrà implementato un backup anche su disco esterno rimovibile.

8. 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	Attualmente si considerano tutti i dati non rilevanti al fine della protezione crittografica, in futuro verrà applicata ad una selezione di dati ritenuta rilevante.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Attualmente si evita le utenze evitano manualmente il traffico verso url non strettamente necessarie alle funzioni della p.a.. In futuro, se necessario, verrà implementato un firewall.

9. ATTIVITÀ DI FUTURA IMPLEMENTAZIONE

Il miglioramento della sicurezza della struttura sarà perseguito mediante le seguenti attività di futura implementazione:

- Acquisto di un apparato Firewall per permettere la creazione di connessioni sicure e di bloccare attacchi Internet provenienti dall'esterno.
- Aggiornamento del programma Antivirus con una versione di programma di livello superiore all'attuale installato. L'obbiettivo è alzare il livello di sicurezza sia all'interno della rete che verso esterno, oltre a questo permettere una gestione centralizzata delle configurazioni e limitazioni da attuare sui vari client.
- Implementazione sul sistema Windows Server della configurazione delle Active Directory. Saranno creati degli Utenti Amministratori del Sistema, scadenzato il cambio Password.
- Nomina di un responsabile di Sistema che abbia possesso di tutte le password, che provveda a verificare che le scadenze programmate vengano rispettate e che riceva sulla sua posta la mail di avvenuto backup.
- Implementazione sui i client di piccole modifiche sul pacchetto Office e sul Sistema Operativo.
- Acquisto di un ulteriore NAS e di un disco esterno per il salvataggio dati.

10. CONCLUSIONI

Il presente documento riporta le modalità con cui ciascuna misura è implementata presso la pubblica amministrazione dell'Ordine degli Ingegneri della Provincia di Udine, alla data del 31 dicembre 2017.
Le misure sono state sinteticamente riportate utilizzando come riferimento il modulo di implementazione di cui all'allegato 2 della circolare "AGENZIA PER L'ITALIA DIGITALE CIRCOLARE 18 aprile 2017, n. 2/2017 - Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 ° agosto 2015)»".
In accordo con le richieste normative, considerate le dimensioni della struttura della specifica pubblica amministrazione, si è ritenuto adeguata l'applicazione delle misure con riferimento al livello minimo.