ALLEGATO 3

CIRCOLARE 17 marzo 2017, n. 1/2017: "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399)"

Implementazione delle linee AGID nel Comune

1.1.1 - *Implementare un inventario delle risorse attive correlato a quello ABSC 1.4:*
È installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

1.1.2 - *Implementare ABSC 1.1.1 attraverso uno strumento automatico:*
È installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

1.3.1 - *Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete:*
È installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

1.3.2 - *Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete*

E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

1.4.1 - *Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura, l'agente infatti è dotato di funzione apposita che effettua la scansione IP della rete e provvede a inventariare i sistemi e dispositivi collegati alla rete, compresi quelli dove non è possibile installare l'agente stesso: marcatempo, stampanti, router e dispositivi simili;

2.1.1 - *Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura. L'agente di monitoraggio stilerà la lista dei software installati e verrà attivata una procedura interna con cadenza mensile che verificherà quali nuovi software sono stati installati e la relativa autorizzazione;

2.3.1 - *Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

2.3.2 - *Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

2.3.3 - *Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

3.1.1 - *Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi:*
Gli amministratori di sistema provvederanno ad utilizzare solo configurazioni standard sicure (hardened);

3.2.1 - *Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione:*
Gli amministratori di sistema provvederanno ad utilizzare solo configurazioni standard sicure (hardened) così come definite dagli standard di settore;

3.2.2 - *Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard:*
I backup delle configurazioni standard delle postazioni di lavoro tipiche di ogni servizio verranno effettuate tramite immagini dei dischi fissi, mentre i Server vengono ripristinati tramite da backup che coinvolgono l'interna Virtual Machine;

3.3.1 - *Le immagini d'installazione devono essere memorizzate offline:*
Le immagini sia dei server che delle postazioni di lavoro vengono memorizzate su posizioni offline;

3.4.1 - *Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri):*
*L*e azioni di amministrazione remota verranno effettuate tramite connessioni criptate;

4.1.1 - *Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

4.1.2 - *Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

4.4.1 - *Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

4.4.2 - *Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura;

4.5.1 - *Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura

4.5.2 - *Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air- gapped, adottando misure adeguate al loro livello di criticità:*
Non sono presenti sistemi air-gapped;

4.7.1 - *Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio*:
Periodicamente verrà valutata la scansione delle vulnerabilità e saranno prese le opportune azioni previste;

4.8.1 - *Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.):*
Verrà stilato apposito documento "Piano Gestione dei Rischi ICT";

4.8.2 - *Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche:*
E' installato sui dispositivi un software/agente di monitoraggio che è dotato di apposita funzionalità per poter soddisfare a questa misura; Tale software provvederà all'installazione delle patch secondo la relativa priorità, resta compito degli amministratori di sistema verificare le situazioni critiche o, in cui la procedura di default ha dato esito negativo;

5.1.1 - *Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi:*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.1.2 - *Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato:*
E' installato apposito agente che registra gli accessi, come descritto al Capo II/Art.6/punto 10. Gli amministratori di sistema adottano quanto previsto da questa misura;

5.2.1 - *Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata:*
Verrà stilato un Documento che conterrà la lista delle utenze amministrative e la relativa custodia che verrà allegato al presente Regolamento;

5.3.1 - *Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso:*
Verrà applicata la procedura descritta al CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI del presente documento;

5.7.1 - *Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri):*
Verranno attivate le procedura descritte al CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI del presente documento e forzata la complessità della password tramite Policy sistema;

5.7.3 - *Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging):*
Verranno attivate le procedura descritte al CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI del presente documento e forzata la complessità della password tramite Policy sistema;

5.7.4 - *Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history):*
Verranno attivate le procedura descritte al CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI del presente documento e forzata la complessità della password tramite Policy sistema;

5.7.6 - *Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi:*
Verranno attivate le procedura descritte al CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI del presente documento e forzata la complessità della password tramite Policy sistema;

5.10.1 - *Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse:*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.10.2 - *Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona:*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.10.3 - *Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso:*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.10.4 - *Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio):*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.11.1 - *Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza:*
Gli amministratori di sistema adottano quanto previsto da questa misura;

5.11.2 - *Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette:*
Attualmente nel sistema non sono presenti certificati che richiedano provvedimenti particolari.

8.1.1 - *Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.1.2 - *Installare su tutti i dispositivi firewall ed IPS personali:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.1.3 - *Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.2.1 - *Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.2.2 - *È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.2.3 - *L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.3.1 - *Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura, inoltre, nel presente regolamento al CAPO II/ Art. 10 è specificatamente previsto quanto richiesto ;

8.3.2 - *Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.7.1 - *Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.7.2 - *Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.7.3 - *Disattivare l'apertura automatica dei messaggi di posta elettronica:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.7.4 - *Disattivare l'anteprima automatica dei contenuti dei file:*
E' installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.8.1 - *Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione:*
È installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;

8.9.1 - *Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam:*
È installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura; Strumenti antispam sono normalmente presenti nei mailserver in uso.

8.9.2 - *Filtrare il contenuto del traffico web:*
È installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura; È presente inoltre un Firewall dotato di apposita funzione;

8.9.3 - *Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab):*
È installato sui dispositivi un software/agente di sicurezza che è dotato di apposita funzionalità per poter soddisfare a questa misura;