REGIONE DEL VENETO

giunta regionale

Direzione ICT e Agenda Digitale
Unità Organizzativa Strategia ICT e Agenda Digitale
P.O. Piani e programmi società dell'informazione

Misure minime di sicurezza ICT per le Pubbliche Amministrazioni AGID

Il Presidente del Consiglio dei Ministri, nella Direttiva del 15 Gennaio 2015 (DPCM 15-1-2015 sul Piano di sicurezza cibernetica nazionale),dispone che:
"Tutte le Amministrazioni,…. devono dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. l'Agenzia per l'Italia digitale (AGID) dovrà rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte."
Per dare seguito a questa Direttiva, a settembre 2016 AGID ha emanato le misure minime di Sicurezza ICT per le PA, che costituiscono un'anticipazione delle Regole Tecniche che dovrà emanare il Dipartimento della Funzione Pubblica.
Anche se non hanno ancora forza di legge, le misure minime costituiscono un parametro di legittimità dell'azione amministrativa a cui le PA devono conformarsi , in attesa di indicazioni più precise.

Si invitano i tecnici informatici delle PA all'analisi dell'intero documento ed al progressivo adeguamento di tutte le misure, almeno per il livello minimo che si intende obbligatorio.

I controlli sono stati classificati in tre livelli: minimo, standard (quello raccomandato), alto (quello a cui mirare).

Le misure si possono riassumere in 8 categorie di controlli. Per ciascuna categoria è stata fatta una tabella con un elenco dettagliato di regole.

Per la definizione delle misure ci si è basati sui SANS20, i cosiddetti 20 controlli critici di sicurezza del CIS CCSC (CisCSC Critical Security Control) dove CIS è Center for Internet Security. Il CIS è la community americana che si propone di definire e promuove le best practices sulla sicurezza informatica.

In particolare i primi 5 CIS Control sono i fondamentali e tutti gli altri devono seguire questi. I primi 5 controlli di AGID (ABSC AgidBased Security Control) corrispondono esattamente ai primi 5 controlli CIS:

- ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Per la scelta degli ultimi 3 si è fatto riferimento alla situazione attuale, visto l'elevato rischio di danni causati dai recenti malware. Il sesto punto riguarda infatti le difese dai malware. Il settimo riguarda le copie di sicurezza (backup) e l'ultimo la cifratura dei dati.

- ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
- ABSC 10 (CSC 10): COPIE DI SICUREZZA

- ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Per la definizione dei controlli si è anche fatto riferimento al Framework nazionale per la cybersecurity pubblicato ad inizio del 2016. Quest'ultimo a sua volta si fonda sul noto "Framework for Improving Critical InfrastructureCybersecurity" emanato dal NIST (Americano). Anche in questo caso a ciascun controllo ABSC definito da Agid corrisponde un controllo FNSC del Framework nazionale italiano, la corrispondenza viene specificata aggiungendo la colonna FNSC nelle tabelle delle misure di AGID.

Osservazioni

Di questo documento si apprezza il riferimento diretto a standard nazionali ed internazionali che danno garanzia di omogeneità e di correttezza.

L'obiettivo di queste misure minime di sicurezza è **la prevenzione alla perdita di dati causata da attacchi informatici** piuttosto che da eventi naturali, non si sono considerati aspetti di risposta ad un incidente e ripristino.
Per questo i primi 2 punti sono volti a rilevare e prontamente bloccare sia nuovi dispositivi che nuovi software. Il controllo 4 prevede l'analisi delle vulnerabilità che sono proprio i punti deboli sfruttati da malintenzionati. Anche il controllo 8 relativo ai sistemi antivirus vuole essere una difesa contro tentativi di violazione dei dati fraudolenta.

Come dichiarato all'interno delle Misure Minime Sicurezza ICT per le PA ", il documento, che contiene le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni e **costituisce parte integrante delle Linee Guida per la Sicurezza ICT delle PP.AA,** viene pubblicato, in attuazione della Direttiva sopra citata, come **anticipazione** urgente della regolamentazione in corso di emanazione".
Quindi si prevedono prossimamente ulteriori indicazioni normative.