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)». (17A03060)

(GU n.103 del 5-5-2017)

Vigente al: 5-5-2017

Premessa.

L'art. 14-bis del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera a), tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonche' 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.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovra' rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia e' parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017).

Art. 1

Scopo

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

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3

Attuazione delle misure minime

Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilita' della attuazione delle misure minime di cui all'art. 1.

Art. 4

Modulo di implementazione delle MMS-PA

Le modalita' con cui ciascuna misura e' 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 dovra' 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.

Art. 5

Tempi di attuazione

Entro il 31 dicembre 2017 le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

Roma, 18 aprile 2017

Il Presidente: Samaritani

Allegato 1

Parte di provvedimento in formato grafico

1. GENERALITA'.

1.1. Scopo.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

Questo documento e' emesso in attuazione della direttiva del Presidente del Consiglio dei ministri 1° agosto 2015 e costituisce un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

Parte di provvedimento in formato grafico

2. PREMESSA.

La direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacita' di risposta delle singole amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della pubblica amministrazione, sollecita tutte le amministrazioni e gli organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel piu' breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. A fine di agevolare tale processo l'Agenzia per l'Italia digitale e' stata impegnata a 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 e' parte.

L'Agenzia e' costantemente impegnata nell'aggiornamento continuo della normativa tecnica relativa alla sicurezza informatica della pubblica amministrazione ed in particolare delle regole tecniche per la sicurezza informatica delle pubbliche amministrazioni la cui emanazione e' pero' di competenza del Dipartimento per la funzione pubblica e richiede l'espletamento delle procedure previste dalla normativa comunitaria per la regolamentazione tecnica. Pertanto il presente 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 pubbliche amministrazioni, viene pubblicato, in attuazione della direttiva sopra citata, come anticipazione urgente della regolamentazione in corso di emanazione, al fine di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilita' per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro e' in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), e' ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. E' comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si e' partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

In realta' nel definire gli AgID Basic Security Control(s) (ABSC) si e' partiti dal confronto tra le versioni 6.0 e 5.1 dei CCSC, che puo' essere assunto quale indicatore dell'evoluzione della minaccia cibernetica nel corso degli ultimi anni. E' infatti evidente l'aumento di importanza delle misure relative agli amministratori di sistema, che balzano dal 12° al 5° posto, entrando nella rosa dei Quick Win, mentre la sicurezza applicativa scivola dal 6° al 18° posto e gli accessi wireless dal 7° al 15° a causa della diffusione delle contromisure atte a contrastare le vulnerabilita' tipiche di tali ambiti.

In definitiva, anche per facilitare il confronto con la definizione originale, si e' deciso di fare riferimento, nell'identificazione degli ABSC, alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli definiti e' piu' vicino a quello della versione 5.1 poiche' si e' ritenuto che molti di quelli che nel passaggio alla nuova versione sono stati eliminati, probabilmente perche' non piu' attuali nella realta' statunitense, siano ancora importanti nel contesto della pubblica amministrazione italiana.

Occorre inoltre osservare che il CCSC e' stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualita' quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime cinque classi si e' deciso di aggiungere quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfiltrazione.

In realta' ciascun CSC e' costituito da una famiglia di misure di

dettaglio piu' fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realta' locale. Nonostante cio' si e' ritenuto che anche al secondo livello ci fosse una granularita' ancora eccessiva, soprattutto sotto il profilo implementativo, che avrebbe costretto soprattutto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione. Per tale ragione e' stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente. Pertanto un ABSC e' identificato da un identificatore gerarchico a tre livelli x, y, z, dove x e y sono i numeri che identificano il CSC concettualmente corrispondente e z individua ciascuno dei controlli di livello 3 in cui questo e' stato raffinato.

Al primo livello, che corrisponde ad una famiglia di controlli destinati al perseguimento del medesimo obiettivo, e' associata una tabella che li contiene tutti. Nella prima colonna, sviluppata gerarchicamente su tre livelli, viene definito l'identificatore univoco di ciascuno di essi. La successiva colonna «Descrizione» specifica il controllo attraverso una definizione sintetica.

Nella terza colonna, «FNSC» (Framework nazionale di sicurezza cibernetica), viene indicato l'identificatore della Subcategory del Framework Core del Framework nazionale per la Cyber Security, proposto con il 2015 Italian Cyber Security Report del CIS «La Sapienza» presentato lo scorso 4 febbraio 2016, al quale il controllo e' riconducibile. Pur non intendendo costituire una contestualizzazione del Framework, le misure minime concretizzano praticamente le piu' importanti ed efficaci azioni che questo guida ad intraprendere. Per il diverso contesto di provenienza ed il differente obiettivo che i due strumenti intendono perseguire, le misure minime pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino.

Le ultime tre colonne sono booleane e costituiscono una linea guida che indica quali controlli dovrebbero essere implementati per ottenere un determinato livello di sicurezza. La prima, «Minimo», specifica il livello sotto il quale nessuna amministrazione puo' scendere: i controlli in essa indicati debbono riguardarsi come obbligatori. La seconda, «Standard», puo' essere assunta come base di riferimento nella maggior parte dei casi, mentre la terza, «Alto», puo' riguardarsi come un obiettivo a cui tendere.

Il raggiungimento di elevati livelli di sicurezza, quando e' molto elevata la complessita' della struttura e l'eterogeneita' dei servizi erogati, puo' essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni amministrazione dovra' avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneita' di requisiti ed obiettivi di sicurezza, all'interno dei quali potra' applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

Le amministrazioni NSC, per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti piu' elevati.

3. LA MINACCIA CIBERNETICA PER LA PUBBLICA AMMINISTRAZIONE.

Nel recente passato si e' assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che e' divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

Se da un lato la pubblica amministrazione continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attivita' condotte da gruppi organizzati, non solo di stampo propriamente criminale.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi. Il primo e' la quantita' di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati. Il secondo e' che il primo obiettivo perseguito e' il

mascheramento dell'attivita', in modo tale che questa possa procedere senza destare sospetti. La combinazione di questi due fattori fa si' che queste misure minime, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attivita' degli utenti rimangano sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi piu' pericolosi e' l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario e' avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, per la mancanza di log, modifiche di configurazione e anche avvicendamenti del personale, l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti efficaci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e cio' rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonche' la protezione della configurazione, che e' quella immediatamente successiva.

La quarta classe deve la sua priorita' alla duplice rilevanza dell'analisi delle vulnerabilita'. In primo luogo le vulnerabilita' sono l'elemento essenziale per la scalata ai privilegi che e' condizione determinante per il successo dell'attacco; pertanto la loro eliminazione e' la misura di prevenzione piu' efficace. Secondariamente si deve considerare che l'analisi dei sistemi e' il momento in cui e' piu' facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe e' rivolta alla gestione degli utenti, in particolare gli amministratori. La sua rilevanza e' dimostrata dall'ascesa, accennata in premessa, dal 12° al 5° posto nelle SANS 20, motivata dalle considerazioni cui si e' fatto riferimento poco dianzi.

La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione puo' impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.

L'ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi piu' gravi e' la sottrazione di informazioni.

Parte di provvedimento in formato grafico

Allegato 2

Parte di provvedimento in formato grafico