PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4993 di Venerdì 06 agosto 2021

Pubblicata una attraente guida alla sicurezza informatica

Sulla Gazzetta Ufficiale dell'11 giugno 2021, il governo ha pubblicato un complesso documento, nel quale è inserito un elenco di misure minime di sicurezza informatica e cartacea, che può risultare utile per qualsiasi azienda.

I lettori mi perdonino se affronto l'argomento, prendendo il tema un po' alla larga. Ricordo a tutti che l'Italia, in ottemperanza precise indicazioni provenienti dall'Europa, ha definito tutta una serie di misure di sicurezza informatica, applicabili a tutti gli enti, pubblici o privati, che esercitano attraverso reti, sistemi informativi e servizi informatici, 223 funzioni essenziali dello Stato, ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche. Queste aziende sono state inserite all'interno di un perimetro di sicurezza informatica. Allo stesso tempo, si è provveduto ad un affinamento di alcune funzioni e servizi essenziali dello Stato già ricompresi nel perimetro.

L'elenco delle 223 funzioni essenziali dello Stato è stato recentemente aggiornato, pubblicando un nuovo elenco dei soggetti inseriti del "perimetro di sicurezza cibernetica nazionale". È stato, così, previsto un allargamento dell'ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che, complessivamente, esercitano, funzioni ritenute critiche per la sicurezza nazionale.

Nei prossimi giorni, il Dipartimento delle informazioni per la sicurezza provvederà a darne comunicazione agli interessati che, entro sei mesi, saranno tenuti a comunicare le reti, i sistemi informativi ed i servizi informatici che impiegano rispettivamente per l'erogazione delle funzioni e dei servizi essenziali dello Stato, inclusi nel perimetro.

Ecco un breve ripasso del calendario della sicurezza nazionale cibernetica:

- il 22 dicembre 2020 il governo ha pubblicato un elenco di soggetti, cui si applicano determinati requisiti di sicurezza informatica,
- l'11 giugno 2021 in Gazzetta Ufficiale è apparso l'elenco delle misure di sicurezza e la tassonomia degli incidenti coinvolti,
- il 23 giugno 2021 questi soggetti dovranno cominciare ad applicare questi requisiti,
- il 31 dicembre 2021 è la data ultima entro la quale tutte le misure pubblicate dovranno essere applicate e pienamente operative.

Il documento in cui troviamo preziose indicazioni sulle misure minime di sicurezza da adottare in un sistema informativo, anche indipendentemente dal fatto che esso sia inserito in questo elenco nazionale, è costituito dall'allegato C, art.9, *al DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81. Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b) , del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.*

Riporto di seguito alcuni commenti specifici.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

1. Trattamenti con l'ausilio di strumenti elettronici

a) Identificazione degli utenti e gestione delle identità digitali;

b) determinazione dei privilegi di accesso alle risorse da associare agli utenti e agli addetti o incaricati alla gestione o alla manutenzione;

c) implementazione di un sistema di autenticazione e autorizzazione degli utenti secondo i privilegi individuati al punto precedente;

i tre punti soprastanti rappresentano fondamentali ed elementari misure di sicurezza, che obbligano il responsabile di un sistema informativo ad identificare i soggetti che accedono ed a stabilire dei profili di accesso, secondo l'ormai noto criterio della autorizzazione a creare, leggere, modificare i dati.

d) protezione contro il software malevolo mediante l'impiego di software antimalware aggiornato

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

i due punti soprastanti fanno riferimento all'obbligo di adottare appropriati ed aggiornati dispositivi antivirus, ivi compresi applicativi di blocco dell'accesso di programmi o collegamenti provenienti da aree non autorizzate;

f) procedure di sicurezza per l'importazione e l'esportazione dei dati sui sistemi impiegati;

questo punto può fare certamente riferimento alle situazioni di sicurezza che occorre rispettare se vengono autorizzati i dispositivi del tipo Bring your own device ? BYOD, o l'utilizzo di dispositivi di memoria portatili

g) procedure per la gestione della configurazione dei sistemi impiegati;

h) procedure per la dismissione dei dispositivi di memorizzazione utilizzati sui sistemi impiegati;

è un argomento su cui numerose autorità sensibili su temi di sicurezza, in particolare l'autorità garante per la protezione dei dati personali, hanno numerose volte cercato di sensibilizzare i responsabili di sistemi informativi, che talvolta non sono sufficientemente diligenti, in fase di dismissione di apparati informatici o circolazione di supporti di memoria,

i) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

penso sia inutile ricordare a tutti i lettori come questa sia la più efficiente ed efficace procedura contro attacchi per ransomware

l) adozione di tecniche di cifratura.

Anche in questo caso, la adozione di tecniche di cifratura di buon livello rappresenta una efficiente ed efficace protezione contro la perdita di dati, sia origine accidentale, sia di origine criminosa.

2. Misure di sicurezza fisica e documentale

a) L'accesso alle informazioni è consentito sulla base del principio della necessità di conoscere (need to know);

questo principio fondamentale deve essere mantenuto costantemente aggiornato, soprattutto quando un addetto al trattamento di dati viene spostato da una posizione ad un'altra, senza provvedere ad un appropriato aggiornamento del suo profilo

b) deve essere individuata la figura di un responsabile incaricato della gestione delle informazioni, preferibilmente già in possesso di abilitazione di sicurezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124;

è questa una specifica che vale solo nel contesto di sistemi inseriti nel regolamento che stiamo esaminando, ma la raccomandazione di avere un responsabile incaricato della gestione delle informazioni, con adeguate competenze, è senz'altro estendibile alla gestione di qualsiasi sistema informativo

c) la documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedura di tracciamento delle chiavi in uso;

il lettore non pensi che questa misura di sicurezza valga solo per i supporti cartacei, ma vale anche per particolari supporti di memoria, ad esempio i supporti di memoria di backup, che risultano così più difficilmente accessibili ad attacchi di ransomware; al proposito, ricordo che tanta attenzione bisogna prestare le chiavi elettroniche o password, quanta va prestata alle chiavi fisiche;

d) la documentazione deve essere registrata su appositi registri di protocollo;

e) la consultazione dei documenti deve avvenire sulla base del principio della necessità di conoscere (need to know) e deve essere tracciata su apposito registro;

f) la riproduzione dei documenti può avvenire solo previa autorizzazione del responsabile della gestione delle informazioni e deve essere registrata su apposito registro;

g) la documentazione deve essere spedita tramite corrieri.

I punti soprastanti fanno riferimento alla corretta gestione di documentazione cartacea, che spesso non viene protetta con la stessa diligenza, che viene posta nella protezione della documentazione informatica. Mi permetto di aggiungere, con riferimento al punto g), che non solo la documentazione deve essere spedita tramite corrieri, ma deve anche essere racchiusa in contenitori dotati di sigillo di garanzia, in grado di mettere in evidenza qualunque tentativo di apertura durante il transito.

Infine, faccio presente ai lettori che questo elenco è stato osservato con molta attenzione dalle compagnie di assicurazione, che si occupano di polizze informatiche, perché potrebbe costituire un prezioso punto di riferimento, in fase di valutazione del rischio di un aspirante assicurato.

Adalberto Biasiotti

Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81 Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it