PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4556 di Mercoledì 09 ottobre 2019

Perimetro di sicurezza nazionale cibernetica: che significa?

Il 21 settembre 2019 è stato approvato decreto-legge numero 105, afferente disposizioni urgenti in materia di sicurezza nazionale cibernetica. Vediamo insieme i problemi che questo decreto affronta.

Il Consiglio dei ministri, su proposta del Presidente Giuseppe Conte, ha approvato il DECRETO-LEGGE 21 settembre 2019, n. 105. - *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica,* che introduce disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. Il decreto mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Inoltre, il testo integra e adegua il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo, con particolare riferimento a quanto previsto dal decreto-legge 15 marzo 2012, n. 21, in modo da coordinare l'attuazione del Regolamento (UE) 2019/452, sul controllo degli investimenti esteri, e apprestare idonee misure di tutela di infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione del decreto-legge 15 marzo 2012, n. 21.

Le nuove norme, tra l'altro:

- definiscono le finalità del perimetro e le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica;
- prevedono il coinvolgimento del Comitato interministeriale per la sicurezza della Repubblica (CISR) nella fase attuativa;
- istituiscono un meccanismo teso ad assicurare un procurement più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di information and communication technology (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;
- prevedono che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate ai sensi del decreto-legge 15 marzo 2012, n. 21, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

A questo punto, vediamo come questo decreto-legge coinvolge i responsabili della sicurezza informatica, a livello locale e nazionale.

Tanto per cominciare, non dimentichiamo che un decreto-legge è sempre passibile di modifica, all'atto della conversione in legge, e conviene pertanto attenersi alle disposizioni del decreto-legge, con una certa prudenza, se gli investimenti coinvolti sono significativi. La conversione in legge infatti potrebbe portare modifiche.

Cominciamo innanzitutto ad esaminare a quali personaggi ed a quali strutture il decreto-legge si applica. L'articolo 1 precisa quanto segue:

Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica.

Il governo si è riservato un lasso di tempo di quattro mesi per poter individuare con accuratezza quali siano i soggetti e le attività, cui il decreto si applica. Ecco perché è meglio non affrettarsi, salvo casi conclamati.

Successivamente il decreto elenca quali siano gli obblighi cui sono assoggettati questi soggetti, ancora da individuare, mettendo subito in evidenza l'obbligo di segnalare incidenti informatici. È questo un aspetto fondamentale nella gestione della sicurezza informatica, che è stato ripreso senza significative varianti dalle disposizioni regolamento generale sulla protezione dati personali, che appunto impone un obbligo generalizzato di segnalare incidenti, sia di natura dolosa, sia corposa, salvo eccezioni ben precise.

Più impegnativa diventa la disposizione afferente al fatto che chi rientra nel perimetro di sicurezza nazionale cibernetica deve non solo rispettare tutt'una serie di norme specifiche, ma deve anche affidarsi solo a fornitori di beni e servizi che diano certe garanzie. In particolare, il Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, può, entro trenta giorni, imporre condizioni e test di hardware e software.

Queste condizioni debbano poi essere inserite in bandi di gara e capitolati di fornitura, creando quindi un elenco di fornitori di beni e servizi che soddisfino i requisiti previsti dal decreto. Nell'esperienza di chi scrive, i tempi necessari per sviluppare queste attività certamente non sono brevi ed è questo il motivo per cui ritengo che l'applicazione pratica di questo decreto non sarà solo legata ai tempi di conversione in legge, ma anche ai tempi necessari per mettere a disposizione strumenti cibernetici a sicurezza certificata.

Un altro elemento garantistico, messo in evidenza dal decreto, riguarda la effettuazione di ispezioni, perché è ben noto che l'emanazione di regole, senza poi attivare adeguati programmi di verifica, lascia il tempo che trovano. Anche in questo caso, la disponibilità di ispettori aventi le necessarie ed elevate qualifiche potrebbe non essere così immediata ed allargata, come forse il Consiglio dei Ministri vorrebbe.

Il comma 9 dell'articolo 1 è tutto dedicato all'elencazione delle sanzioni economiche, che sono indubbiamente significative, in allineamento con i crescenti massimali, previsti ad esempio dello stesso regolamento generale per la protezione dei dati personali.

Forse su sollecito del presidente degli Stati Uniti, l'articolo *3. Disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5G,* è tutto dedicato a queste nuove tecnologie, i cui criteri di sicurezza rappresentano ancora una relativa incognita.

L'articolo 4 si applica alle infrastrutture tecnologie critiche, che erano state già prese in considerazione nella legge 11 maggio 2012, numero 56. Tuttavia, si allarga notevolmente il bacino di applicazione di queste disposizioni, perché esse si applicano non solo a sistemi informativi afferenti alla sicurezza ed all'ordine pubblico, ma anche ad altri sistemi, che in qualche modo possano impattare sul regolare funzionamento della società civile.

Infine, è suggestiva la lettura dell'articolo 5, che prende in considerazione crisi di natura cibernetica.

In considerazione del fatto che questo articolo attribuisce al presidente del consiglio poteri oltremodo allargati, è del tutto naturale che tali poteri possano essere esercitati solamente dopo che il presidente abbia sentito il parere degli esperti di settore, vale a dire il Comitato interministeriale per la sicurezza della Repubblica.

Questo decreto-legge, in poche parole, non fa altro che recepire l'assunto, ormai generalizzato, circa il fatto che la sicurezza informatica rappresenti un aspetto essenziale della vita di una qualunque attività, sia pubblica sia privata, sia a grandissimo impatto sulla società civile, sia anche ad impatto relativamente limitato.

Ormai una azienda, pubblica o privata, che non prenda in sufficiente considerazione la sicurezza dei propri sistemi informativi, si espone a gravi rischi e questi rischi possono coinvolgere sia l'azienda stessa, sia, in molti casi, l'intera società civile.

Ancora una volta, la sicurezza informatica richiede l'adozione di misure di valutazione, prevenzione e messa sotto controllo, in perfetta armonia con le modalità di individuazione, gestione e messa sotto controllo di un rischio qualsivoglia, sia esso un furto, rapina od una infedeltà.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it