SICUREZZA INFORMATICA

La protezione dal rischio di gravi attacchi cibernetici: le misure minime da adottare nella PA

Il Servizio nazionale della Protezione civile è stato istituito anche al fine di tutelare l'integrità della vita, i beni, gli insediamenti e l'ambiente dai danni o dal pericolo di danni derivanti da calamità naturali, da catastrofi e da altri eventi calamitosi. Siamo abituati a pensare che gli eventi e le calamità naturali, ovvero gli altri eventi connessi con l'attività dell'uomo, che la legge istitutiva del Servizio indica come attività di cui si deve occupare la Protezione civile, consistano in terremoti, frane, alluvioni e nei contesti in cui tipicamente operano gli addetti al servizio.
Abbiamo visto però che, soprattutto nei tempi più recenti, occorre tenere nel dovuto conto anche le problematiche derivanti da attacchi cibernetici, come li definisce la normativa vigente e che nel linguaggio giornalistico troviamo descritti come cyberattacks o attacchi da parte di hackers

Le potenziali conseguenze di attacchi informatici come quello che la scorsa primavera ha messo a dura prova il servizio sanitario nazionale inglese e i sistemi informatici di numerose organizzazioni pubbliche e private di decine di Paesi del mondo, hanno contribuito a mantenere acceso l'interesse sul fenomeno dei cyberattacks almeno da due punti di vista: da una parte il dato di fatto che l'attività della Protezione civile, anche negli ambiti tradizionali sopra richiamati, può essere effettuata solo attraverso servizi informatici ormai essenziali. Pertanto infezioni o intrusioni nei sistemi informatici possono porre in pericolo la stessa struttura organizzativa della Protezione civile, chiamata a erogare i suoi servizi.

Basta ricordare in proposito alcuni titoli di giornale: "Emergenza terremoto, il sito della Protezione civile sotto attacco hacker", riferito al caso del sito della PC del Molise, reso indisponibile durante l'emergenza terremoto che ha interessato il territorio di quella Regione, per rendersi conto dell'attualità di tali rischi. Dall'altra eventuali attacchi da parte di hacker su larga scala possono costituire di per sé eventi catastrofici, ormai assimilabili a quelli tradizionalmente di competenza della Protezione civile, perché i danni che attacchi di quel tipo possono provocare sono potenzialmente gravissimi e vanno assolutamente prevenuti con ogni sforzo e investimento. Del resto, di fronte agli attacchi che hanno preso di mira diverse strutture sanitarie, come accaduto di recente nel Regno Unito, è immediatamente percepibile la gravità dei rischi da fronteggiare, potendo i danni arrecati alle strutture informatiche provocare anche vittime o comunque gravi interruzioni di servizi essenziali.

Al riguardo la BBC ha di recente riportato che il Prof. Bill Buchanan, a capo del Centre for Distributed Computing and Security e della Cyber Academy, professore presso la School of Computing e l'Institute for Informatics and Digital Innovation (IIDI) presso la Edinburgh Napier University, intervistato sugli attacchi occorsi nel maggio scorso ad 11 istituzioni sanitarie in Scozia, ha affermato che la diffusione del virus Wannacry sarebbe stata evitabile. In particolare ha sottolineato che non è in alcun modo scusabile il fatto che alcune patch o upgrade non fossero state eseguite sui sistemi, aprendo in tal modo la via all'infezione. Da ciò la convinzione, pubblicamente espressa dal Prof. Buchanan, che l'incidente di sicurezza accaduto dovrebbe costituire un forte motivo di allarme, evidenziando l'esigenza di un'attenta revisione dell'infrastruttura IT del sistema socio-sanitario scozzese.

Del resto i problemi sono d'impatto enorme, anche sotto il profilo semplicemente economico, tanto che il sistema pubblico del Regno Unito spende all'anno circa 100 milioni di sterline solo per i programmi di gestione IT centralizzata nel settore sanitario, ai quali Andy Robertson, responsabile IT presso il National Services Scotland, ha proposto di aggiungere un investimento extra di ulteriori 15 milioni di sterline/anno. Se la proposta può apparire ad alcuni d'impatto rilevante, d'altra parte

l'importo è stato peraltro descritto come un puro e semplice 'sticking plaster' (un cerotto) sempre dal Prof. Buchanan, il quale ha affermato: "Penso sia necessario aggiungere uno zero, e poi forse un altro zero" alla cifra sopra quantificata.
Stiamo quindi discutendo, seppur su posizioni diversificate, di un problema molto attuale e di rilevanza cruciale, dalle ricadute potenzialmente enormi.

Per capire compiutamente di quale ordine di grandezza di somme si tratta, possiamo riportare quanto pubblicato su 'The Guardian' dello scorso 17 luglio, con riferimento agli esiti di uno studio dei Lloyd's di Londra, in base al quale si recepisce forte e chiaro l'avvertimento che un grave attacco cyber potrebbe costare all'economia globale più di 120 miliardi di dollari - ovvero tanto quanto sono costati disastri naturali catastrofici come gli uragani Katrina e Sandy - esempi quanto mai calzanti, visto che siamo in tema di Protezione civile.

Non è un caso, dunque, se la BBC riportava in data 14 febbraio scorso che, in occasione dell'inaugurazione del Centro per la Protezione Nazionale dai cyberattacks, è stato illustrato personalmente alla Regina Elisabetta come gli hackers potrebbero prendere di mira il sistema di trasmissione e fornitura dell'energia elettrica in UK. Il National Cyber Security Centre, che costituisce parte dell'Agenzia d'intelligence del GCHQ - Government Communications Headquarters ha iniziato la sua attività nell'ambito di un programma quinquennale di investimenti da 1 miliardo e 900 milioni di sterline, ha sede a Victoria, nel centro di Londra e sarà supportato anche dai migliori esperti del settore privato per cercare di identificare e prevenire le minacce, al fine di raggiungere l'obiettivo individuato dal capo del Centre, Ciaran Martin, il quale ha affermato: "Vogliamo fare in modo che il Regno Unito sia l'obiettivo più difficile da raggiungere".

Da Inghilterra e Scozia all'Italia: come si è attrezzato e si sta adeguando il nostro paese per proteggersi dai rischi di attacchi informatici?
Con riferimento specifico alla Pubblica amministrazione, lo scorso 18 aprile nel nostro Paese è stata adottata la circolare n. 2/2017 dell'Agenzia per l'Italia Digitale, recante 'Misure minime di sicurezza ICT per le pubbliche amministrazioni', con l'avvertimento che 'la presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017)' in attuazione della Direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015.

Entro fine anno dunque tutte le amministrazioni, sotto la responsabilità del dirigente preposto ai sistemi informativi dell'organizzazione o alla sua digitalizzazione, dovranno adottare le misure minime, elencate nella circolare e tratte dall'insieme di controlli noto come SANS 20 (SysAdmin, Audit, Networking, and Security), ovvero dalla fonte più affidabile e di gran lunga la più importante per la formazione sulla sicurezza informatica nel mondo, controlli oggi pubblicati dal Center for Internet Security come CCSC 'CIS Critical Security Controls for Effective Cyber Defense' nella versione 6.0 dell'ottobre 2015.

Le Misure Minime, denominate AgID Basic Security Controls (ABSC) predisposte in base ai cosiddetti CSC (Critical Security Controls), sono state adattate alla specifica realtà nazionale italiana, fatta anche di piccole articolazioni di cui la pubblica amministrazione si compone, e sono state suddivise come segue:
■ controlli del primo gruppo (livello 'Minimo') sono quelli strettamente obbligatori che ogni Pubblica Amministrazione deve attivare, indipendentemente dalla sua natura e dimensione, rappresentando il livello al di sotto del quale nessuna Amministrazione può scendere;
■ controlli del secondo gruppo (livello 'Standard') rappresentano la base di riferimento per la maggior parte delle Amministrazioni e costituiscono un ragionevole compromesso fra l'efficacia delle misure preventive e l'onerosità della loro implementazione;

■ controlli del terzo gruppo (livello ‘Alto’) rappresentano infine il livello adeguato per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati e può riguardarsi come un obiettivo a cui tendere.

Le Misure Minime prevedono, nella loro formulazione attuale, otto insiemi di controlli.

ABSC1 (CSC1): inventario dei dispositivi autorizzati e non autorizzati e
ABSC2 (CSC2): inventario dei software autorizzati e non autorizzati

I controlli delle prime due classi riguardano rispettivamente l’inventario Hardware (ovvero di tutti i sistemi di rete (compresi i dispositivi di rete stessi) registrando almeno l’indirizzo IP e quello dei Software autorizzati (e relative versioni), imponendo come misura minima che gli inventari siano dinamici, vale a dire predisponendo e mantenendo aggiornati i rispettivi inventari, al fine di individuare e/o impedire tutte le anomalie operative. L’installazione di software non presenti nell’elenco è vietata.

ABSC3 (CSC3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

I controlli della terza classe riguardano la protezione delle configurazioni hardware e software sui sistemi in uso presso l’organizzazione, con il tassativo rispetto di tali standard impostati nelle fasi di installazione o ripristino dei sistemi.

ABSC4 (CSC4): valutazione e correzione continua della vulnerabilità

I controlli della quarta classe sono finalizzati alla ricerca e all’individuazione tempestiva, in vista della loro correzione, delle vulnerabilità dei sistemi in uso, che sono l’elemento essenziale per il successo dell’attacco e la cui eliminazione preventiva costituisce la misura di prevenzione più efficace. Questa classe di controlli impone l’installazione sistematica di patch e contromisure idonee a contrastare le vulnerabilità riscontrate. Inoltre l’analisi delle vulnerabilità dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute nei sistemi e rilevare l’esistenza di un attacco in corso.

ABSC5 (CSC5): uso appropriato dei privilegi di amministratore

I controlli della quinta classe sono rivolti agli amministratori di sistema e impongono l’adozione di una policy di gestione degli utenti con diritti amministrativi. L’importanza dei controlli è testimoniata dall’ascesa dal 12° al 5° posto nelle SANS 20, visto anche il loro fine di assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi sui sistemi in uso (controlli sulle scadenze delle password alla creazione di profili nominativi).

ABSC8 (CSC8): difese contro i malware

I controlli della sesta classe impongono l’installazione e l’aggiornamento automatico di sistemi antimalware, firewall e Intrusion Prevention Systems (IPS) in considerazione del fatto che anche gli attacchi complessi prevedono in qualche fase l’installazione di codice malevolo. I controlli hanno lo scopo di contrastare l’ingresso e la diffusione nell’organizzazione di tali codici, in modo che la loro individuazione possa impedirne il successo o rilevarne la presenza. Sempre in chiave preventiva, si

deve prevedere l’adozione di strumenti filtraggio dei contenuti, sia sulla navigazione Internet che sulla posta elettronica.

ABSC10 (CSC10): copie di sicurezza

I controlli della settima classe sono relativi alla gestione delle copie di sicurezza delle informazioni critiche dell’organizzazione, che sono l’unico strumento che garantisce il ripristino dopo un incidente e impone l’esecuzione di una copia almeno settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema (in linea con le misure minime di sicurezza previste dal Codice della Privacy, anche se perdere una settimana di lavoro potrebbe essere troppo penalizzante per una PA).

ABSC13 (CSC13): protezione dei dati

L’ottava e ultima classe riguarda infine la protezione contro l’esfiltrazione dei dati, visto che l’obiettivo principale degli attacchi resta quello della sottrazione di informazioni.
Il sistema di controlli stabilisce di effettuare un’analisi dei dati per individuare quelli con particolari requisiti di riservatezza, ai quali applicare una protezione crittografica.

La norma attuativa prevede che ciascuna Amministrazione oltre a implementare i controlli rilevanti, debba anche dare brevemente conto della modalità di implementazione, compilando un apposito modulo da firmare digitalmente e da conservare a cura dell’Amministrazione stessa.

Il livello Standard prevede ulteriori azioni da svolgere per garantire la sicurezza dei sistemi, ma come approccio iniziale sarebbe corretto che le PA verificassero il proprio ‘stato di salute’ attraverso specifici risk assessment informatici, e in particolare per mezzo di adeguati vulnerability test, per valutare eventuali azioni correttive da compiere, al fine di ottemperare agli obblighi imposti dal legislatore al livello minimo di sicurezza informatica imposta. E soprattutto al fine di consentire una difesa nazionale di una certa consistenza ed efficacia, basata sul rafforzamento dei sistemi locali e su policies e misure che consentano di limitare al massimo gli attacchi che hanno successo e la diffusione d’infezioni e intrusioni.

Di tutto questo, oltre che dei riflessi sugli adempimenti di sicurezza informatica che le normative in materia di privacy (Regolamento (UE) 679/2016), di sicurezza dei sistemi (Direttiva UE NIS 1148/2016 (Network and Information Security)) e di responsabilità amministrativa degli Enti (D.Lgs. n. 231/2001) impongono o suggeriscono a breve scadenza, si è potuto trattare nel recente convegno del 13.07.2017 u.s., organizzato dalla rete **Doctis** a Montecchio Maggiore (VI), al quale **Italica Forensis*** ha preso parte, illustrando ai presenti i profili legali ed informatici di maggior rilievo per dotarsi dei presidi più efficaci e per limitare al massimo i rischi di attacchi. I prossimi mesi saranno decisivi per verificare chi e come si sarà adeguato alle prescrizioni in materia di sicurezza informatica, con la speranza di poter prevenire eventi disastrosi, anche su vasta scala.

* con l’avvocato **Silvio Regis** e l’esperto in cybersecurity **Carloalberto Sartor**

(Pubblicato su LaProtezioneCivile, settembre 2017)