Alert
Corporate - Review

Cybersecurity ed imprese

SISTEMI DI SICUREZZA INFORMATICA E CERTIFICAZIONI

Sistemi di sicurezza informatica: obbligo o semplice cautela?

Di fronte all'accresciuto attivismo degli *hacker* ed all'aumento dei crimini cibernetici, le imprese si trovano ad investire sempre di più nella *cybersecurity*: ma – la domanda è d'obbligo – vi sono in qualche modo tenute o lo fanno esclusivamente su base volontaria?

Ebbene, per alcuni settori ciò risponde ad uno specifico obbligo di legge. Il riferimento è, ad esempio, ai c.d. **operatori di servizi essenziali (OSE)**, ossia quei soggetti – pubblici o privati – che forniscono servizi nei settori di energia, trasporti, banche e infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; ed ai **fornitori di servizi digitali** [1].

Più specificamente, gli OSE[2] ed i fornitori di servizi digitali sono tenuti all'adozione di misure atte a garantire la sicurezza dei sistemi di rete e di informazione, nonché a prevenire e minimizzare l'impatto di eventuali incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati, al fine di assicurare la continuità dei servizi. Inoltre, in caso di incidente – per tale intendendosi un evento con effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi – avente un impatto sulla continuità dei servizi essenziali forniti, è previsto un obbligo di notifica al CSIRT (gruppo di intervento per la sicurezza informatica in caso di incidente) ed all'autorità competente NIS.

Se si esclude il caso degli OSE e dei fornitori di servizi digitali – e fermi restando gli analoghi obblighi posti a presidio, ad esempio, della sicurezza dei dati privati[3] - può ragionevolmente sostenersi che le imprese siano del tutto esenti da obblighi in ambito di *cybersecurity*?

Tipicamente un *cyberattack* può avere varie finalità che vanno dallo spionaggio industriale all'estorsione: una società non adeguatamente presidiata, quindi, rischia di lasciare alla mercé degli hacker il cuore della propria attività (si pensi alle imprese ad alta connotazione tecnologica), così come – ad esempio - informazioni commerciali e finanziarie riguardanti le proprie controparti contrattuali.

---

[1] D.Lgs. 18.5.2018, n. 65 di attuazione della direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6.7.2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[2] Gli OSE con sede sul territorio nazionale vengono identificati con periodicità almeno biennale dalle autorità competenti per settore in materia di sicurezza delle reti e dei sistemi informativi (NIS): l'elenco aggiornato degli OSE viene quindi trasmesso alla Commissione europea. Per ricadere nella definizione di OSE – oltre a dover operare in uno dei settori sopra indicati – occorre che i) il soggetto fornisca un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali; ii) la fornitura di tale servizio dipenda dalla rete e dai sistemi informativi; e iii) un incidente avrebbe effetti rilevanti sulla fornitura di tale servizio. La rilevanza degli effetti viene determinata in base – tra gli altri – al numero degli utenti che dipendono dal servizio fornito e dall'impatto che l'incidente potrebbe avere sulle attività economiche e sociali e sulla pubblica sicurezza.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR).

Alert
Corporate - Review

Rientra nella diligenza richiesta agli amministratori di società nell'assolvimento del proprio incarico l'assunzione di misure necessarie a salvaguardare l'integrità del patrimonio della società: pertanto, se a seguito di un attacco la società si vede sottrarre dei segreti industriali per via della mancanza o inadeguatezza delle misure protettive poste in essere, l'amministratore (negligente) può ragionevolmente essere chiamato a risponderne. La società, a sua volta, è essa stessa potenzialmente passibile di un'azione risarcitoria nel caso in cui l'attacco *hacker* abbia avuto ad oggetto segreti industriali e/o informazioni riservate di una propria controparte contrattuale (sempre che quest'ultima abbia sofferto un danno per effetto diretto della loro diffusione): e questo a titolo di responsabilità contrattuale – quando ad esempio l'ipotesi dell'incidente sia espressamente disciplinata da accordi di riservatezza vigenti tra le parti, o comunque in virtù del generico obbligo di comportarsi secondo diligenza e buona fede che grava sulle parti di un contratto – ovvero di responsabilità extra-contrattuale, in base al generico principio del *neminem laedere* (e cioè del dovere che grava su ciascuno di noi di non arrecare un danno ingiusto a terzo per effetto della nostra condotta).

Quindi può sostenersi che le società ed i loro amministratori siano di massima tenuti a dotarsi di sistemi di *cybersecurity* (nei limiti di quanto lo richieda l'attività svolta): e questo sia a tutela del proprio patrimonio (in)tangibile, sia al fine di evitare di causare colpevolmente danni a terzi. Non grava, invece, sulle stesse l'obbligo di notifica di eventuali incidenti espressamente previsto per gli OSE ed i fornitori di servizi digitali; anche se la legge prevede espressamente che soggetti diversi dagli OSE e dai fornitori di servizi digitali possano provvedervi su base volontaria.

Certificazioni

"*Il mercato unico digitale, in particolare l'economia dei dati e l'Internet degli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un determinato livello di cbersicurezza*": muovendo da questa constatazione il *Cybersecurity Act*[4] ha istituito il quadro europeo di certificazione della cibersicurezza. In tale contesto è previsto che vengano istituiti sistemi di certificazione della cibersicurezza in base ai quali gli organismi pertinenti possano attestare la conformità a determinati requisiti di sicurezza di prodotti, servizi e processi TIC (tecnologia dell'informazione e della comunicazione) mediante il rilascio di appositi certificati europei di cibersicurezza. I primi sistemi di certificazione riguarderanno proprio i settori in cui sono attivi gli OSE.

Sono previsti tre livelli di affidabilità: "di base", "sostanziale" e "elevato" che si differenziano tra loro perché i relativi prodotti, servizi e processi sono stati valutati ad un livello inteso a ridurre al minimo, rispettivamente:

[4] Regolamento (UE) 2019/881 del 17.4.2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

i) i rischi di base noti di incidenti e attacchi informatici;
ii) i rischi di attacchi informatici causati da soggetti dotati di abilità e risorse limitate; e
iii) i rischi di attacchi informatici avanzati commessi da attoriche dispongono di abilità e risorse significative.

È altresì consentita, per fabbricatori e fornitori, l'autovalutazione - sotto la propria responsabilità - della conformità di prodotti, servizi e processi TIC che presentino un rischio corrispondente al livello di affidabilità "di base".

La certificazione avviene su base volontaria: tuttavia recentemente il Parlamento Europeo ha invitato la Commissione a valutare la necessità di introdurre certuni requisiti di obbligatorietà in materia di *cybersecurity* per i prodotti di consumo[5]. È pur vero, comunque, che man mano che si affermeranno le certificazioni – pure se su base volontaria – il mercato le renderà di fatto obbligatorie, giacché la scelta dei fruitori si orienterà inevitabilmente verso i prodotti, servizi e processi certificati.

L'introduzione di un sistema europeo di certificazione di cibersicurezza e la conseguente armonizzazione dei sistemi nazionali di certificazione (quando esistenti) rappresenta un significativo passo in avanti. Anzitutto perché scongiura la scelta della certificazione più vantaggiosa in base ai diversi livelli di rigore esistenti nei singoli Stati: e quindi perché solleva le imprese dalla necessità di chiedere certificazioni nei diversi Stati in cui intendano operare (con conseguente risparmio di costi).

Fin qui la certificazione di prodotti, servizi e processi: ma che dire delle imprese che li producono e forniscono? Esiste una certificazione che attesti l'adeguatezza delle misure di cibersicurezza poste in essere?

La nostra libertà e la nostra prosperità dipendono sempre più dalla solidità e dall'innovazione di internet … Ma la libertà online presuppone la sicurezza. È necessario che il ciberspazio sia protetto da incidenti, attività dolose e abusi.[6] Questo vale tanto per i cittadini quanto per le imprese, anche se la normativa di derivazione comunitaria in materia di *cybersecurity* per il momento guarda alle seconde soprattutto in chiave di tutela dei primi. In altre parole, almeno in tema di certificazioni, si predilige il B2C rispetto al B2B.

È pur vero che, come si è visto, sono previsti specifici obblighi in capo agli OSE ed ai fornitori di servizi digitali: ma questi sono finalizzati a garantire la sicurezza dello Stato e dei suoi cittadini e comunque nulla è previsto dalla normativa di derivazione comunitaria in materia di certificazione circa l'adeguatezza dei sistemi di sicurezza informatica adottati dalle imprese. L'unica disciplina che viene in soccorso al riguardo è quella delle certificazioni ISO: ed in particolare quelle della c.d. famiglia 27k (*Information Security Management Systems*) e, ancor più nello specifico, la certificazione ISO 27.032 sulla *cybersecurity* (in fase di aggiornamento).

[5] Risoluzione del Parlamento europeo del 25 novembre 2020 sul tema "Garantire la sicurezza dei prodotti nel mercato unico"
[6] Comunicazione della Commissione del 7.2.2013 sulla strategia dell'UE per la cibersicurezza: un ciberspazio aperto e sicuro.

NUNZIANTE • MAGRONE

Alert

Corporate - Review

Le certificazioni delle imprese rivestono un ruolo fondamentale nello sviluppo del commercio: aiutano i *players* ad interfacciarsi con i propri interlocutori con maggiore consapevolezza circa i processi organizzativi che regolano l'attività di questi ultimi. E più si procederà sulla via della digitalizzazione, più si avvertirà la necessità di fare affidamento sull'adeguatezza dei sistemi di cibersicurezza adottati dalle proprie controparti: giacché un attacco cibernetico non colpisce soltanto l'impresa *target*, ma (potenzialmente) anche la sua rete di fornitori e clienti.

23.12.2020

Gianmatteo Nunziante, Partner
E: g.nunziante@nmlex.it
T.: +39 06 695181

Per chiarimenti o informazioni potete contattare l'autore oppure il Vostro Professionista di riferimento all'interno dello Studio

www.nunziantemagrone.it