Regolamento DORA: tempi, contenuti e implicazioni di cybersecurity. 7Layers in prima fila

Da tempo, l'evoluzione delle minacce informatiche occupa una posizione primaria nelle agende di governi e organizzazioni internazionali, portando ad una crescente produzione legislativa in materia, intesa a creare un contesto omogeneo e un ambiente affidabile per operatori e investimenti.

In particolare, le istituzioni europee negli ultimi anni si sono spese per l'adozione di normative avanzate a protezione di dati, infrastrutture e cittadini dell'Unione Europea, perseguendo la duplice finalità di uniformare le regole per chi opera in UE e innalzare il livello complessivo della sicurezza di reti e sistemi a salvaguardia di informazioni e servizi.

In tale contesto, tra le principali novità normative in via di applicazione vi è sicuramente il *Digital Operational Resilience Act*, più noto con la sigla DORA.

Origini e scopi del Regolamento DORA

Il DORA è stato pubblicato sulla Gazzetta Ufficiale dell'UE il 27 dicembre 2022 come Regolamento Europeo 2022/2554 relativo alla resilienza operativa digitale per il sistema finanziario. In quanto Regolamento, il DORA è da considerarsi in vigore in tutti gli stati membri dell'UE dal 17 gennaio 2023 e risulterà pienamente applicabile a partire dal 17 gennaio 2025. Ne deriva che i soggetti coinvolti hanno a disposizione ancora qualche mese per adeguarsi a una cornice giuridica vincolante

circa la gestione del rischio informatico e la capacità di fronteggiare incidenti, che potrebbero compromettere reti e sistemi, a discapito della sicurezza delle informazioni e dell'erogazione dei servizi finanziari.

Del resto, nelle intenzioni del legislatore comunitario, la nuova normativa *"accresce il livello di armonizzazione delle varie componenti della resilienza digitale"* e *"introduce requisiti in materia di gestione dei rischi informatici e segnalazione di incidenti connessi alle TIC più rigorosi rispetto a quelli contenuti nell'attuale normativa dell'Unione"*, così migliorando la resilienza operativa e la sicurezza delle organizzazioni finanziarie.

In tale quadro, la regolamentazione da un lato deve rivolgersi a una maggiore varietà di soggetti attivi sui mercati finanziari, mentre dall'altro è tenuta a considerare nuove tipologie di *Threat Actor* e strumenti sempre più sofisticati a loro disposizione, senza trascurare l'estensione della superficie di attacco legata al frequente ricorso a fornitori di servizi ICT a supporto delle funzioni essenziali e importanti erogate dai soggetti a perimetro.

DORA e NIS2

Il DORA non è l'unica norma in materia di cybersecurity a livello europeo. Nei Considerando del Regolamento viene infatti richiama la Direttiva UE 2016/1148, già dedicata a stabilire criteri minimi di cybersicurezza per gli operatori di servizi essenziali, abrogata dalla più recente 2022/2555 (nota come NIS2), che ne amplia il perimetro di applicazione.

L'intersezione fra le prescrizioni del Regolamento DORA e le indicazioni della direttiva NIS2 è certamente significativa: la governance e la centralità della gestione del rischio e degli incidenti informatici ne costituiscono forse gli esempi più evidenti.

Tuttavia, il DORA prevede requisiti più rigorosi per le entità finanziarie ed è pertanto da considerarsi *lex specialis* rispetto alla direttiva (UE) 2022/2555 (cfr. Considerando 15-16 del Regolamento) e quindi su di essa prevalente laddove applicabile.

Chi è interessato dal Digital Operational Resilience Act?

Se la direttiva del 2016 si rivolgeva a tre sole tipologie di entità finanziarie (enti creditizi, sedi di negoziazione e controparti centrali), il DORA amplia notevolmente la platea dei propri destinatari.

Vi rientrano infatti, accanto alle istituzioni finanziarie "tradizionali" – come le banche o le società di investimento – anche realtà emerse solo da pochi anni, quali i gestori di piattaforme di *crowdfunding* o i vari attori del mondo delle criptovalute.

Un'ulteriore innovazione è rappresentata dal coinvolgimento, diretto o indiretto, di quelle terze parti che, pur non essendo strettamente del settore, rivestono un ruolo rilevante nella catena di valore dei mercati finanziari: tra questi, a mero titolo di esempio, citiamo i fornitori di servizi *Cloud* nonché le aziende che svolgono attività di *Data Analytics* o di *rating* che, qualora identificate come fornitori terzi critici, potranno essere sottoposti alla supervisione delle autorità di vigilanza.

Le prescrizioni del Regolamento DORA

A tutte le entità che rientrano nel suo campo di applicazione il DORA richiede innanzitutto di:

- definire un'organizzazione interna che preveda un quadro di governance della sicurezza informatica, in grado di garantire una gestione efficace dei rischi,

l’approvazione di contromisure e controlli adeguati, nonché la loro effettiva applicazione

- pianificare la gestione dei rischi per tecnologie e servizi ICT, mediante l’adozione di un framework di risk management a supporto della definizione di una strategia di resilienza digitale, che garantisca la continuità operativa e una adeguata capacità di affrontare scenari di crisi
- classificare gli incidenti, ivi inclusi gli incidenti correlati ai fornitori terzi di servizi ICT, e le minacce che potrebbero insidiare la sicurezza informatica dell’entità finanziaria
- predisposizione di un sistema di segnalazione degli incidenti informatici, dal monitoraggio alla comunicazione, laddove previsto, alle autorità competenti e agli stakeholder potenzialmente coinvolti: si rendono necessari piani per la gestione degli incidenti (IRP) per contenerne l’impatto e accelerare il ripristino dei servizi coinvolti.
- pianificare lo svolgimento di Threat Lead Penetration Test (TLPT) mirati a valutare, con frequenza almeno triennale, la resilienza delle infrastrutture informatiche rispetto al mutato panorama delle minacce
- gestire i rischi informatici correlati a fornitori, mediante l’identificazione di servizi e processi che prevedano il coinvolgimento di soggetti terzi e la conseguente definizione di clausole contrattuali, che garantiscano un livello di sicurezza adeguato e strumenti di monitoraggio dei servizi forniti.

I requisiti del Regolamento implicano pertanto la necessità di:

- ricorrere a framework di sicurezza di riconosciuta affidabilità ed efficacia (es. ISO/IEC 27001) per garantire un approccio sistemico e coerente alla gestione della sicurezza delle informazioni

- adottare configurazioni sicure per i sistemi e le reti, facendo riferimento alle best practice internazionali (in particolare a quelle del NIST);
- valutare la criticità dei componenti ICT e documentare le dipendenze esistenti a livello di sistemi, processi e third party provider (TPP), prevedendo adeguate misure a protezione degli asset più critici.

Si impone altresì l'adozione di robusti framework di gestione dei rischi ICT, che includano:

- l'uso di metodologie avanzate per identificare e valutare i rischi, come l'analisi delle minacce (threat modeling) e la periodica valutazione delle vulnerabilità (vulnerability assessment)
- il ricorso a strumenti di controllo e mitigazione delle minacce quali firewall avanzati, sistemi di prevenzione delle intrusioni (IPS) o soluzioni di crittografia end-to-end
- l'implementazione di sistemi di monitoraggio continuo per rilevare e rispondere tempestivamente a comportamenti anomali e potenziali incidenti di sicurezza.

Il DORA richiede poi che le organizzazioni prevedano piani dettagliati di continuità operativa che comporteranno:

- l'esecuzione di Business Impact Analysis (BIA) per identificare le funzioni critiche e determinare l'impatto di possibili interruzioni operative
- lo sviluppo di piani di recupero dettagliati che comprendano il backup dei dati, il ripristino dei sistemi (Disaster Recovery) e le procedure di failover
- lo svolgimento di regolari test sui piani e protocolli così definiti, per assicurarne l'efficacia e garantirne il loro costante aggiornamento.

Il Regolamento enfatizza l'importanza del monitoraggio continuo e della capacità di rispondere rapidamente agli

eventuali incidenti informatici. Tali requisiti sono attuabili tramite:

- l'utilizzo di *Security Information and Event Management* (SIEM) per aggregare e analizzare i *log* di sicurezza, fornendo visibilità in tempo reale su tutti gli eventi rilevanti;
- l'integrazione di *feed* di *intelligence* sulle minacce per migliorare la capacità di rilevamento e risposta agli attacchi emergenti;
- l'adozione di soluzioni di *Security Orchestration, Automation and Response* (SOAR) per ridurre drasticamente i tempi di reazione agli incidenti.

Infine, non può essere trascurato l'aspetto documentale: il Regolamento richiede alle entità finanziarie di definire dettagliate politiche di sicurezza e procedure operative standard (SOP) per la gestione del rischio informatico.

RTS, ITS e regolamenti delegati

Il DORA affida alle autorità europee di vigilanza (le AEV: EBA, ESMA, EIOPA) la definizione di norme tecniche di regolamentazione (RTS) e di attuazione (ITS) che contengano indicazioni puntuali riguardo gli aspetti più rilevanti e delicati. Le norme che ne derivano sono adottate dall'UE mediante atti (o regolamenti) delegati della Commissione Europea.

Al riguardo citiamo:

- il regolamento delegato (UE) 2024/1772, che sancisce i criteri primari e secondari da adottare per la classificazione degli incidenti informatici sulla base dei servizi impattati, del profilo dei clienti coinvolti, della perdita di dati, nonché dell'impatto reputazionale, economico e dell'ambito geografico. Il regolamento stabilisce per ogni criterio una soglia

intesa a supportare l’individuazione degli incidenti da considerarsi gravi e, dunque, da notificare alle autorità di settore

- il Regolamento delegato (UE) 2024/1773, che riporta i principi che dovranno comparire nelle politiche di gestione dei contratti per l’acquisizione di servizi ICT da terze parti a supporto di funzioni essenziali e importanti dell’Entità Finanziaria. Tali politiche dovranno definire ruoli e responsabilità nell’ambito dell’organizzazione e garantire la definizione di clausole che consentano di stabilire il livello dei servizi forniti dalla terza parte, il rapporto con eventuali sub-fornitori, i requisiti di sicurezza delle informazioni, i diritti di audit e le strategie di uscita a cui poter ricorrere.
- Il Regolamento delegato (UE) 2024/1774, che delinea le politiche di risk management per l’identificazione e la valutazione dei rischi a cui sono esposti tecnologie e servizi ICT, al fine di individuare e attuare le misure di sicurezza tecniche e organizzative necessarie, quali politiche per la gestione delle chiavi crittografiche, vulnerability management, asset management, politiche per la gestione degli ambienti di produzione, testing e sviluppo, politiche per l’acquisizione e sviluppo di applicazioni software da integrare con i sistemi ICT dell’Entità Finanziaria.

Il set di atti delegati non è ancora da considerarsi completo: altri ne sono attesi entro la fine del 2024.

“Il DORA – secondo Guido Arrigoni, Cybersecurity compliance manager di 7Layers – è da considerarsi una normativa in divenire e, come tale, richiede una verifica costante delle sue evoluzioni unitamente a una valutazione delle indicazioni fornite dalle autorità di settore, sia a livello europeo sia a livello nazionale”.

Il ruolo dei fornitori di servizi ICT

Come accennato, il DORA presenta implicazioni non trascurabili per i fornitori di servizi ICT a supporto dell'attività delle Entità Finanziarie incluse nel perimetro di applicazione del Regolamento, che dovranno redigere un registro dei contratti stipulati con i TPP (cfr. DORA, art. 23). Coerentemente con le prescrizioni del Regolamento, i requisiti in capo alle Entità Finanziarie si tradurranno in clausole a cui i fornitori dovranno essere capaci di rispondere esprimendo una security posture tale da soddisfare le esigenze dei propri clienti.

I fornitori più rilevanti potranno essere classificati come critici dalle autorità di vigilanza europee sulla base dei criteri indicati dall'art. 31 del Regolamento e dettagliati dal Discussion Paper pubblicato dalle AEV, per stabilire il percorso che porterà a identificare i CTPP (Critical Third Party Provider) sulla base della continuità, della qualità dei servizi forniti e del possibile impatto sistemico che potrebbe derivare da un eventuale incidente che comprometta la sicurezza del fornitore.

DORA: implicazioni per la Cyber Security

L'implementazione del Regolamento DORA richiede senz'altro risorse significative, che andranno indirizzate verso:

- investimenti in tecnologie avanzate di sicurezza, come sistemi di rilevamento delle intrusioni (IDS), soluzioni di crittografia e strumenti di monitoraggio continuo;
- formazione continua del personale sulle migliori pratiche di cybersecurity e la gestione dei rischi ICT;
- definizione di una chiara *governance* della sicurezza informatica, che individui ruoli e responsabilità legati alla gestione degli incidenti nonché ai relativi obblighi di documentazione e reportistica di eventuali incidenti.

Conclusioni

Oltre a garantire la necessaria *compliance*, l’adeguamento alle nuove regole porterà maggiore trasparenza, responsabilità e innovazione presso le aziende e gli enti interessati, uniformando i livelli di resilienza digitale dei servizi finanziari sul mercato europeo.

Sebbene l’implementazione del DORA possa presentare delle sfide, è prevedibile che nel lungo termine i costi siano compensati dall’accresciuto valore derivante dalla maggiore affidabilità e sicurezza garantite ai propri clienti e dalla capacità di affrontare scenari in grado di arrivare a compromettere l’intero mercato finanziario europeo se non adeguatamente gestiti.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/regolamento-dora-tempi-contenuti-e-implicazioni-di-cybersecurity-7layers-in-prima-fila/