SOLUTION NOTE

LEGGE SULLA RESILIENZA OPERATIVA DIGITALE (DORA) E DNS

Come applicare le best practice DNS per garantire la conformità al regolamento DORA

INTRODUZIONE

Il Digital Operational Resiliency Act, affettuosamente noto come DORA, è un regolamento dell'Unione Europea (UE) progettato per rafforzare la resilienza digitale delle istituzioni finanziarie. È entrato in vigore il 17 gennaio 2025 e garantisce che banche, compagnie assicurative, società di investimento e altre entità finanziarie possano resistere, rispondere e recuperare dalle interruzioni delle tecnologie dell'informazione e della comunicazione (ICT), come attacchi informatici o guasti di sistema.

Il regolamento DORA è organizzato in nove capitoli con i corrispondenti standard tecnici regolamentari (RTS). Oltre alle banche e ad altre organizzazioni di servizi finanziari tradizionali, la legge e i suoi standard si applicano ad altre aziende del settore finanziario, come i fornitori di servizi di criptovalute e i fornitori ICT di terze parti. Secondo PWC, la conformità obbligatoria al regolamento DORA si estende a più di 22.000 entità,[1] poiché la direttiva non si limita alle aziende situate nell'UE, ma anche a qualsiasi istituzione finanziaria che opera o svolge attività commerciali all'interno della zona.

L'articolo 1 del regolamento DORA delinea i vari standard normativi relativi alla sicurezza delle reti e dei sistemi informativi. Gli argomenti trattati includono la gestione del rischio, la segnalazione degli incidenti, i test di resilienza, la gestione del rischio ICT di terze parti e la condivisione di informazioni e intelligence sulle minacce informatiche.[2]

Con l'evoluzione di questi standard, i requisiti specifici ad essi associati diventeranno più chiari per le organizzazioni finanziarie. Ad esempio, il *Final Report on draft RTS specifying elements related to threat-led penetration tests*[3] fornisce ulteriore chiarezza sui requisiti dei test di penetrazione. Il report spiega che i requisiti DORA interagiranno con altre iniziative normative relative alla sicurezza, come il framework TIBER-EU (Threat Intelligence-Based Ethical Red-Teaming) associato alla Banca centrale europea. Come afferma il report, "[il framework TIBER-EU] può anche aiutare le autorità competenti e le entità finanziarie a soddisfare i requisiti per i test di penetrazione basati sulle minacce ai sensi del Digital Operational Resilience Act (DORA)".[4] Il report fa anche riferimento al documento della Banca centrale europea, *Adopting TIBER-EU will help fulfil DORA requirements*.[5]

IN CHE MODO IL DNS AIUTA CON LA CONFORMITÀ AL REGOLAMENTO DORA

Il Domain Name System (DNS) svolge un ruolo centrale in tutte le interazioni di rete tra dispositivi, applicazioni, domini internet, database e risorse cloud. Quando gestito e implementato strategicamente, il protocollo DNS funge anche da punto di applicazione proattivo per la sicurezza della rete, una preziosa fonte di analisi forense digitale e un efficace facilitatore per una rapida risposta agli incidenti. In quanto tale, il DNS è in una posizione unica per assistere le istituzioni finanziarie nell'esecuzione di una serie di attività di conformità al regolamento DORA, tra cui:

- Gestione del rischio ICT (Capitolo II)
- Gestione, classificazione e segnalazione degli incidenti legati alle ICT (Capitolo III)
- Test di resilienza operativa digitale (Capitolo IV)
- Gestione del rischio ICT di terze parti (Capitolo V)
- Accordi di condivisione delle informazioni (Capitolo VI)

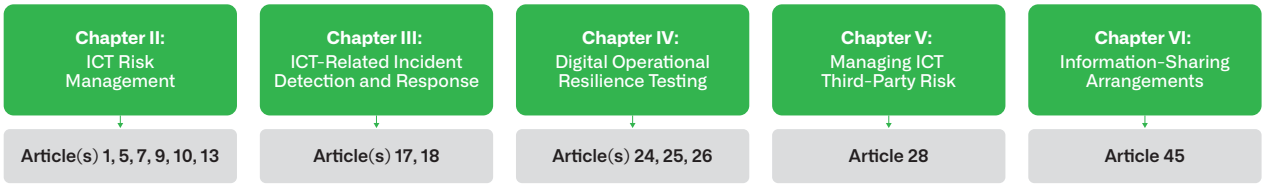

Figura 1. Dove il DNS contribuisce alle attività di conformità al regolamento DORA

È importante notare che, oltre ad allinearsi a particolari principi DORA, l'efficacia del DNS è tale che molte organizzazioni trarrebbero vantaggio dall'utilizzare le sue capacità per soddisfare la maggior parte delle normative. Poiché il DNS è già integrato nelle reti organizzative, esso offre un modo più pratico ed efficiente per migliorare la resilienza e la sicurezza rispetto all'adozione di tecnologie e controlli completamente nuovi. Quando si considera dove il DNS può contribuire alle attività DORA, le entità dovrebbero applicare il principio di proporzionalità dell'articolo 4 del regolamento.

Le raccomandazioni qui sotto sono organizzate per capitoli pertinenti delle linee guida DORA, insieme alle annotazioni per gli articoli specifici del regolamento con cui si allineano.

GESTIONE DEI RISCHI ICT

Molte organizzazioni finanziarie considerano il DNS come "solo una parte dell'infrastruttura di rete", ma è fondamentale per la resilienza operativa che il regolamento DORA cerca di migliorare. Un'interruzione del DNS è catastrofica, in quanto ha un impatto su quasi tutte le applicazioni e i servizi di un istituto finanziario. Per questo motivo, le entità che rispettano il regolamento DORA dovrebbero incorporare la disponibilità del servizio DNS nella pianificazione della gestione del rischio, al pari di altri sistemi principali.[6] Parte di questo sforzo implica l'utilizzo delle best practice del settore nell'implementazione e nella gestione dell'infrastruttura DNS interna.

Inoltre, poiché gli istituti finanziari interagiscono regolarmente con entità e utenti esterni, è necessario prestare uguale attenzione all'igiene della sicurezza del DNS esterno. Ai fini della conformità, le organizzazioni dovrebbero garantire che i domini DNS pubblici (autorevoli) rimangano resilienti e sicuri. I Threat actors prendono di mira costantemente i domini autorevoli mal configurati a causa di politiche e processi di sicurezza poco rigorosi. La gestione esterna del DNS può coinvolgere anche terze parti, per le quali le normative restano applicabili; pertanto, i responsabili della conformità al regolamento DORA dovrebbero considerare la gestione e la mitigazione dei rischi dei servizi DNS associati a queste parti.

Consigli:

- Implementare architetture DNS resilienti, progettate per supportare la continuità del servizio e dimensionate per la capacità di picco, insieme a politiche e procedure coerenti per mantenere l'infrastruttura DNS e garantire la disponibilità e la sicurezza del servizio. (Articoli 7, 9)
- Assicurarsi che una parte dell'organizzazione sia responsabile della gestione dei nomi di dominio esterni, agendo come registrar/registro interno, per evitare che parti diverse dell'organizzazione registrino e gestiscano i domini tramite più fornitori. (Articolo 5)
- Implementare i servizi di DNS protettivi per bloccare e registrare il traffico DNS dannoso, impedire l'utilizzo del DNS per l'esfiltrazione dei dati, identificare il traffico anomalo e fornire dati per l'analisi forense e la risposta agli incidenti. (Articoli 9, 10, 13)

GESTIONE, CLASSIFICAZIONE E SEGNALAZIONE DEGLI INCIDENTI RELATIVI ALLE ICT

I professionisti della sicurezza utilizzano il DNS durante la risposta agli incidenti per identificare e bloccare ulteriori comunicazioni dannose e per aiutare nella classificazione e nella definizione dell'ambito di qualsiasi compromissione. Tutte le comunicazioni di rete iniziano con una query DNS, rendendo i log, che contengono dati di query e risposta, insieme ai log DHCP e alle informazioni sulle risorse, fondamentali per la gestione degli incidenti. Ad esempio, un accesso immediato ai record di quali dispositivi su una rete possono aver comunicato con un host dannoso aiuta i team di sicurezza a identificare l'entità e la classificazione di qualsiasi incidente. Analogamente, i log DHCP identificano quali indirizzi IP sono stati associati a una determinata risorsa. Poiché la maggior parte dei log di sicurezza identifica i dispositivi in base a indirizzi IP temporanei o fissi, le organizzazioni che desiderano garantire una correlazione accurata e coerente tra eventi e minacce devono assicurarsi che i dati e il contesto pertinenti a livello di dispositivo possano essere condivisi con gli strumenti delle operazioni di sicurezza.

Consigli:

- Registrare continuamente i dati delle query e delle risposte DNS, l'attività dei lease DHCP e i dati degli asset per facilitare una correlazione accurata degli eventi e fornire un contesto per l'analisi forense come parte della gestione degli incidenti. (Articoli 17(3), 18(1))
- Implementare i servizi di DNS protettivi come punto di controllo per bloccare il traffico DNS dannoso. Questo punto di controllo dovrebbe includere la threat intelligence relativa agli indicatori utilizzati nel servizio di DNS protettivo, in modo che il contesto associato a qualsiasi traffico bloccato possa essere condiviso con gli strumenti dell'ecosistema di sicurezza per facilitare la valutazione. (Articolo 17)

TEST DI RESILIENZA OPERATIVA DIGITALE

Il rispetto dello standard di resilienza digitale per il regolamento DORA richiede ulteriori test per la continuità operativa e il disaster recovery (articolo 24), nonché test di vulnerabilità e penetrazione all'interno di un framework di autorità competente (articoli 25 e 26). Come per le considerazioni sui rischi, coloro che supervisionano la conformità al regolamento DORA dovrebbero considerare il ruolo fondamentale che il DNS svolge nella disponibilità della rete. Ad esempio, le organizzazioni possono sfruttare il DNS per garantire la continuità aziendale tramite il bilanciamento globale del carico dei server. Sul fronte del disaster recovery, un'interruzione del DNS causata da un attacco informatico, una configurazione errata o un disastro naturale può portare all'interruzione delle operazioni aziendali. Pertanto, è imperativo che gli istituti finanziari fortifichino il DNS e i servizi di rete critici associati, come il DHCP, per soddisfare i requisiti di resilienza operativa.

Consigli:

- Rivedere l'architettura e i servizi DNS interni ed esterni per "identificare i punti deboli, le carenze e le lacune nella resilienza operativa digitale e implementare tempestivamente le misure correttive". A questo proposito possono essere utili standard tecnici come NIST 800-81. (Articolo 24(1))
- Quando si sviluppa un programma completo di test di resilienza operativa digitale, ci si deve assicurare che copra specificamente i servizi DNS, l'infrastruttura e i protocolli. Il ripristino dei servizi DNS è un prerequisito essenziale per il recupero delle applicazioni e dei servizi di un'organizzazione, e il DNS stesso può facilitare la continuità del servizio e il disaster recovery. (Art. 24(1))
- Data la dipendenza di una rete dal DNS, assicurarsi che le procedure di test specifiche per i servizi e l'infrastruttura DNS siano incluse nel piano generale di test di resilienza. (Articolo 24(2))
- Quando si eseguono test per la resilienza operativa con collabori con fornitori esterni di penetration testing (TLPT), assicurarsi che vengano eseguiti test specifici relativi al DNS per la disponibilità e la sicurezza. (Articoli 25, 26)
- Aree chiave da includere:
    - » Verificare che la resilienza del DNS funzioni come previsto, in particolare che ci siano percorsi ridondanti multipli per la risoluzione dei nomi.
    - » Assicurarsi che il traffico DNS in uscita dalle reti di un'organizzazione venga instradato attraverso resolver DNS controllati (che dovrebbero registrare i dati delle query e delle risposte).
    - » Interrogare tramite query i nomi di dominio associati all'attuale attività dannosa.
    - » Eseguire un test per determinare se i dati possono essere esfiltrati attraverso le query DNS e se è possibile l'infiltrazione di malware tramite le risposte DNS.
    - » Mettere in atto procedure e strumenti automatizzati che considerino l'igiene della sicurezza DNS, ad esempio assicurandosi che i domini orfani e le deleghe errate dei sottodomini vengano corretti.

GESTIONE DEL RISCHIO DELLE TERZE PARTI ICT

I servizi DNS, come i DNS esterni, rientrano nell'ambito del regolamento DORA perché possono essere gestiti da terze parti. Inoltre, possono gestire anche i sottodomini DNS che sono stati loro delegati per servizi specifici.

Consigli:

- Esaminare i contratti con eventuali terze parti che gestiscono servizi o infrastrutture DNS, ad esempio domini esterni, per assicurarti che siano conformi alle normative e ai criteri dell'organizzazione e forniscano gli stessi livelli di resilienza operativa e sicurezza. (Articolo 28)

ACCORDI DI CONDIVISIONE DELLE INFORMAZIONI

Gli istituti finanziari condividono regolarmente indicatori di compromissione (IoC) e tattiche, tecniche e procedure (TTP) con comunità fidate di servizi finanziari, includendo protezioni adeguate per salvaguardare le informazioni sensibili. All'interno di questi gruppi fidati, le entità finanziarie possono utilizzare i log delle query e delle risposte DNS, così come le informazioni provenienti da domini dannosi bloccati, come parte delle informazioni che condividono.

Consigli:

- Prepararsi alla condivisione delle informazioni implementando una policy per fornire IoC correlati al DNS. Concordare in anticipo i formati dei dati con un gruppo di condivisione aiuterebbe operativamente, soprattutto quando gli indicatori verranno inseriti in strumenti operativi come un sistema di gestione degli eventi di sicurezza delle informazioni (SIEM). In particolare, le informazioni provenienti da attività dannose acquisite e condivise tramite i servizi DNS protettivi spesso aiutano altre entità finanziarie a potenziare la difesa della rete. (Articolo 45)

SEMPLIFICA LA CONFORMITÀ AL REGOLAMENTO DORA CON INFOBLOX

Per ottenere più facilmente la conformità al regolamento DORA, le organizzazioni finanziarie dovrebbero allineare i propri servizi DNS ai principi del regolamento DORA, concentrandosi sulla resilienza e sulla sicurezza per gestire efficacemente i rischi ICT. Questo allineamento include il miglioramento delle protezioni contro minacce come il phishing e l'esfiltrazione di dati e l'adesione a framework come TIBER-EU e MITRE ATT&CK per la threat intelligence. Infoblox offre soluzioni su misura per mitigare questi rischi e supportare la conformità alle normative sulla gestione dei rischi ICT.

Inoltre, l'infrastruttura DNS robusta e le soluzioni di sicurezza di Infoblox sono posizionate in modo unico per supportare le entità finanziarie nel raggiungere la conformità ai principi DORA. Concentrandosi su servizi DNS sicuri e resilienti, Infoblox aiuta le organizzazioni soggette al regolamento DORA a mitigare i rischi associati alla comunicazione DNS non gestita, come il phishing, il comando e controllo del malware e l'esfiltrazione di dati. Sfruttando framework leader del settore come MITRE ATT&CK, Infoblox fornisce informazioni fruibili e mitigazioni su misura che si allineano ai requisiti di gestione dei rischi ICT. Inoltre, l'esperienza di Infoblox nell'integrare le linee guida di ENISA e NIST assicura che le entità finanziarie rispettino gli obblighi di disponibilità e sicurezza, navigando efficacemente in complessi contesti normativi.

1. How the digital operational resilience act helps your continuity, PwC.
2. DORA Capitolo 1 Disposizioni Generali, Articolo 1(1) Oggetto
3. Final Report on draft RTS specifying elements related to threat led penetration tests (riferimento JC 2024 29), European Securities and Markets Authority (ESMA), 7 luglio 2024.
4. What is TIBER-EU?, Banca centrale europea.
5. Adopting TIBER-EU will help fulfil DORA requirements, Banca centrale europea, settembre 2024.
6. Regolamento DORA "(22) Per 'funzione critica o importante' si intende una funzione la cui interruzione comprometterebbe in modo sostanziale la performance finanziaria di un'entità finanziaria, o la solidità o la continuità dei suoi servizi e delle sue attività, oppure l'interruzione, il difetto o la mancata esecuzione di tale funzione comprometterebbe in modo sostanziale la continua conformità di un'entità finanziaria con le condizioni e gli obblighi della sua autorizzazione, o con gli altri obblighi previsti dalla legge sui servizi finanziari applicabile."

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/it

Versione: 20250625v1