NOTE DE SYNTHÈSE

RÈGLEMENT SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE (DORA) ET DNS

Comment appliquer les meilleures pratiques DNS pour se conformer à DORA

INTRODUCTION

Le règlement européen sur la résilience opérationnelle numérique, communément appelé DORA, est un règlement de l'Union européenne (UE) conçu pour renforcer la résilience numérique des institutions financières. Entré en vigueur le 17 janvier 2025, il veille à ce que les banques, compagnies d'assurance, sociétés d'investissement et autres entités financières puissent résister, faire face et surmonter les perturbations liées aux technologies de l'information et de la communication (TIC), telles que les cyberattaques ou les pannes de système.

DORA est structuré en neuf chapitres auxquels correspondent des normes techniques de réglementation (RTS). En plus des banques et des institutions financières traditionnelles, le règlement et ses normes s'appliquent également à d'autres acteurs du secteur financier, tels que les prestataires de services de crypto-actifs et les fournisseurs tiers de services TIC. Selon PWC, la conformité obligatoire à DORA concerne plus de 22 000 entités[1], car le règlement ne se limite pas aux entreprises situées dans l'UE, mais s'étend aussi à toute institution financière qui opère ou effectue des transactions au sein de l'Union européenne.

L'article 1 de DORA définit les différentes normes réglementaires relatives à la sécurité des réseaux et des systèmes d'information. Les thèmes abordés incluent la gestion des risques, la déclaration des incidents, les tests de résilience, la gestion des risques liés aux prestataires tiers de services TIC, ainsi que le partage d'informations et de threat intelligence sur les cybermenaces.[2]

Au fur et à mesure de l'évolution de ces normes, les exigences spécifiques qui y sont associées deviendront plus claires pour les institutions financières. À titre d'exemple, le *rapport final sur le projet de RTS précisant les éléments relatifs aux tests d'intrusion basés sur la menace*[3] apporte des éclaircissements supplémentaires sur les exigences en matière de tests d'intrusion. Ce rapport explique que les exigences de DORA interagiront avec d'autres initiatives réglementaires liées à la sécurité, telles que le cadre TIBER-EU (Threat Intelligence-Based Ethical Red-Teaming) de la Banque centrale européenne. Comme l'indique ce rapport, « [le cadre TIBER-EU] peut également aider les autorités compétentes et les entités financières à satisfaire aux exigences relatives aux tests d'intrusion basés sur les menaces dans le cadre du règlement sur la résilience opérationnelle numérique (DORA) ».[4] Le rapport fait également référence au document de la Banque centrale européenne intitulé *L'adoption de TIBER-EU contribuera à satisfaire aux exigences DORA*.[5]

COMMENT LE DNS CONTRIBUE À LA CONFORMITÉ DORA

Le système de noms de domaine (DNS) joue un rôle central dans toutes les interactions réseau entre appareils, applications, domaines internet, bases de données et ressources cloud. Lorsqu'il est géré et déployé de façon stratégique, le protocole DNS devient un point d'application proactif pour la sécurité réseau, une source précieuse d'analyses forensiques et un outil clé pour accélérer la réponse aux incidents. À ce titre, le DNS est particulièrement bien positionné pour aider les institutions financières à se conformer aux exigences du règlement DORA dans plusieurs domaines clés, notamment :

- Gestion des risques liés aux TIC (Chapitre II)
- Gestion, classification et notifications des incidents liés aux TIC (Chapitre III)
- Test de résilience opérationnelle numérique (Chapitre IV)
- Gestion des risques liés aux tiers TIC (Chapitre V)
- Dispositifs de partage d'informations (Chapitre VI)

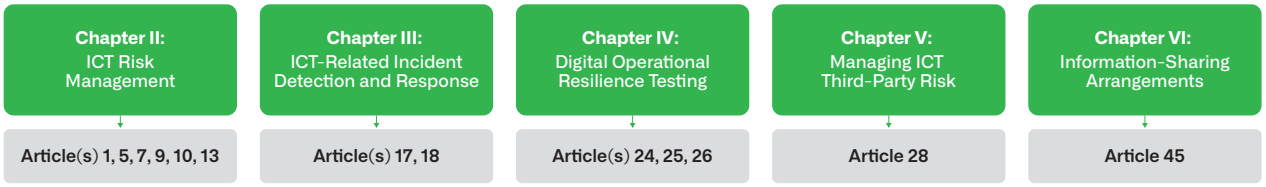

Figure 1. Contribution du DNS aux activités de conformité DORA

Il convient de noter qu'au-delà de son alignement avec certains principes du règlement DORA, l'efficacité du DNS est telle que de nombreuses entreprises bénéficieraient de ses capacités pour répondre à la majorité des exigences de la réglementation. Comme le DNS est déjà intégré aux réseaux organisationnels, il représente une solution plus simple et plus efficace pour renforcer la résilience et la sécurité que l'adoption de technologies ou de contrôles entièrement nouveaux. Lorsqu'elles déterminent que le DNS peut contribuer aux activités liées au règlement DORA, les entreprises doivent appliquer le principe de proportionnalité défini à l'article 4 du règlement.

Les recommandations ci-dessous sont organisées selon les chapitres pertinents des lignes directrices DORA, accompagnées des références aux articles spécifiques du règlement auxquels elles correspondent.

GESTION DES RISQUES LIÉS AUX TIC

De nombreuses organisations financières considèrent le DNS comme « un simple élément de l'infrastructure réseau », alors qu'il est essentiel à la résilience opérationnelle que DORA s'efforce d'améliorer. Une panne de DNS est catastrophique car elle a un impact sur la quasi-totalité des applications et des services d'une institution financière. C'est pourquoi les entreprises qui se conforment au règlement DORA doivent intégrer la disponibilité du service DNS dans la planification de la gestion des risques, au même titre que les autres systèmes centraux.[6] Une partie de cet effort consiste à utiliser les meilleures pratiques du secteur pour mettre en œuvre et gérer l'infrastructure DNS interne.

De plus, étant donné que les institutions financières interagissent régulièrement avec des entités et des utilisateurs externes, une attention égale doit être accordée à l'hygiène de sécurité concernant le DNS externe. Pour des raisons de conformité, les organisations doivent s'assurer que les domaines DNS publics (autoritaires) restent résilients et sécurisés. Les acteurs malveillants ciblent activement les domaines faisant autorité mal configurés en raison de politiques et de processus de sécurité peu rigoureux. La gestion externe des DNS peut également impliquer des tiers, pour lesquels les règlements restent applicables. Par conséquent, les responsables de la conformité DORA doivent prendre en compte la gestion des risques et l'atténuation des services DNS associés à ces tiers.

Recommandations :

- Mettez en œuvre des architectures DNS résilientes, conçues pour assurer la continuité des services et dimensionnées pour les pics de capacité, ainsi que des politiques et des procédures cohérentes pour maintenir la disponibilité et la sécurité de l'infrastructure et des services DNS. (Articles 7, 9)
- Assurez-vous qu'une partie de l'organisation soit responsable de la gestion des noms de domaine externes, agissant en tant que registraire/registre interne, afin d'éviter que des parties disparates de l'organisation n'enregistrent et ne gèrent des domaines via plusieurs fournisseurs. (Article 5)
- Mettez en œuvre des services DNS de protection pour bloquer et enregistrer le trafic DNS malveillant, empêcher l'utilisation du DNS pour l'exfiltration de données, identifier le trafic anormal et fournir des données pour les investigations et la réponse aux incidents. (Articles 9, 10, 13)

GESTION, CLASSIFICATION ET NOTIFICATIONS DES INCIDENTS LIÉS AUX TIC

Les praticiens de la sécurité utilisent le DNS lors de la réponse à un incident pour identifier et bloquer toute communication malveillante ultérieure et aider à la classification et à l'étendue de toute compromission. Toutes les communications réseau commencent par une requête DNS, ce qui rend les journaux, contenant les données de requête et de réponse, ainsi que les journaux DHCP et les informations sur les actifs, essentiels à la gestion des incidents. Par exemple, un accès rapide aux enregistrements des appareils d'un réseau qui ont pu communiquer avec un hôte malveillant aide les équipes de sécurité à déterminer l'ampleur et la classification de tout incident. De même, les journaux DHCP identifient quelles adresses IP ont été associées à un actif donné. La plupart des journaux de sécurité identifiant les dispositifs sur la base d'adresses IP transitoires plutôt que fixes, les organisations qui souhaitent assurer une corrélation précise et cohérente des événements et des menaces doivent veiller à ce que les données et le contexte pertinents au niveau des dispositifs puissent être partagés avec les outils d'opérations de sécurité.

Recommandations :

- Consignez en continu les données de requête et de réponse DNS, l'activité des baux DHCP et les données d'actifs pour faciliter la corrélation précise des événements et fournir un contexte pour les analyses d'investigation dans le cadre de la gestion des incidents. (Articles 17(3), 18(1))
- Mettez en œuvre des services DNS de protection en tant que point de contrôle pour bloquer le trafic DNS malveillant. Ce point de contrôle devrait inclure des Threat Intelligence liées aux indicateurs utilisés dans le service DNS de protection, afin que le contexte associé à tout trafic bloqué puisse être partagé avec les outils de l'écosystème de sécurité pour en faciliter l'évaluation. (Article 17)

TEST DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

Le respect de la norme de résilience numérique pour le DORA nécessite des tests supplémentaires pour la continuité des activités et la reprise après sinistre (article 24), ainsi que des tests de vulnérabilité et d'intrusion dans le cadre d'une autorité compétente (articles 25 et 26). Comme pour les considérations de risque, les responsables de la conformité au règlement DORA doivent prendre en compte le rôle fondamental que joue le DNS dans la disponibilité du réseau. Par exemple, les organisations peuvent tirer parti du DNS pour assurer la continuité des activités grâce à un équilibrage global de charge des serveurs. En ce qui concerne la reprise après sinistre, une panne de DNS due à une cyberattaque, à une mauvaise configuration ou à une catastrophe naturelle peut entraîner l'arrêt des opérations commerciales. Il est donc impératif que les institutions financières renforcent le DNS et les services réseau critiques associés, tels que le DHCP, pour satisfaire aux exigences de résilience opérationnelle.

Recommandations :

- Examinez l'architecture et les services DNS internes et externes pour « identifier les faiblesses, les déficiences et les lacunes dans la résilience opérationnelle numérique, et mettre rapidement en œuvre des mesures correctives ». Des normes techniques telles que NIST 800-81 peuvent être utiles à cet égard. (Article 24(1))
- Lors de l'élaboration d'un programme complet de tests de résilience opérationnelle numérique, assurez-vous qu'il couvre spécifiquement les services, l'infrastructure et les protocoles DNS. La restauration des services DNS est une condition préalable essentielle à la reprise des applications et services d'une organisation, et le DNS lui-même peut faciliter la continuité du service et la reprise après sinistre. (Article 24(1))
- Étant donné la dépendance d'un réseau au DNS, assurez-vous que des procédures de test spécifiques pour les services et l'infrastructure DNS sont incluses dans le plan global de test de résilience. (Article 24(2))
- Lorsque vous testez la résilience opérationnelle et que vous travaillez avec des fournisseurs externes de tests d'intrusion basés sur les menaces (TLPT), veillez à ce que des tests spécifiques liés au DNS soient effectués pour la disponibilité et la sécurité. (Articles 25, 26)
- Principaux domaines à inclure :
    - » Vérifiez que la résilience du DNS fonctionne comme prévu, en particulier qu'il existe plusieurs chemins redondants pour la résolution des noms.
    - » Veillez à ce que le trafic DNS sortant des réseaux d'une organisation passe par des programmateurs DNS contrôlés (qui doivent enregistrer les données de requête et de réponse).
    - » Recherchez les noms de domaine associés à l'activité malveillante en cours.
    - » Testez s'il est possible d'exfiltrer des données via des requêtes DNS et d'infiltrer des malwares via des réponses DNS.
    - » Mettez en place des procédures et des outils automatisés qui prennent en compte l'hygiène de sécurité du DNS, par exemple en veillant à ce que les noms de domaine orphelins et les délégations incorrectes de sous-domaines soient corrigées.

GESTION DES RISQUES LIÉS AUX TIERS TIC

Les services DNS, tels que les DNS externes, entrent dans le champ d'application DORA parce que des tiers peuvent les gérer. En outre, ils peuvent également gérer des sous-domaines DNS qui leur ont été délégués pour des services spécifiques.

Recommandations :

- Examinez les contrats conclus avec les tiers qui gèrent les services ou l'infrastructure DNS, tels que les domaines externes, pour vous assurer qu'ils se conforment aux réglementations et aux politiques de votre organisation et qu'ils fournissent les mêmes niveaux de résilience opérationnelle et de sécurité. (Article 28)

DISPOSITIFS DE PARTAGE D'INFORMATIONS

Les institutions financières partagent régulièrement des indicateurs de compromission (IoC) et des tactiques, techniques et procédures (TTP) avec des communautés de services financiers de confiance, y compris des protections appropriées pour protéger les informations sensibles. Au sein de ces groupes de confiance, les entités financières peuvent utiliser les journaux de requêtes et de réponses DNS, ainsi que les informations provenant de domaines malveillants bloqués, dans le cadre des informations qu'elles partagent.

Recommandations :

- Préparez-vous au partage d'informations en mettant en œuvre une politique visant à fournir des IoC liés au DNS. Un accord préalable sur les formats de données avec un groupe de partage serait utile sur le plan opérationnel, en particulier lorsque les indicateurs seront intégrés dans des outils opérationnels tels qu'un système de gestion des événements de sécurité (SIEM). En particulier, les informations sur les activités malveillantes collectées et partagées par l'intermédiaire des services DNS de protection aident souvent d'autres entités financières à renforcer la défense de leur réseau. (Article 45)

SIMPLIFIEZ LA CONFORMITÉ DORA AVEC INFOBLOX

Pour se conformer plus facilement au règlement DORA, les organisations financières devraient aligner leurs services DNS sur les principes DORA en se concentrant sur la résilience et la sécurité afin de gérer efficacement les risques liés aux TIC. Cette mise en conformité passe notamment par le renforcement des protections contre les menaces telles que le phishing et l'exfiltration de données, et par l'adhésion à des cadres tels que TIBER-EU et MITRE ATT&CK pour la threat intelligence. Infoblox propose des solutions sur mesure pour atténuer ces risques et soutenir la conformité aux réglementations de gestion des risques TIC.

En outre, l'infrastructure DNS fiable et les solutions de sécurité d'Infoblox sont particulièrement bien adaptées pour aider les entités financières à se conformer au règlement DORA. En se concentrant sur des services DNS sécurisés et résilients, Infoblox aide les entités soumises au règlement DORA à atténuer les risques associés aux communications DNS non gérées, tels que le phishing, la gestion et le contrôle de malwares et l'exfiltration de données. En s'appuyant sur des cadres de référence de premier plan tels que MITRE ATT&CK, Infoblox fournit des renseignements exploitables et des mesures d'atténuation sur mesure qui sont conformes aux exigences de gestion des risques TIC. En outre, l'expertise d'Infoblox dans l'intégration des directives de l'ENISA et du NIST garantit que les entités financières respectent leurs obligations en matière de disponibilité et de sécurité tout en naviguant efficacement dans des environnements réglementaires complexes.

---

1. Comment le règlement DORA renforce la continuité de vos activités, PwC.
2. Chapitre 1 – Dispositions générales, Article 1(1) – Objet
3. Rapport final – Projet de normes techniques de réglementation précisant les éléments liés aux tests de pénétration fondés sur les menaces (référence JC 2024 29), Autorité européenne des marchés financiers (ESMA), 7 juillet 2024.
4. Qu'est-ce que TIBER-EU?, Banque centrale européenne.
5. L'adoption de TIBER-EU permet de satisfaire aux exigences du règlement DORA, Banque centrale européenne, septembre 2024.
6. Règlement DORA « (22) “fonction critique ou inmportante” : une fonction dont l'interruption compromettrait gravement les résultats financiers d'une entité financière, ou la solidité ou la continuité de ses services et activités, ou dont l'interruption, la défaillance ou l'échec de l'exécution de cette fonction compromettrait gravement le respect permanent par une entité financière des conditions et obligations liées à son agrément, ou de ses autres obligations en vertu de la législation applicable en matière de services financiers ».

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20250625v1