

Exercice du 29 septembre : les premières heures d'un déni de service qui touche des tiers

Note aux participants de l'exercice de crise du 29 septembre 2026 · état du droit au 1er octobre 2026

L'exercice du 29 septembre plaçait chacun face à une attaque par déni de service multivectorielle contre un groupe dont deux filiales relèvent l'une de DORA, l'autre de NIS 2. Les effets débordaient sur ses clients et ses partenaires, y compris sur le plan financier. Cette note complète le débrief à chaud pour ceux qui veulent aller plus loin. Elle reprend ce qui fait en pratique la différence dans les premières heures, les horloges de notification qui courent en parallèle, et une courte liste de chantiers à lancer au retour. Elle ne rapporte rien de ce qui s'est dit aux tables.

1. Les premières heures

Un déni de service se voit tout de suite et occupe toute la salle, ce qui peut aussi en faire une diversion. Pendant que les équipes réseau activent la protection, la première question est donc de savoir s'il cache autre chose, une intrusion ou une exfiltration en cours ailleurs dans le système d'information. Il vaut mieux qu'une personne de l'équipe sécurité soit affectée à cette seule question, à l'écart de la gestion du trafic, et rende compte régulièrement à la cellule de crise.

La deuxième habitude à prendre est d'ouvrir un journal des décisions dès la première minute : qui a décidé quoi, à quelle heure, sur la base de quelle information. Ce journal nourrit ensuite chaque notification, la déclaration à l'assureur et l'explication que le superviseur demandera probablement, parfois des mois plus tard. Il se complète des éléments techniques à conserver, journaux, captures de trafic et rapports du fournisseur de protection. Une demande de rançon accompagne parfois ce type d'attaque : elle se conserve aussi, et ni échange ni paiement sans l'avis du conseil juridique.

La chaîne de protection, enfin, gagne à être connue avant l'incident. Il s'agit du contrat avec le fournisseur de protection ou l'opérateur, de la capacité réellement souscrite, des contacts d'escalade joignables la nuit, et de la personne qui a l'autorité de basculer le trafic. Dans beaucoup d'organisations, ces éléments existent mais sont entre des mains différentes, et c'est souvent ce qui coûte les premières heures.

2. Les horloges qui courent en parallèle

Deux filiales, deux régimes : les délais, les destinataires et les formulaires ne sont pas les mêmes, et d'autres horloges s'y ajoutent. Le tableau reprend celles qui comptent dans ce scénario. Pour NIS 2, ce sont les délais de la directive, à anticiper, l'état du droit français étant précisé sous le tableau.

Qui notifie	Délais	Destinataire
La filiale sous DORA, si l'incident est classé majeur	Notification initiale au plus tard 4 heures après la classification en incident majeur, et 24 heures au plus après la prise de connaissance · rapport intermédiaire sous 72 heures après la notification initiale, même sans changement, puis rapport intermédiaire actualisé sans retard injustifié dès le retour à la normale · rapport final au plus tard un mois après le rapport intermédiaire ou, le cas échéant, le dernier rapport intermédiaire actualisé	L'autorité compétente : en France l'ACPR pour les banques, les établissements de paiement, les entreprises d'investissement et les assureurs, via le portail OneGate (l'ACPR transmet à la BCE le dossier des banques importantes) · l'AMF, via sa messagerie sécurisée (Sesterce), pour les sociétés de gestion de portefeuille, les prestataires de services sur crypto-actifs, les prestataires de services de financement participatif et les entreprises de marché
La même filiale, si l'incident majeur a une incidence sur les intérêts financiers de clients	Information sans retard injustifié, dès la prise de connaissance, de l'incident et des mesures prises pour en atténuer les effets	Les clients concernés
La filiale relevant de NIS 2, si l'incident est important (régime prévu par NIS 2, pas encore applicable en France au 1er octobre 2026)	Alerte précoce dans les 24 heures de la prise de connaissance · notification dans les 72 heures de la prise de connaissance · rapport intermédiaire sur demande de l'ANSSI · rapport final au plus tard un mois après la notification, ou, si l'incident est encore en cours, rapport d'avancement puis rapport final dans le mois suivant son traitement	L'ANSSI (son CERT-FR est le CSIRT national)
La même filiale aujourd'hui en France, si elle est opérateur de services essentiels, fournisseur de service numérique ou opérateur d'importance vitale	Déclaration sans délai après la prise de connaissance d'un incident ayant un impact significatif sur la continuité ou la fourniture du service (opérateurs de services essentiels, fournisseurs de service numérique) ou affectant le fonctionnement ou la sécurité d'un système d'information d'importance vitale (opérateurs d'importance vitale)	L'ANSSI (pour les opérateurs d'importance vitale, au nom du Premier ministre)
Le responsable du traitement (un sous-traitant alerte le responsable, qui notifie), si	Notification dans les meilleurs délais et si possible sous 72 heures après la prise de connaissance, sauf si la violation n'est pas susceptible d'engendrer un risque pour les personnes · documentation interne	La CNIL, et les personnes concernées en cas de risque élevé

Qui notifie	Délais	Destinataire
l'indisponibilité ou la perte de données personnelles constitue une violation	dans tous les cas · information des personnes en cas de risque élevé	
Toute personne morale ou tout professionnel qui compte sur son assurance cyber	Plainte au plus tard 72 heures après la connaissance de l'atteinte, condition du versement de l'indemnité au titre de la garantie des atteintes à un système de traitement automatisé de données, dont relève le déni de service (art. 323-2 du code pénal) · déclaration à l'assureur dans le délai du contrat, qui ne peut être inférieur à cinq jours ouvrés	Police, gendarmerie ou procureur de la République · l'assureur

Une entité relevant de DORA notifie au titre de DORA, pas de NIS 2 : les deux régimes ne se cumulent pas pour la notification, sauf si la loi française retient l'option de double envoi que DORA laisse aux États membres. Cette règle vaut pour NIS 2 : elle n'écarte ni la déclaration des opérateurs d'importance vitale, ni le RGPD, ni les clauses contractuelles. En France, NIS 2 n'est pas encore transposée et le projet de loi est examiné en première lecture en séance publique à l'Assemblée nationale à partir du 7 octobre 2026 (ordre du jour de l'Assemblée consulté le 6 octobre 2026). D'ici son adoption et ses décrets, seuls les régimes existants s'appliquent : opérateurs de services essentiels et fournisseurs de service numérique issus de NIS 1, opérateurs d'importance vitale et, selon le secteur, des régimes propres comme celui des établissements de santé. Tous imposent une déclaration sans délai de l'incident qui atteint leur seuil propre, donc plus tôt que les 24 heures de la directive. Si la filiale n'est aujourd'hui ni opérateur de services essentiels, ni fournisseur de service numérique, ni opérateur d'importance vitale, ni soumise à un régime sectoriel, aucune déclaration à l'ANSSI n'est obligatoire au 1er octobre 2026. Un signalement volontaire au CERT-FR reste possible, et les obligations RGPD, contractuelles et d'assurance demeurent.

Le délai de quatre heures court à partir de la classification, la limite de vingt-quatre heures dès la prise de connaissance. Si, par exception, l'incident n'est classé majeur qu'après ces vingt-quatre heures, il se notifie dans les quatre heures suivant la classification, et le dépassement s'annonce sans retard injustifié et se motive auprès de l'autorité (règlement délégué 2025/301, art. 5, § 2 et 3). Le portail OneGate de l'ACPR est fermé de 0 h à 4 h du matin et le dimanche, alors que, pour un établissement de crédit, le week-end et les jours fériés ne suspendent ni la notification initiale ni le rapport intermédiaire : l'ACPR prévoit alors un courriel de prévenance, à l'adresse indiquée dans sa FAQ DORA en vigueur, qui ne remplace pas le formulaire, à déposer sur OneGate à la réouverture.

Pour un déni de service, l'incident est majeur s'il touche un service critique et s'y ajoute un accès malveillant non autorisé réussi, susceptible d'entraîner des pertes de données, ce qui vise le déni de service qui masque une intrusion (un tel accès remplit à lui seul le critère du service critique). Sinon, il faut franchir au moins deux autres seuils, notamment de durée, de clients touchés ou de coûts. Des vagues répétées doivent aussi, sous conditions, être comptées comme un seul incident majeur.

Chaque filiale a besoin d'une personne nommée à l'avance qui tient son horloge et la rappelle à voix haute. Les faits transmis à l'autorité financière, à l'ANSSI, aux clients et à la presse doivent rester cohérents et sans contradiction d'un destinataire à l'autre, seul le niveau de détail variant.

3. Quand l'incident devient celui des autres

Dans le scénario, l'attaque ne s'arrête pas au groupe : des clients et des partenaires voyaient des paiements ou des commandes bloqués. Pour eux, l'incident peut devenir le leur, avec leurs propres notifications à faire, et ils se tournent alors vers l'entreprise attaquée pour obtenir des éléments précis. Répondre au cas par cas et sous pression risque de produire plusieurs versions du même incident. Une fiche factuelle partageable, mise à jour à heure fixe, évite en grande partie cet écart. Elle tient en quatre rubriques, la chronologie, le périmètre touché, les mesures prises et l'heure du prochain point, et sert aussi de base aux échanges avec la presse. Les contrats méritent d'être relus dans le même esprit, car beaucoup prévoient l'information des partenaires en cas d'incident, avec leurs propres délais. La loi en ajoute : sous NIS 2, l'information des destinataires des services touchés, le cas échéant, sous DORA celle des clients dont les intérêts financiers sont touchés par un incident majeur, et sous le RGPD l'alerte du responsable du traitement par son sous-traitant.

4. Ce qu'on peut lancer dès cette semaine

- Nommer, pour chaque entité du groupe, qui qualifie l'incident et qui valide chaque notification, avec un suppléant joignable la nuit et le week-end.
- Préremplir les formulaires de notification (autorité financière, formulaire actuel de l'ANSSI pour les opérateurs de services essentiels et les fournisseurs de service numérique, CNIL) avec les parties fixes : identifiants de l'entité, contacts, description des services. Noter au même endroit le canal de secours quand un portail est fermé.
- Vérifier la chaîne de protection contre le déni de service : contrat, capacité souscrite, contacts d'escalade, date du dernier test.

- Lister les clients et partenaires qui dépendent des services du groupe, et les clauses qui obligent à les informer, avec leurs délais.
- Relire la police d'assurance cyber avec le juridique : la plainte sous 72 heures, le délai de déclaration, et ce qui est couvert en cas de simple indisponibilité.
- Rejouer un exercice court tous les six mois en changeant une variable, par exemple un déni de service qui masque une intrusion, ou un agent IA ou un compte de service compromis qui agit avec des droits légitimes.

Amin Hasbini · mahasbini.org

Références : Règlement (UE) 2022/2554 (DORA), art. 1er, § 2, 18, 19 et 46 · Règlement délégué (UE) 2024/1772, art. 6, 8 et 9 (classification des incidents, incidents récurrents à l'art. 8, § 2) · Règlement délégué (UE) 2025/301, art. 5 (délais de notification, classification tardive au § 2, week-ends et jours fériés aux § 4 et 5) · Règlement d'exécution (UE) 2025/302 (formulaires) · Directive (UE) 2022/2555 (NIS 2), art. 4 et 23 · FAQ DORA de l'ACPR (horaires de OneGate et courriel de secours), consultée le 6 octobre 2026 · Loi n° 2018-133 du 26 février 2018, art. 7 et 13 · Code de la défense, art. L. 1332-6-2 · Code de la santé publique, art. L. 1111-8-2 · Règlement (UE) 2016/679 (RGPD), art. 33 et 34 · Code des assurances, art. L. 12-10-1 et L. 113-2 · Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (dossiers législatifs du Sénat et de l'Assemblée nationale). Cette note ne constitue pas un avis juridique.