Checklist de notification d'incident NIS2

Ce qu'il faut préparer avant un incident, et ce qu'il faut envoyer au CCB dans les 24 heures, 72 heures et un mois après un incident significatif.

NIS2 Aware · nis2aware.eu · novembre 2026

Avant un incident : être prêt

- [ ] **Rédigez une procédure d'incident d'une page**
  Qui appeler, qui décide, qui notifie, et comment les joindre en dehors des canaux habituels.
- [ ] **Définissez ce qu'est un incident significatif pour vous**
  Traduisez les critères (perturbation grave, pertes financières, dommages à des tiers) en seuils concrets pour vos services.
- [ ] **Désignez les personnes qui notifient le CCB, avec des suppléants**
  L'alerte précoce est due dans les 24 heures, y compris le week-end et les jours fériés.
- [ ] **Gardez les contacts et la procédure disponibles hors ligne**
  La messagerie et les systèmes peuvent être indisponibles pendant un incident.
- [ ] **Veillez à conserver les journaux assez longtemps**
  Vous en aurez besoin pour comprendre l'incident et rédiger les rapports.
- [ ] **Préparez des modèles de messages**
  Pour le CCB, pour les clients concernés et pour le personnel.
- [ ] **Testez la procédure lors d'un exercice**
  Un court exercice sur table une fois par an révèle les lacunes.

Dans les 24 heures : alerte précoce

- [ ] **Envoyez l'alerte précoce au CCB**
  Dans les 24 heures après avoir pris connaissance de l'incident significatif.
- [ ] **Indiquez s'il pourrait être causé par des actes illicites ou malveillants**
  Une première impression suffit à ce stade.
- [ ] **Indiquez s'il pourrait avoir un impact transfrontière**
  Par exemple si des services dans d'autres pays de l'UE sont touchés.

Dans les 72 heures : notification d'incident

- [ ] **Envoyez la notification d'incident**
  Dans les 72 heures après avoir pris connaissance de l'incident, en complétant l'alerte précoce.
- [ ] **Donnez une première évaluation de la gravité et de l'impact**
  Quels services, combien d'utilisateurs, pendant combien de temps.
- [ ] **Partagez les indicateurs de compromission disponibles**
  Par exemple des adresses IP, domaines ou fichiers suspects.

Dans le mois : rapport final

- [ ] **Décrivez l'incident en détail**
  Y compris sa gravité et son impact.
- [ ] **Expliquez le type de menace ou la cause**
  Ce qui s'est passé, comment l'attaquant est entré, ou ce qui a failli.
- [ ] **Listez les mesures d'atténuation appliquées et en cours**
  Ce que vous avez fait pour l'arrêter et éviter qu'il se reproduise.
- [ ] **Mentionnez l'éventuel impact transfrontière**
  Le cas échéant.
- [ ] **Si l'incident est toujours en cours, envoyez un rapport d'avancement**
  Le rapport final suit alors dans le mois après le traitement de l'incident.

Après l'incident

- [ ] **Informez les destinataires de vos services si nécessaire**
  Les clients touchés par l'incident, et les mesures qu'ils peuvent prendre.
- [ ] **Organisez un retour d'expérience**
  Ce qui a fonctionné, ce qui n'a pas fonctionné, ce qu'il faut changer.
- [ ] **Mettez à jour votre analyse des risques, vos mesures et votre procédure**
  Et faites rapport à l'organe de direction.

Information générale sur le cadre NIS2 belge en date de novembre 2026, pas un avis juridique. Consultez toujours les dernières informations du CCB (ccb.belgium.be et atwork.safeonweb.be).