

**FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE CYBERSECURITE**

**Déclaration :**  [ ]  initiale, [ ]  intermédiaire, [ ]  post-mortem

**Informations générales**

|  |  |
| --- | --- |
| Date de déclaration |  |
| Dénomination de l’entreprise  |  |
| Type d’entreprise |  |
| LEI ou SIREN |  |
| Pays du siège social de la maison mère de l’entreprise (si filiale d’un groupe étranger) |  |

|  |  |
| --- | --- |
| Fonction du déclarant |  |
| Adresse électronique |  |
| Téléphone(s) |  |

(Le déclarant est la personne chargée, au nom de l’entreprise, d’effectuer la présente déclaration.)

**Informations sur l’incident**

|  |  |
| --- | --- |
| Date et heure auxquelles l’incident a été constaté | Jj/mm/aaaa - hh / mm |
| Durée de l’incident si clos |  |
| Incident découvert par :  | [ ]  Interne : Préciser :Externe :[ ]  Client/adhérent[ ]  Prestataire externeSi autre, préciser :  |
| Origine de l’incident | [ ]  Négligence[ ]  Dysfonctionnement opérationnel[ ]  Malveillance interne[ ]  Malveillance externe |
| Moyens, identifiés ou supposés, mis en œuvre par l’attaquant pour s’introduire dans le système d’information ou perturber son fonctionnement :  | [ ]  Point d’eau (*drive-by compromise – watering hole*)[ ]  Hameçonnage[ ] Exploitation de sites Internet, d’applications accessibles par Internet ou de services d’accès à distance (vulnérabilité ou accès légitime)[[1]](#footnote-1)[ ]  Rebond depuis un tiers, un logiciel ou un service de confiance[ ]  Accès physique[ ]  Saturation[ ]  AutreSi autre, préciser : |
| Description des moyens mis en œuvre par l’attaquant :*Si un prestataire externe est à l’origine de l’incident, merci d’indiquer ses coordonnées.* | Champ libre |
| Objectif(s) atteints par l’attaquant : | [ ]  Intrusion dans le système d’information[ ]  Maintien dans le système d’information[ ]  Progression dans le système d’information[ ]  Atteinte au fonctionnement du système d’information ou à ses données |
|  Actions réalisées par l’attaquant : | ☐ Déni de service (DoS ou DDoS)☐ Fuite/Exfiltration de données ☐ Chiffrement de données (rançongiciel)☐ Crypto-jacking☐ Effacement des données (*wiper*)☐ Défiguration (*defacement*)☐ AutreSi autre, préciser |
| Description générale de l’incident :*Exemples :* *périmètre du système d’information affecté par l’incident, origine et déroulé de l’incident, etc.* | Champ libre |

**Impacts de l’incident**

|  |  |
| --- | --- |
| Identification des activités affectées par l’incident : | [ ]  Gestion de la relation client/adhérent[ ]  Gestion de portefeuille/gestion d’actifs[ ]  Négociations et ventes[ ]  Paiements[ ]  Règlement-livraisons[ ]  Souscription[ ]  Indemnisation des sinistres[ ]  Autre*Si autre, préciser :*  |
| Identification des services et composants affectés par l’incident : | [ ]  Applications spécifiques au secteur de l’entité[ ]  Bases de données[ ]  Systèmes comptables[ ]  Progiciels[ ]  Tout équipement matériel[ ]  Réseaux et télécommunications[ ]  Sites internet[ ]  Autre *Précisions complémentaires :*  |
| Impacts avérés ou potentiels de l’incident*Choix multiples possibles* | Impacts sur les données : [ ] Confidentialité[ ] Intégrité[ ] Disponibilité |
| Impacts pour l’entreprise : [ ] Impact sur la réputation de l’entreprise[ ] Impact financier[ ] Impact juridique (légal, réglementaire, contractuel) |
| Impacts opérationnels : [ ] Pas d’impact[ ] Impact minimal sur les services[ ] Impact modéré sur les services[ ] Impact significatif sur les services |
| % de clients/d’adhérents touchés  | [ ] 0 – 30 %[ ] 30 – 60 %[ ] 60 – 100 %  |
| % d’utilisateurs internes touchés  | [ ] 0 – 30 %[ ] 30 – 60 %[ ] 60 – 100 %  |
| Est-ce que des services essentiels (au sens de l’établissement) sont arrêtés ?  | [ ] Oui | [ ] Non |
| Localisation physique des systèmes d’information affectés par l’incident | Champ libre |
| Si ces systèmes d’information sont 1) hébergés par un ou des tiers,2) exploités par un ou des tiersMerci d’indiquer les noms de ces tiers : | Champ libre |
| À votre connaissance, est-ce que des parties prenantes externes ont été affectées par l’incident ? | [ ] Oui | [ ] Non |
| Si oui, précisez la manière dont elles l’ont été. | Champ libre |

**Traitement de l’incident**

|  |  |
| --- | --- |
| Actions conduites par l’entreprise  | ☐ Identification☐ Analyse☐ Contingentement/Endiguement☐ Arrêt de la fonctionnalité atteinte☐ Fonctionnement en mode dégradé☐ Rétablissement |
| Description des mesures techniques et organisationnelles prises et envisagées pour traiter l’incident  |  |
| L’incident a-t-il fait l’objet d’une remontée d’information en interne? | [ ]  Oui : [ ]  Au responsable de la sécurité des systèmes d’information (RSSI)[ ]  Au directeur des systèmes d'information/des opérations[ ]  Au Comité de direction[ ]  À la Direction générale[ ]  À l’organe de surveillance (ex : Conseil d’administration)[ ]  Autre, précisez :[ ]  Non |
| Un dispositif de gestion de crise a-t-il été activé ? | [ ]  Oui | [ ]  Non |

|  |  |  |
| --- | --- | --- |
| À votre connaissance, l’incident est-il connu du public ? | [ ]  Oui | [ ]  Non |
| Un prestataire de réponse aux incidents a-t-il été engagé par l’entreprise pour gérer l’incident ? | [ ]  Oui | [ ]  Non |

Si oui, coordonnées du prestataire :

|  |  |
| --- | --- |
| Dénomination sociale |  |
| Adresse postale |  |

1. Renvoie aux techniques [MITRE ATT&CK®](https://attack.mitre.org/techniques/enterprise/) suivantes : [T1190] *Exploit public-facing application, [T1133] External remote services et [T1078] Valid accounts.* [↑](#footnote-ref-1)