Réagir efficacement à une cyberattaque : l'importance d'anticiper sa communication

Union des Villes et Communes de Wallonie asbl

Wallonie

Webinaire – 2 décembre 2022

Nos invité.es

Fanny COTON
Avocate
LEXING

Patrick VANDOORNE
Directeur - Com4you
Professeur - IHECS

Fabian NAMUR
Directeur de la communication
Vivalia

Menu de la séance

01 **Cyberattaque et communication : quelles sont les obligations de votre organisation ?**

02 **Anticiper sa communication en cas de cyberattaque : que doit comporter votre plan de communication ?**

03 **La gestion d'une cyberattaque : quels enseignements tirer de la communication de mon organisation ?**

01 02 03

Cyberattaque et communication : quelles sont les obligations de votre organisation ?

Fanny COTON

Lexing

Que faut-il prendre en compte ?

Dans un monde idéal :

- Avant :
  - Mesures techniques et organisationnelles de sécurité des systèmes et des installations
  - Mécanisme de gestion des incidents
- Pendant :
  - **Plan de gestion des incidents**
  - **Procédure de gestion des violation de données**
  - **Registre des incidents**
  - Documentation dans un journal interne
- Après :
  - Plan de reprise d'activités
  - Suivi et audit

Textes légaux pertinents

- **RGPD**
- Directive NIS et sa transposition en droit belge : Loi 7 AVRIL 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique
- **Directive NIS-2 (nouveau !)** : étend le champ d'application aux entités de l'administration publique.
  - Adoptée mais pas encore publiée.
  - La Belgique disposera de 21 mois pour la transposer : fin 2024/début 2025.
- **Directive UE 2019/1937 sur les lanceurs d'alerte** : Canal de signalement interne

RGPD : violation des données personnelles

- *de manière **accidentelle***
- ***ou illicite***

- *destruction*
- *perte*
- *altération*
- *divulgation non autorisée*
- *accès non autorisé*

Atteinte à :
Confidentialité / Disponibilité / Intégrité

RGPD : quels types de cyberattaques sont concernés ?

- Installation de virus
- Phishing
- Ransomware
- Vol ou perte de données
- Paralysie des systèmes et indisponibilité des informations
- Attaque par déni de service

Chaque fois atteinte à :
Confidentialité / Disponibilité / Intégrité

Mais aussi…

- Perte d'une clé USB contenant un fichier Excel avec les données de parents d'élèves
- Perte d'une mallette contenant les soumissions à un marché public
- …

Chaque fois atteinte à :
Confidentialité / Disponibilité / Intégrité

Directive NIS-2

- Entités publiques = **entités essentielles**
- **Peu importe leur taille**
- Est une entité publique si rassemble les critères suivants :

- établie pour rencontrer des **besoins d'intérêt général**
- n'a **pas de caractère industriel ou commercial** ;
- **personnalité juridique** ou juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique;
- **financée majoritairement par l'Etat** les collectivités régionales ou d'autres organismes de droit public ; ou leur gestion est soumise à un contrôle de la part de ces autorités ou organes ; ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public ;
- a le pouvoir de prendre des **décisions affectant les droits des personnes.**

Comment se préparer ?

Quel niveau de sécurité ?

Obligation légale : Approche **par risque**

- ✓ Sensibiliser les utilisateurs ;
- ✓ Authentifier les utilisateurs ;
- ✓ Gérer les habilitations ;
- ✓ Tracer les accès ;
- ✓ Sécuriser les postes de travail ;
- ✓ Protéger le réseau informatique interne ;
- ✓ Sécuriser les serveurs et les sites web ;
- ✓ Prévoir des back-ups ;
- ✓ Archiver de manière sécurisée ;
- ✓ Encadrer la maintenance et la destruction des données ;
- ✓ Gérer la sous-traitance ;
- ✓ Protéger les locaux ;
- ✓ Chiffrer,…

Etablir des procédures

- Procédure de gestion des incidents (« **Security Breach Management Policy** »)
- Procédure en cas de violation des données (« **Data Breach Procedure** » ou « DBP »)
- Plan de continuité d'activités (« **Business Continuity Plan** » ou « BCP »)
- Plan de reprise d'activités (« **Disaster Recovery Plan** » ou « DRP »)

Etablir un canal de signalement interne pour signaler des *irrégularités*

Directive UE 2019/1937
sur les lanceurs d'alerte

Notamment concernant :

- **la protection des données à caractère personnel,**
- **la sécurité des réseaux et des systèmes d'information.**

POUVOIRS LOCAUX WALLONS

Texte en attente des avis de l'APD et du C. Etat.

Début 2023

Obligatoire pour :

- **Communes**
  > 10 000 habitants
- **Pouvoirs locaux**
  > 50 travailleurs

Comment réagir ?

Exemple

- Une commune de 20.000 habitants.
- Les serveurs subissent une attaque. Ils sont indisponibles.
- Une rançon est réclamée.
- Menace de publier les données si la rançon n'est pas payée (notamment les listes des élèves et parents d'élèves des écoles de la commune, avec leur numéro de registre national).

Obligations de notification

RGPD	NIS/ NIS-2
72 h	NIS -2 : 24 h alerte précoce 72 h notification
Si risque	NIS : si impact significatif NIS-2 : si impact important
À l'APD	- au CSIRT national ; - à l'autorité sectorielle - au CCB
Si risque élevé : aux personnes concernées	NIS-2 : aux destinataires des services qui sont potentiellement affectés par une cybermenace importante
Sanctions ~~administratives et~~ pénales	Sanctions administratives ? Pénales ?

Concrètement

Notification à l'APD

- https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles

Notification au CSIRT

- https://www.cert.be/fr/signaler-un-incident

Documenter ce qui est fait !!!

Exemple

Commune victime d'une cyberattaque

- Prévenir APD car risques pour les données personnelles des parents/enfants
- Prévenir CSRIT
- Prévenir les parents

Quelles sanctions possibles ?

Poursuites administratives

19 NOV 2021

L'APD contacte la COCOM suite à une potentielle fuite de données de la plateforme Bruvax

13 OCT 2021

L'APD se penche sur une potentielle faille de sécurité de l'application CovidScan

ACTUALITÉS

Fuite de données Facebook : l'APD intervient et encourage les citoyens à faire valoir leurs droits

La presse a fait état d'une fuite de données issues du réseau social Facebook qui concernerait des millions d'utilisateurs, dont 3 millions ...

Publié le 7 avril 2021

Poursuites pénales

	Infraction
RGPD	Absence de notification à l'APD
	Absence de notification à la personne concernée
NIS	Absence de notification de l'incident
NIS 2	?

Signalement direct à l'APD

Divulgation publique

Conclusion

Anticiper pour que le plan se déroule sans accro :

- Avant :
  - Mesures techniques et organisationnelles de sécurité des systèmes et des installations
  - Mécanisme de gestion des incidents
- Pendant :
  - **Exécution du plan de gestion des incidents**
  - **Notification de l'incident à une autorité de contrôle et/ou aux personnes affectées**
  - Documentation dans un journal interne
- Après :
  - Plan de reprise d'activités
  - Suivi, d'audit et de contrôle

Anticiper pour :

- Limiter le risque d'incident
- Communication maîtrisée
  - Limite le préjudice d'image
  - Limite la surcharge de travail
- Éviter un signalement sur la place publique
- Circonstances atténuantes en cas de poursuites pénales/administratives

Merci pour votre attention !

Des questions ?

Fanny COTON
Spécialiste en droit de la vie privée

f.coton@lexing.be
T +32 2 381 11 91

01 02 03

Anticiper sa communication en cas de cyberattaque : que doit comporter votre plan de communication ?

Patrick VANDOORNE

Come4you / IHECS

Anticiper sa communication : préalable

- Faire – actualiser l'analyse de risques
- Intégrer cette analyse aux plans d'urgences
- Communiquer les plans d'urgences à toutes les personnes concernées, surtout en interne
- Faire des exercices en intégrant la communication (coordination planu – D5 – chargé.e de com,…)

→ Une bonne communication de crise repose obligatoirement sur une bonne analyse des risques

Anticiper sa communication : préparation

- Pour chaque « scénario » issu de l'analyse de risques, préparer les messages correspondants - internes et externes - bien identifier les différents publics
- Toujours favoriser la stratégie de la transparence, dans le respect du cadre légal, sauf si cette communication met des personnes où la structure en danger
- Mettre en place les procédures de remontée de l'information (réseau interne…)

Anticiper sa communication : préparation

- Pour les responsables de com : préparer vos outils
  - → Fichiers de contacts - messages - médias - les parties prenantes - etc. – Avoir tous les documents en LOCAL sur votre PC
  - → Préparez un site « noir »
  - → Déterminer qui peut parler à l'extérieur - ce qu'il peut dire - et le communiquer en interne

Au départ de la crise, vous avez 0 seconde pour communiquer : soyez prêts

Anticiper sa communication: préparation

- Une bonne communication de crise s'enracine dans une communication quotidienne performante

→ Si votre communication quotidienne n'est pas fluide, transparente et crédible, il en sera de même pour votre communication de crise

- La communication n'est pas un coût, c'est un investissement

→ L'imprévu n'existe pas – il n'y a que ce que nous refusons d'anticiper (cf. toutes les crises des 20 dernières années)

Anticiper sa communication : préparation

Depuis 2018, le rapport annuel
de la Fédération européenne des Risk Managers,
classe les cyberattaques en n°1

Anticiper sa communication : pendant la crise

- Communiquer rapidement : le premier donne le ton
- Organiser la veille pour savoir ce que l'on dit de vous
- Attention à bien différencier
  - Communication de gestion de crise et…Communication de crise

Gérer la situation

Informer sur la situation et la gestion

Anticiper sa communication : pendant la crise

- Ne pas oublier les médias classiques
- Utiliser votre site « noir » comme point unique
  et y faire pointer tous les autres canaux
- Adopter le principe du centre de crise pour la composition de message
  - We know — ce que nous savons (faits)
  - We do — ce que nous faisons
  - We care — nous sommes conscients de… (empathie)

Anticiper sa communication : pendant la crise

- Communiquer régulièrement, notamment avec la presse
- Oser dire « je ne sais pas… » à condition de bien expliquer pourquoi et de fixer un RV pour des compléments d'information
- Une fois terminé, faire le « storytelling » de la crise

Merci pour votre attention

Patrick Vandoorne
Directeur Com4you
Professeur à l'IHECS

01 02 03

La gestion d'une cyberattaque : quels enseignements tirer de la communication de mon organisation ?

Fabian NAMUR
Vivalia

01
La crise et sa gestion

Samedi 14 mai 2022

« Ceci n'est malheureusement pas une fake news. Nous sommes victimes d'une attaque informatique. Instructions données de couper l'internet et shutdown l'IT »

Impact direct

- ✓ 1 500 machines et 200 serveurs détruits par le virus
  - ➢ A reformater : zone sale – neutre – propre
- ✓ 400 Gb de données volées (messagerie, données RH…)
- ✓ Plus aucune connexion avec l'extérieur → nous avons coupé pour nous protéger
- ✓ Plus aucune connexion entre nos machines, les hackers ont coupé tous les flux
  - ➢ Exemple d'impact : radiologie/scanner et salle d'op'
- ✓ Plus de centrale téléphonique

Mode dégradé

- ✓ 6 300 consultations/semaine à gérer dès le lundi matin
- ✓ Opérations, suivis médicaux, dialyse, radiologie, etc.

Gestion de la crise

- Déclenchement du Plan d'Urgence Hospitalier (PUH) - procédures
- Mise en place de cellules de crise transversales et locales
- Cascade décisionnelle et de communication

Restart / Rebuild

Mode « sortie de crise » / réponses

- Informatique =
  - ✓ Restart : remise en route progressive
  - ✓ Rebuild : reconstruction
- Médical : labo, radiologie, dossiers médicaux
  - ✓ Assurer la sécurité des patients et services vitaux et maintenir la médecine d'urgence
- Téléphonie : call center 0800 (+ de 40.000 appels)
- RH / paie du personnel
- Etc.

Situation évolutive = adaptation permanente !

02
La crise et sa communication

Mode « Com de crise »

- Communication de crise ?
  - Evénement
    - Impact négatif
      - Communication de crise
- Expérience COVID !

Mode « Com de crise »

- Prise de connaissance du problème = évaluation… incident ou crise réelle ?
- Prendre les premières informations, faire valider, dégager les lignes de force
- Définir le message, les publics cibles et la priorité dans l'ordre d'information
- Etablir de quels moyens de communication on dispose
- Planifier sa communication
- COMMUNIQUER !

Mode « Com de crise »

Fabian Namur
Admin · 14 mai, 07:44 ·

⚠️⚠️L'informatique de Vivalia victime d'un incident majeur

Cette nuit, les systèmes informatiques de Vivalia ont été victimes d'une attaque, un virus qui a bloqué tous les serveurs Windows de notre institution.

➡️ Ce matin, plus aucun ordinateur n'est utilisable au sein de Vivalia et Internet a été coupé.

Nos équipes travaillent sans relâche pour tenter de rétablir la situation, elles analysent l'étendue des dégâts.

➡️ Il est prématuré de pouvoir fixer une échéance pour un retour à la normale.

Nous vous demandons de rester calme, de recourir à d'autres moyens pour continuer de travailler (retour au papier...) malgré ces conditions difficiles. Merci déjà de votre compréhension.

Nous vous tenons informés de l'évolution de la situation via notre page Facebook privée qui n'est pas impactée par la panne. C'est par ce canal que nous vous tiendrons informés de l'évolution de la situation. Merci de bien vouloir informer vos collègues.

Pour la cellule de crise de Vivalia,

Voir les statistiques — Couverture de la publication : 1,6 K

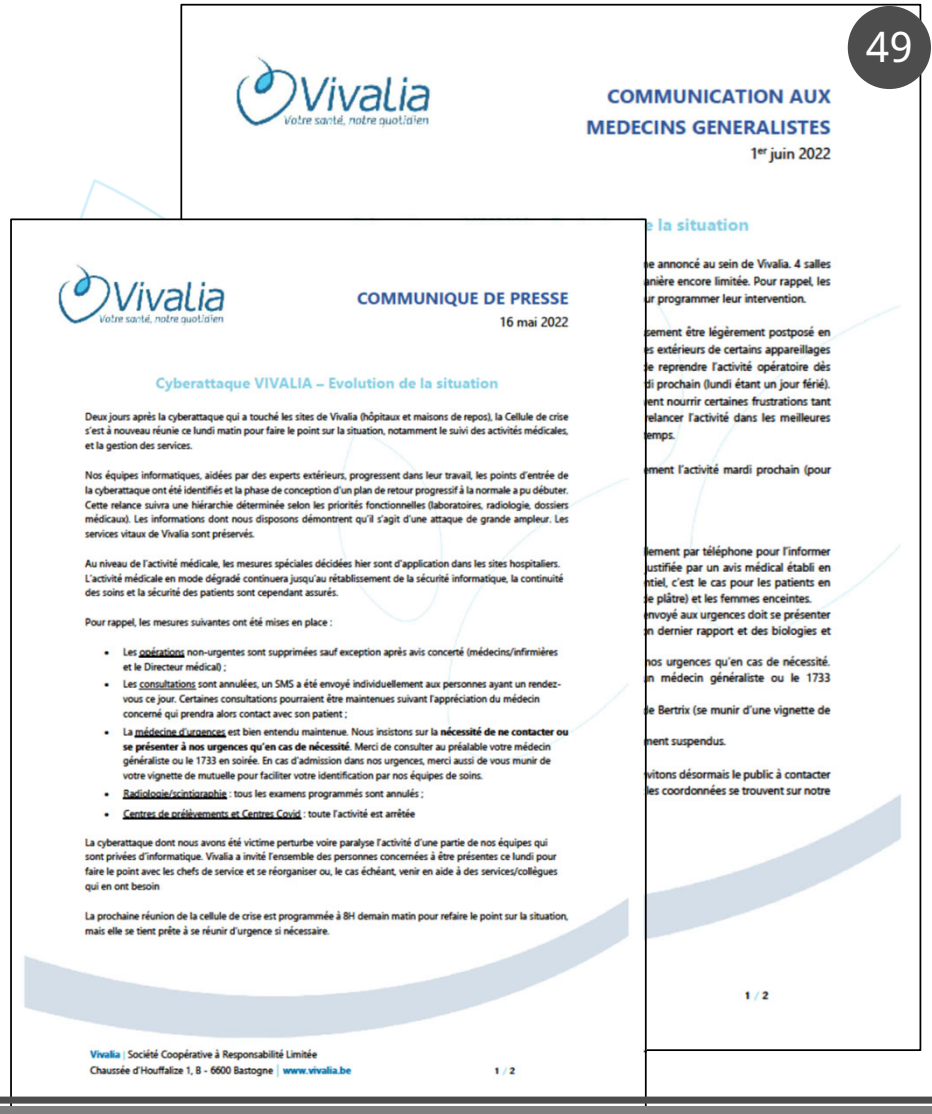
Nancy Cavelier, Lise Grandjean et 55 autres personnes — 51 commentaires

J'aime — Commenter

Voir 26 commentaires précédents — Tous les commentaires

Mode « Com de crise »

- Communication dense = transparence
- Suivi des cellules de crise → com systématique
- Proximité, ouverture
- Gestion de la tension
- Compréhension = ~~rumeurs~~
- Structuration selon les publics cibles et leurs attentes



Vivalia
Votre santé, notre quotidien

COMMUNICATION AUX MEDECINS GENERALISTES
1er juin 2022

Vivalia
Votre santé, notre quotidien

COMMUNIQUE DE PRESSE
16 mai 2022

Cyberattaque VIVALIA – Evolution de la situation

Deux jours après la cyberattaque qui a touché les sites de Vivalia (hôpitaux et maisons de repos), la Cellule de crise s'est à nouveau réunie ce lundi matin pour faire le point sur la situation, notamment le suivi des activités médicales, et la gestion des services.

Nos équipes informatiques, aidées par des experts extérieurs, progressent dans leur travail, les points d'entrée de la cyberattaque ont été identifiés et la phase de conception d'un plan de retour progressif à la normale a pu débuter. Cette relance suivra une hiérarchie déterminée selon les priorités fonctionnelles (laboratoires, radiologie, dossiers médicaux). Les informations dont nous disposons démontrent qu'il s'agit d'une attaque de grande ampleur. Les services vitaux de Vivalia sont préservés.

Au niveau de l'activité médicale, les mesures spéciales décidées hier sont d'application dans les sites hospitaliers. L'activité médicale en mode dégradé continuera jusqu'au rétablissement de la sécurité informatique, la continuité des soins et la sécurité des patients sont cependant assurés.

Pour rappel, les mesures suivantes ont été mises en place :

- Les opérations non-urgentes sont supprimées sauf exception après avis concerté (médecins/infirmières et le Directeur médical) ;
- Les consultations sont annulées, un SMS a été envoyé individuellement aux personnes ayant un rendez-vous ce jour. Certaines consultations pourraient être maintenues suivant l'appréciation du médecin concerné qui prendra alors contact avec son patient ;
- La médecine d'urgences est bien entendu maintenue. Nous insistons sur la **nécessité de ne contacter ou se présenter à nos urgences qu'en cas de nécessité**. Merci de consulter au préalable votre médecin généraliste ou le 1733 en soirée. En cas d'admission dans nos urgences, merci aussi de vous munir de votre vignette de mutuelle pour faciliter votre identification par nos équipes de soins.
- Radiologie/scintigraphie : tous les examens programmés sont annulés ;
- Centres de prélèvements et Centres Covid : toute l'activité est arrêtée

La cyberattaque dont nous avons été victime perturbe voire paralyse l'activité d'une partie de nos équipes qui sont privées d'informatique. Vivalia a invité l'ensemble des personnes concernées à être présentes ce lundi pour faire le point avec les chefs de service et se réorganiser ou, le cas échéant, venir en aide à des services/collègues qui en ont besoin

La prochaine réunion de la cellule de crise est programmée à 8H demain matin pour refaire le point sur la situation, mais elle se tient prête à se réunir d'urgence si nécessaire.

Vivalia | Société Coopérative à Responsabilité Limitée
Chaussée d'Houffalize 1, 8 - 6600 Bastogne | www.vivalia.be

1 / 2

- Associer tout le monde, proximité
- Inquiétudes → compréhension

Gestion de la presse

- Hyper sollicités
- Priorité = interne
- Organisation et méthode
- Message réaliste, factuel, répondre aux inquiétudes, tenter de rassurer
- Gestion de la *crisis space*
- Dir com' : gestion, barrage, formation

Volet judiciaire

- Volet judiciaire
- Collaboration avec le parquet fédéral
- Consignes

03
Conseils pour la com de crise

Conseils com de crise

- Prévoir et anticiper
- Développer des outils pour fonctionner de manière indépendante
- Matériel performant et à jour
- Désigner, former des personnes ressources / Organiser les rôles
- Connaître sa « maison »
- Garder la maîtrise de l'info
- Être résistant !!!!

Où trouver de l'aide ?

- **CERT** (Cyber Emergency Response Team), service du Centre pour la Cybercriminalité en Belgique
  → www.cert.be
- **SPF Stratégie et appui** : https://bosa.belgium.be/fr/search?search=COMM+Collection
- **Centre de crise national** : https://centredecrise.be/fr/documentation/publications
- **UVCW** : https://www.uvcw.be/publications/1 + formations
- Etc.
- Etablir ou développer des contacts et partages avec d'autres organismes, sociétés, etc.

Merci de votre attention !

www.vivalia.be

Pour aller plus loin…

Nos webinaires « Nouvelles technologies » en replay :
https://www.uvcw.be/formations/webinaires

✓ **Nos formations « Communication»**
https://www.uvcw.be/formations/list/communication
- ***Maîtriser une communication de crise***

✓ **Nos formations « Management de la donnée»**
https://www.uvcw.be/formations/list/data
- ***Que faire en cas de fuite de données à caractère personnel ?***

Votre espace eCampus
Procédure de connexion : https://vimeo.com/518713611/f3c95176c9