

SÉCURITÉ INFORMATIQUE À MORGES

Présenté par Jean-Luc Blanc, ingénieur cybersécurité

📍 Morges, le 25.02.2026

✉ jean-luc.blanc@morges.ch



SOMMAIRE

- Effectif de l'équipe informatique
- Plans d'urgence et de continuité
- Exercice national de gestion de crise
- Sensibilisation et formation des utilisateurs au phishing
- Quick Wins

EFFECTIF DE L'ÉQUIPE INFORMATIQUE

- 1 chef de service
- 3 ingénieurs système
- 1 ingénieur en cybersécurité

Dans le cadre de la cyberadministration :

- 1 responsable de la transition numérique (membre du greffe)

PLANS D'URGENCE

- S'utilise comme une marche à suivre
- Permet d'avoir une succession de gestes planifiés dans une situation de crise
- On ne cède pas à la panique, puisqu'on a un plan

PLANS D'URGENCE

- Précise les responsabilités
- Indique les contacts en cas de crise (police, CSIRT, ...)
- Prépare à l'avance la communication interne comme externe
- Nécessite de bien connaître son infrastructure

PLANS D'URGENCE

- Ne pas négliger l'aspect forensique (sauvegarder les preuves, noter les événements)
- Note les étapes pour rétablir la situation après un incident
- Anticipe les impacts des mesures d'urgence sur les activités de l'administration

PLANS DE CONTINUITÉ

- Permet de fonctionner en mode dégradé
- S'active sur la période où la totalité ou une partie de l'informatique ne serait plus disponible
- Doit être réfléchi et défini par chaque service ou association
- Précise les tâches à effectuer, leurs priorités, y a-t-il une alternative sans informatique (description détaillée)
- A partir de cette liste, l'informatique sait dans quel ordre elle doit rétablir les services

EXERCICE NATIONAL DE GESTION DE CRISE

- Exercice national g rer par la conf d ration et les cantons
- Pr sence d'un observateur neutre afin de rendre un retour critique
- D but de la crise d s 9H00 – Fin de la crise vers 18H00
- D placement de tous les membres de la cellule de gestion de crise dans une salle d di e
- Pr sence de membres du Greffe, de la Communication, de la Police et de l'Informatique
- Communication constante avec les autorit s cantonales
- Sc nario rapidement identifi e : Attaque DDOS
 - Une attaque DDOS est une cyberattaque qui permet de noyer nos serveurs sous un grand nombre de requ te afin de perturber notre infrastructure et notre r seau
- Identit  de l'attaquant rapidement r v l e -> Revendication de l'attaque

EXERCICE NATIONAL DE GESTION DE CRISE

- Utilisation du plan d'urgence pour gérer la crise
- Attaque DDOS couplé à des mails de phishing entre 2 vagues DDOS
- Recommandation de l'informatique : S'isoler du réseau extérieur
 - Décision prise suite à la connaissance de l'acteur malveillant
 - L'attaque DDOS n'est pas leur attaque principale, c'est une diversion
 - Vont probablement tenter d'infecter notre réseau avec un ransomware
 - Donc on s'isole du monde extérieur, afin de s'immuniser à cette attaque en 2 temps
 - Stratégie adverse vérifiée suite à la vague de mails de phishing reçue, contenant un malware
- Retour d'expérience :
 - Le plan d'urgence nous a aidé dans notre prise de décision durant la journée
 - Quelques améliorations notables ont été faites au plan
 - Relever l'importance de connaître l'identité de l'attaquant

SENSIBILISATION ET FORMATION DES UTILISATEURS AU PHISHING

- Sensibilisation au phishing
- Campagne de phishing interne
- 3 niveaux définis
- Adaptation au fil du temps
- Évolution de l'échec aux phishings
- Incrémentation du niveau de difficulté des campagnes de phishing

QUICK WINS - DÉFINITION

- Mesure technique ou organisationnelle
- Permet de maximiser les gains en sécurité informatique
- Recherche à minimiser les efforts à fournir
- L'objectif, c'est de monter en maturité rapidement sans dépenser trop de ressources

QUICK WINS - TECHNIQUE

- Instauration de gestionnaire de mots de passe
- Activation de l'authentification à multi-facteurs
- Gestion de ses mises à jours
- Mise en place d'une solution d'anti-virus / EDR

QUICK WINS - ORGANISATIONNELLE

- Mise en place de campagne de formations
- Mise en place de campagne de phishing
- Politique de mots de passe plus strictes
- Mise en garde sur les lecteurs de données amovible (Clé USB, disque dur externe, CD...)
- Verrouillage de l'ordinateur quand on se lève de son bureau

MERCI POUR VOTRE ATTENTION

📍 Morges, le 25.02.2026

✉ jean-luc.blanc@morges.ch

