cinémathèque suisse

Les défis de la sécurité informatique du patrimoine numérique
Herausforderungen für die IT-Sicherheit des digitalen Erbes
Le sfide della sicurezza informatica del patrimonio digitale
The challenges of digital heritage cybersecurity

Introduction

- Dans cette présentation, nous aborderons plusieurs points essentiels concernant la sécurité informatique du patrimoine numérique. Voici les principaux sujets que nous traiterons :

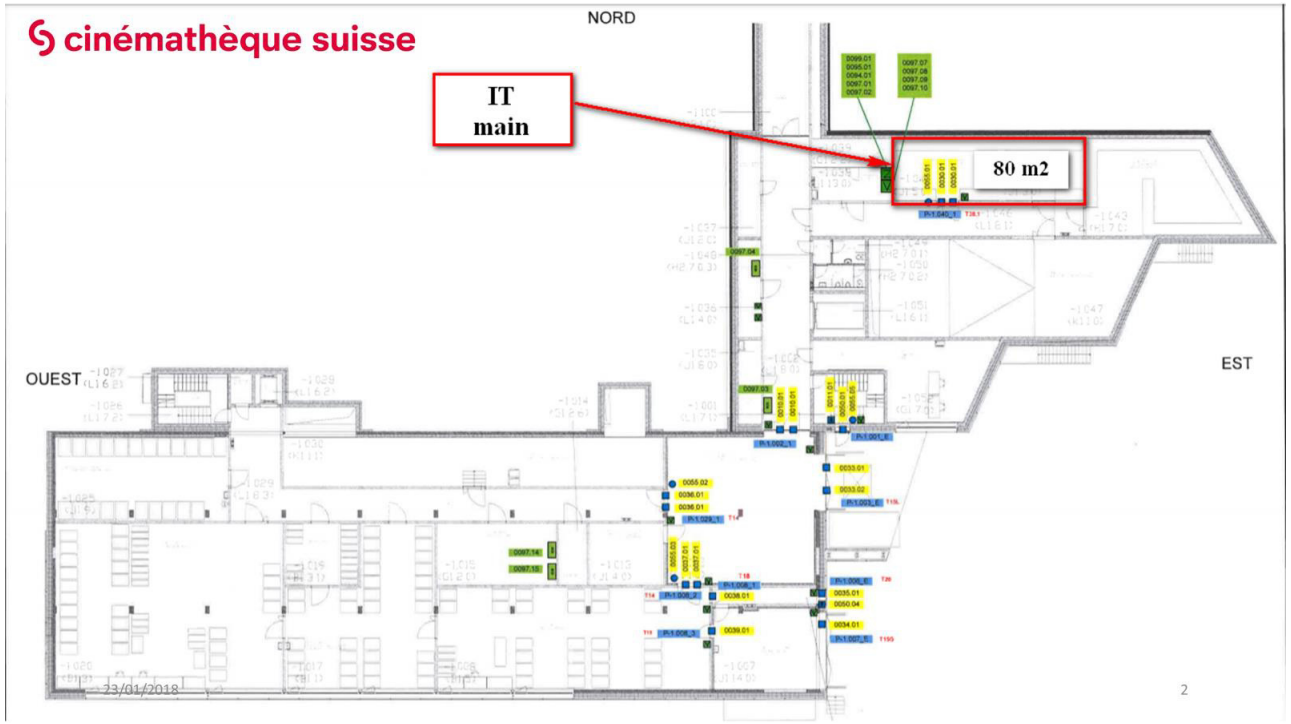
  - Présentation générale de l'infrastructure informatique de la Cinémathèque Suisse (CS)
  - Description des types de contenus gérés par les différents pôles.
  - Gestion informatique du patrimoine numérique
  - Cyberattaque - Partage d’expérience
  - Conclusions et recommandations
  - Session de questions (selon le temps disponible)

cinémathèque suisse

Infrastructure informatique de la Cinémathèque Suisse

cinémathèque suisse

Infrastructure informatique de la Cinémathèque Suisse



cinémathèque suisse

Infrastructure informatique de la Cinémathèque Suisse

Description des pôles et des contenus gérés

- Pôle Patrimoine
  - Le rôle du pôle patrimoine est de préserver et valoriser les biens culturels et historiques, ainsi que de promouvoir leur protection et transmission aux générations futures (Films, affiches, photos, livres, etc).
- Pôle Valorisation
  - Le pôle valorisation a pour rôle de promouvoir et développer les actifs culturels et patrimoniaux, en maximisant leur impact économique, éducatif et touristique.
- Pôle Ressources et Projets
  - Le pôle ressources et projets a pour rôle de gérer et optimiser les ressources nécessaires à la réalisation des projets, en assurant leur coordination et suivi pour atteindre les objectifs fixés.

Gestion informatique du patrimoine numérique

- Inventaire

Un inventaire à jour de tous les objets de la collection est essentiel pour définir une stratégie de sauvegarde ou d'archivage à long terme.

- Classement
  - Catégoriser les objets de la collection pour pouvoir définir leur criticité. Définir le type des données et déterminer la stratégie de sauvegarde appropriée à mettre en place.

- Stratégie de conservation à long terme

Exemple d'une stratégie globale.

La Cinémathèque suisse a décidé de préserver l'archive numérique de l'institution sur des supports informatiques de type « bande LTO » (Linear Tape Open). Idéal pour la sauvegarde, la restauration et l'archivage de fichiers de grande envergure, le LTO est un format de stockage extrêmement fiable et durable destiné aux entreprises gérant un grand volume de données.

cinémathèque suisse

Gestion informatique du patrimoine numérique

Stratégie de conservation à long terme → Plan d'urgence

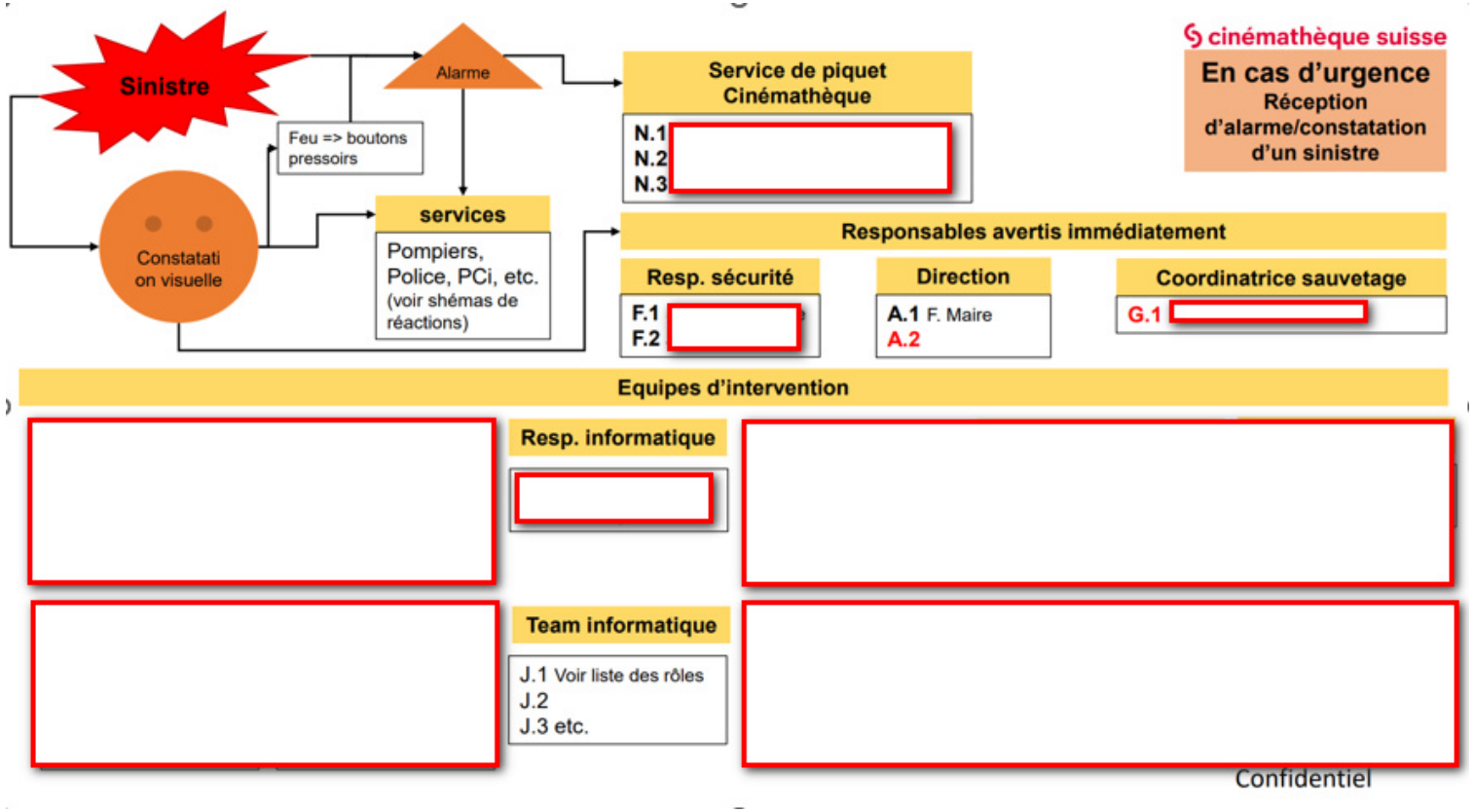
Un plan d'urgence est essentiel pour réagir efficacement en cas de crise. Voici les points clés à inclure :

1. **Identification des risques** : Analyse des dangers potentiels (naturels, technologiques, sanitaires, etc.).
2. **Rôles et responsabilités** : Définition claire des responsabilités pour chaque membre de l'équipe.
3. **Communication** : Établissement de protocoles de communication interne et externe.
4. **Procédures d'évacuation** : Plans détaillés pour l'évacuation des personnes en danger.
5. **Mesures de protection** : Stratégies pour protéger les personnes et les biens.
6. **Ressources disponibles** : Inventaire des ressources matérielles et humaines mobilisables.
7. **Formation et exercices** : Programmes de formation régulière et simulations pour préparer les équipes.
8. **Coordination avec les autorités** : Collaboration avec les services d'urgence et les autorités locales.
9. **Plan de continuité** : Stratégies pour maintenir ou reprendre rapidement les activités essentielles.
10. **Révision et mise à jour** : Évaluation et révision régulières du plan pour l'adapter aux nouvelles menaces et situations.

Gestion informatique du patrimoine numérique

- Plan d'urgence

2. Rôles et responsabilités



Gestion informatique du patrimoine numérique

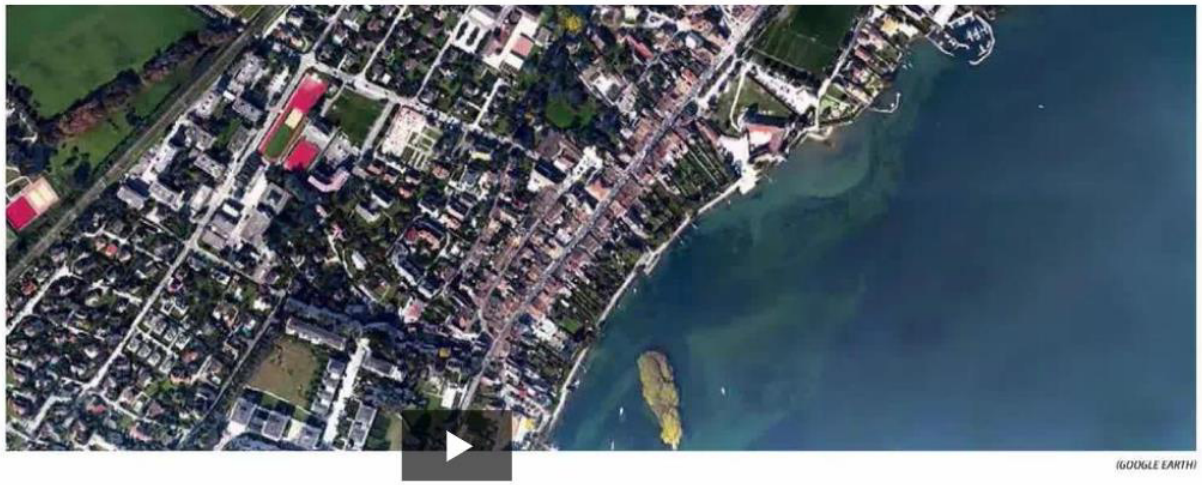
- Plan d'urgence

3. Communication

Vaud Publié le 25 août 2021 à 21:09

La gravité de la cyberattaque de la commune de Rolle sous-estimée par les autorités

TECHNOLOGIE
Contrairement à ce que la commune vaudoise avait affirmé, les données de plus de 5000 habitants sont en ligne à la suite d'un piratage. Des rapports d'évaluation des employés ou encore des demandes d'exonération fiscale sont accessibles sur le darknet



Rolle, brutalement mise à nu en ligne

Gestion informatique du patrimoine numérique

- Plan d'urgence

4. Procédure d'évacuation

5. Mesures de protection

6. Ressources disponibles

Modèle fiche d'évacuation

Un document Word A4 par fiche

Penthaz II	C07 (niveau -1)		
Cellule allée-verticale	C07 01-a		
			
Bandes LT0, sauvegardes informatiques		12 tiroirs par hauteur	
EVACUATION		Nombre de personnes : 2 par caisse	

Gestion informatique du patrimoine numérique

- Plan d'urgence

6. Ressources disponibles

Gestion informatique du patrimoine numérique

- Plan d'urgence

7. Formation et exercices

f. La collaboration avec la Protection des Biens Culturels (PBC)

Juin 2015 à la Cinémathèque suisse, semaine de collaboration préventive avec la PCi (PBC)

En cas de sinistre dans les collections, et si l'ampleur de celui-ci nécessite un soutien humain et technique, la Cinémathèque suisse collabore avec la section « Protection des Biens Culturels » de la Protection Civile du Gros-de-Vaud.

Gestion informatique du patrimoine numérique

- Plan d'urgence

8. Coordination avec les autorités

ORPC Gros-de-Vaud

Mesures d'évacuation / de protection fiche n° 530844 | 161160 | M-A | 01 | 01 | 001

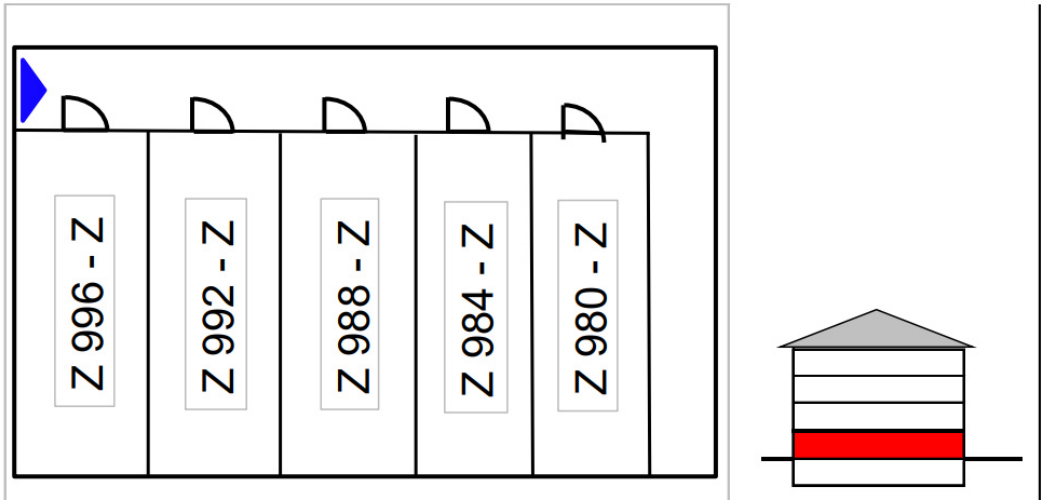
EVACUATION

si démontage, marche à suivre	*matériel*	*particularité*
CELLULE A8.4.1/0057 Z 980-111 à Z983-783, 4960 boîtes **CELLULE A8.4.2/00.056** Z 984-111 à Z 987-783, 4325 boîtes **CELLULE A8.4.3/00.055** Z 988-111 à Z 991-783, 3645 boîtes **CELLULE A8.4.4/00.054** Z 992-111 à Z 995-783, 3680 boîtes **CELLULE A8.4.5/00.053** Z 996-111 à Z 999-784, 1657 boîtes	- 2 Tentes orca - 5 tables - 5 chaises - 8 caisses (avec poignée) (cinémathèque) - Matériel d'éclairage extérieur, chemin d'accès - 10 caisse Pci (avec poignée)	- Vêtements en coton - Masque avec filtre à charbon actif (si émanation de gaz ou ouverture des boîtes) - Gants fins en vinyle. - Matériel d'écriture - Liste de rencensement

2

Par caisse

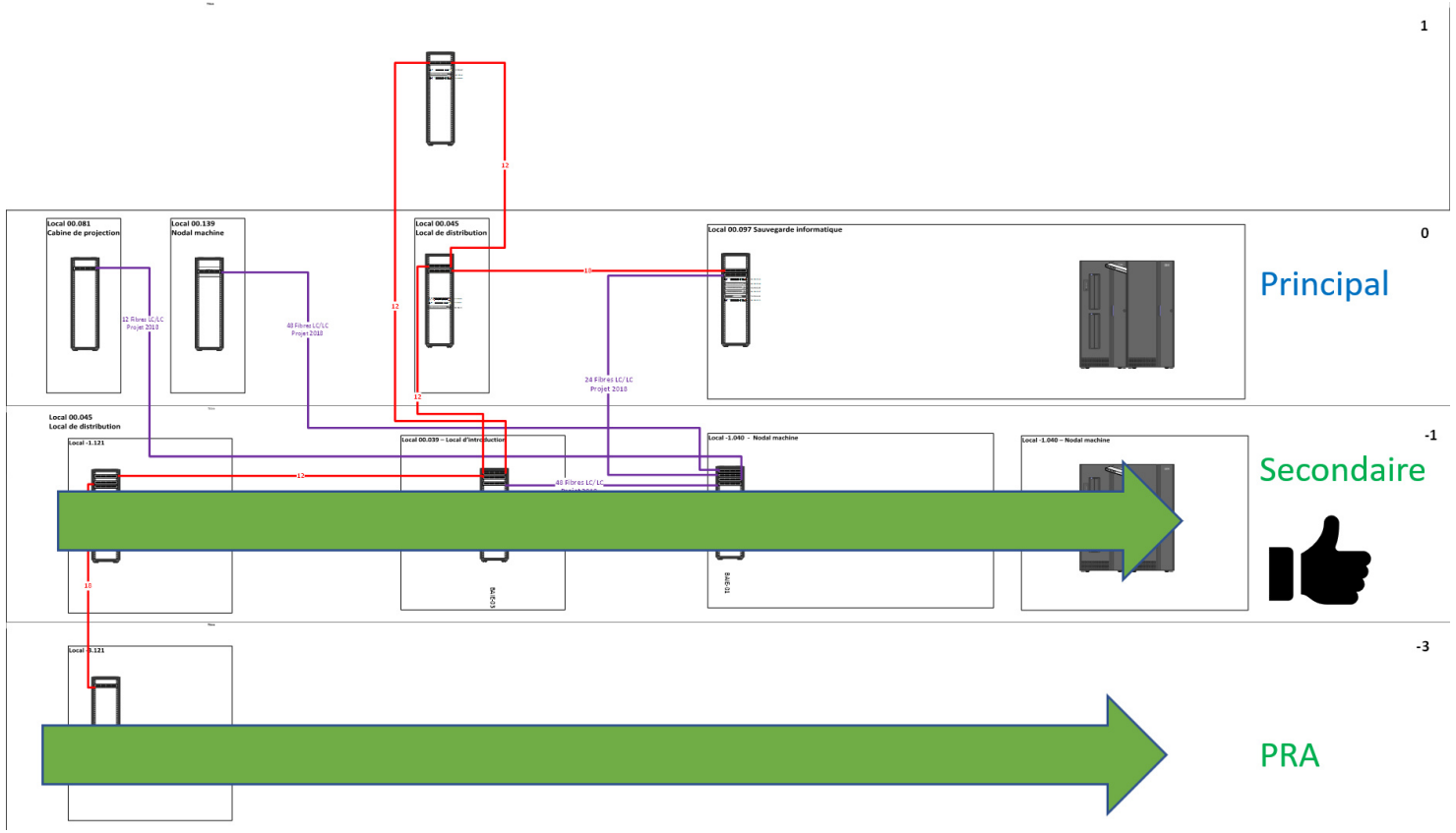
poste collecteur	Tente Orca à l'extérieur
stockage définitif	Container réfrigéré à l'extérieur
moyen de transport	Dans des caisses de tranport avec poignée, à l'horizontale



Gestion informatique du patrimoine numérique

- Plan d’urgence

9. Plan de continuité



Gestion informatique du patrimoine numérique

- Plan d'urgence

10. Révision et mise à jour

Chefs d'équipes prévention : tâches pour tenir à jour le PdU

à établir et tenir à jour par chaque chef d'équipe avec son équipe

établissement des procédures de gestion de sinistre pour son équipe	comment évacuer ? comment traiter objets sinistrés ? qui contacter à partir de quand ? etc.
établissement des fiches techniques pour un cas de sinistre	sur demande de la coordination PdU si jugé nécessaire. P.ex. : fiches d'évacuation, cartographies, fiches de documentation, liste de matériel, etc.
une fois par année Mettre à jour les procédures de gestion de sinistre pour son équipe	- vérifier les procédures et protocoles techniques en cas de sinistre pour son équipe et les mettre à jour si nécessaire - en informer la coordination PdU - en collaboration avec la coordination PdU, mettre à jour liste des contacts
une fois par année (pour équipes collections)	- communiquer des besoins de matériel à la coordination PdU
chaque fois qu'une localisation reçoit nouvellement l'attribution PBC (ou la perd) mettre à jour les fiches techniques pour son équipe (pour équipes collections)	-basé sur les infos fournis par la régie de collection, la logistique et les documentalistes film - mettre à jour à jour les fiches d'évacuation et les cartographies - en informer le comité PdU de chaque nouvelle version

Questions

- ✓ Présentation générale de l'infrastructure informatique de la Cinémathèque Suisse (CS)
- ✓ Description des types de contenus gérés par les différents pôles.
- ✓ Gestion informatique du patrimoine numérique

Suite..

- ➢ Cyberattaque - Partage d’expérience
- ➢ Conclusions et recommandations
- ➢ Session de questions (selon le temps disponible)

Conclusions et recommandations

Il n'existe malheureusement pas de solution simpliste pour se prémunir contre une récidive de cyberattaque, mais nous préconisons un ensemble de mesures résumées en 10 points :

1. **Inventaire à jour de l'infrastructure** : Maintenir un inventaire à jour de l'ensemble de l'infrastructure informatique.
2. **Mise à jour des outils de surveillance** : Tenir à jour les outils de surveillance comme les antivirus, EDR (Endpoint Detection and Response), pare-feu, routeurs, etc.
3. **Composants réseaux exposés** : Tenir à jour les composants réseaux exposés à l'extérieur.
4. **Analyse permanente des accès** : Effectuer une analyse permanente des accès à l'infrastructure informatique de la CS.
5. **Externalisation des services** : Externaliser les services nécessitant une surveillance continue (24 heures sur 24, 7 jours sur 7).
6. **Renforcement de l'équipe** : Renforcer l'équipe d'administration des systèmes.
7. **VPN et télétravail** : Limiter l'accès VPN et télétravail à la Suisse, avec gestion des exceptions.
8. **Téléphonie mobile** : Mettre en place un système de communication par SMS.
9. **PRA et directives de sécurité** : Valider et tester annuellement le Plan de Reprise d'Activité. Compléter les directives de sécurité.
10. **Formation continue** : Assurer la formation continue des collaborateurs de l'institution.

Merci de votre participation et restez vigilants…