CLUSIS

Vidéoconférence 5à7 du 11 mars 2025

«Gestion des prestataires externes»

BIENVENUE

www.clusis.ch

Un grand merci à nos sponsors pour leur soutien

CLUSIS

SPONSORS OR

ANSAM

BOLL IT Security Distribution

EVOLINK Thinking Solutions Together

ImmuniWeb® AI for Application Security

Hacknowledge

SPONSORS ARGENT

almond

e-secure

ELCA

iC CONSULT

kaspersky

Rumya

swisscom

The Positive Way WAVESTONE

SPONSORS BRONZE

C2SEC

Dina The Swiss IT Company

DREAMLAB TECHNOLOGIES

eb-Qual PART OF SWISSEXPERTGROUP

eraneos powered by AWK

KYOS

Cyberdefense

SOFTCOM

SWISS AWARE Swiss Alliance for Web Awareness Ressources, Education & Ethics

Agenda

1. Introduction de Sylvie Perrinjaquet, Présidente du Clusis
2. Présentation des intervenants
3. Intervention de Mme Anne Lupfer
4. Intervention de M. Frédéric Gaudun
5. Questions & Réponses
6. Take Aways
7. Conclusion

«Gestion des prestataires externes»

CLUSIS

Au programme:

- **Anne Lupfer,** Deputy Group CISO, Econocom
- **Frédéric Gaudun,** Chief Information Security Officer, CIGES SA

Modérateur :

- **Philippe Emery,** Consultant en management de la sécurité

2. Présentation des intervenants 1/2

Anne Lupfer : https://www.linkedin.com/in/annelupfer/

Une femme active et dynamique !

Qui a suivie deux voies qui ont forgé son expérience et sa vision :

- la gestion des risques cyber
- la formation.

Consultante senior, elle a construit :

des organisations sécurité, mis en place des stratégies de sécurité de l'information et mené des études de risques pour diverses entreprises.

Passionnée par cette thématique , elle porte les messages sur l'importance de la cybersécurité a travers ses missions, elle s'adapte en permanence en fonctions des menaces et des solutions pour être au mieux pour ses clients se remettre en question pour rester juste et pertinente.

Simultanément, la formation fut une évidence. Elle a conçu et dispensé des milliers d'heures de formation sur son sujet de prédilection : la gestion des risques.

Convaincue que la gestion des risques est un outil d'aide à la décision efficace et pertinent, elle poursuit avec passion ses actions de partage et de formation sur le sujet.

La gestion des risques facilite l'apport de réponses claires aux questions les plus complexes. En tant que Risk manager, elle se considère comme une facilitatrice permettant de mettre autour d'une même table des personnes de différentes directions pour prendre collégialement des décisions complexes et stratégiques.

2. Présentation des intervenants 2/2

Frédéric Gaudun https://www.linkedin.com/in/fgaudun/

Franco-suisse titulaire d'un Bac commercial. Depuis 20 ans en Suisse !

Anciennement engagé dans la Marine nationale en 1993, où il a servis plusieurs années dans diverses unités.

En 2000, il s'est reconvertit dans l'informatique comme administrateur système et réseau. En 2001, il rejoint une société spécialisée dans la sécurité des systèmes d'information.

Des 2005 il arrive en Suisse et rejoins une société de service.

Dés 2011, il travaille comme Responsable systèmes et réseaux pour le Canton du Jura.

Puis en 2019, il intervient en tant que RSSI pour le secteur de la santé publique, notamment pour les hôpitaux, le secteur des soins à domicile et les EMS pour le Canton de Neuchâtel.

Il est également Vice-président de l'association CLUSIS.

Le Modérateur de ce jour : Emery Philippe

https://www.linkedin.com/in/philippe-emery-124212/

Ingénieur en Télécommunications de l'Ecole d'ingénieurs de Genève. Membre du Comité de l'ISMA et Trust Advisor à la Trust Valley. Ex RSSI du TCS et d'une Banque privée, actuellement Consultant en management de la sécurité (Risques / LPD/ Vulnerability Management)

Thème très sensible !

L'info

TV • Radio • Proche-Orient • Ukraine • Suisse • Monde • Santé • Société • Environnement • Eco • Plus

La Confédération réclame des garanties de sécurité à ses fournisseurs IT

Suisse

Publié le 19 juillet 2023 à 22:51

Partager

Des garanties de sécurité réclamées par la Confédération aux entreprises IT / Le Journal horaire / 24 sec. / le 19 juillet 2023

Conséquence de la cyberattaque qui a visé l'entreprise Xplain, la Confédération réclame désormais des garanties de sécurité aux entreprises qui lui fournissent des services informatiques. Une lettre en ce sens a été envoyée à 2871 firmes.

La nécessité d'une visibilité accrue dans la chaîne d'approvisionnement

Il sera primordial d'améliorer la **visibilité** tout au long de la chaîne d'approvisionnement en 2025. Les technologies telles que l'Internet des objets (IoT) permettront de suivre en temps réel les stocks, les expéditions et les performances, offrant ainsi aux gestionnaires une vue d'ensemble précieuse.

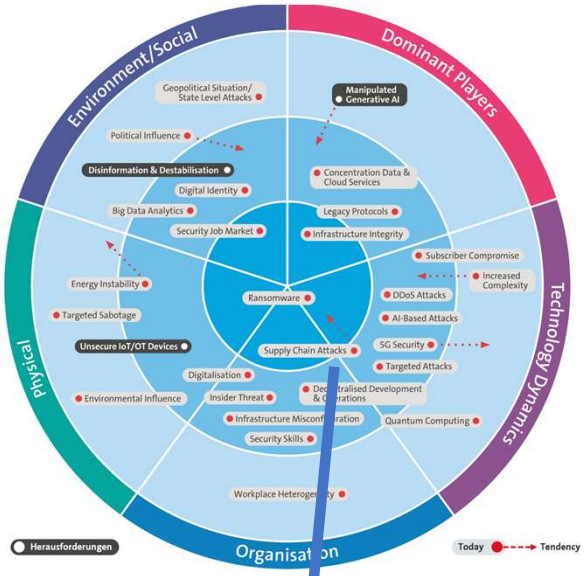
Cette visibilité facilitera la prise de décision rapide et éclairée, tout en permettant d'anticiper les problèmes potentiels. Les entreprises qui investissent dans des solutions de visibilité pourront répondre plus efficacement aux besoins des clients et réduire les coûts opérationnels.

https://supply-chain.net/perspectives-de-la-chaine-dapprovisionnement-en-2025-tendances-majeures-et-risques-a-surveiller/

XPLAIN !

CLUSIS

Swisscom Cyber Security Threat Radar 2024



Thème très sensible bis !

Login rétabli

Cyberattaque: la panne de Onelog est enfin résolue (update)

Lun 04.11.2024 - 10:45
par Yannick Chavanne et René Jaun et (traduction/adaptation ICTjournal)

La plateforme Onelog a été victime d'une cyberattaque. En panne depuis le 24 octobre 2024, le système de Single Sign-On porté conjointement par plusieurs entreprises de médias suisses fonctionne à nouveau.

Panne informatique mondiale de juillet 2024

33 langues

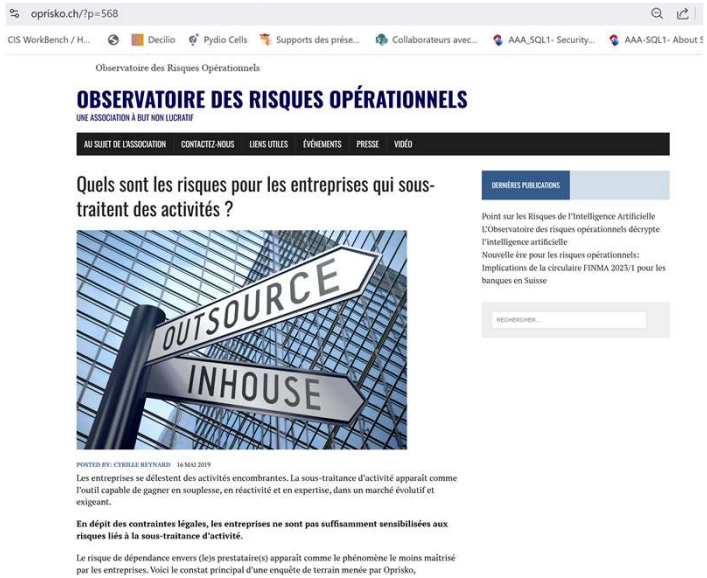
Article Discussion | Lire Modifier Modifier le code Voir l'historique Outils

La **panne informatique mondiale du 19 juillet 2024** est causée par la mise à jour de *Falcon Sensor*, un logiciel développé par la société de cybersécurité américaine CrowdStrike. Cette mise à jour défectueuse provoque partout à travers le monde le plantage d'environ 8,5 millions d'ordinateurs et serveurs utilisant le système d'exploitation Microsoft Windows, causant d'importantes perturbations, essentiellement au sein des entreprises. Le *cloud* de Microsoft est aussi partiellement tombé en panne ce jour-là, mais un peu avant et donc sans rapport avec la mise à jour défectueuse.

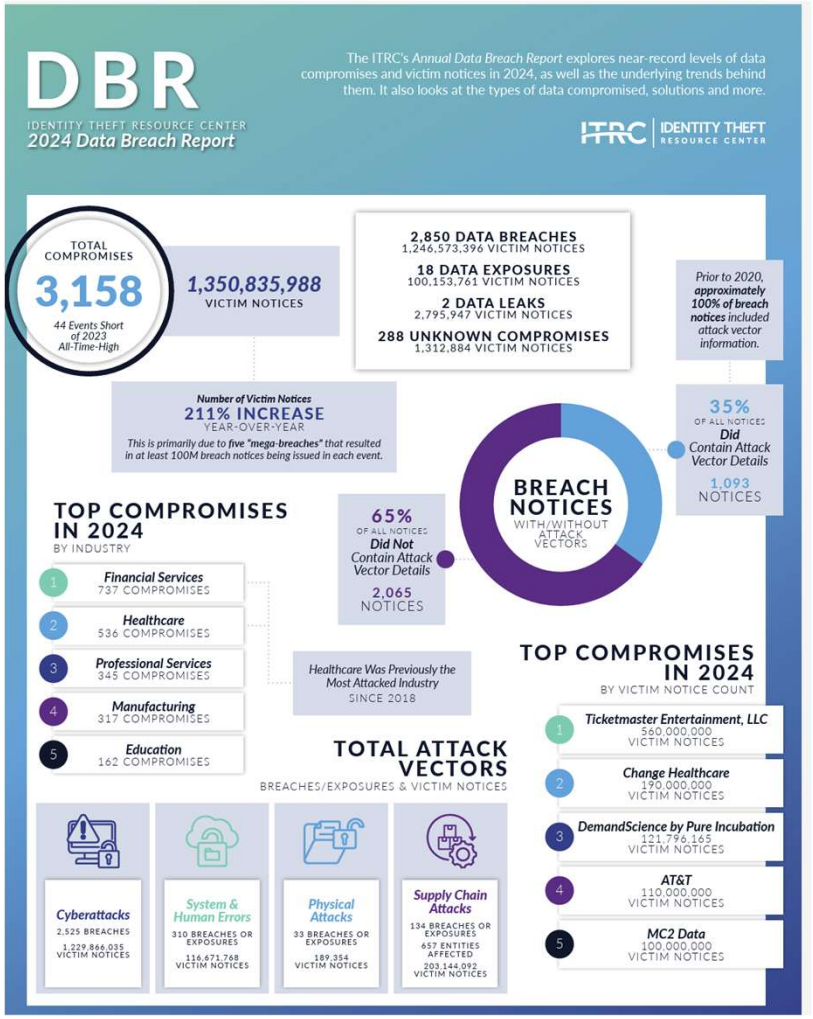
Divers secteurs économiques sont affectés tels que les aéroports, les banques, les hôtels, les hôpitaux, la grande distribution, les marchés financiers, la restauration, des services de diffusion gouvernementaux comme les numéros d'appels d'urgence et des sites internet. L'erreur est découverte et corrigée le jour même par Microsoft et CrowdStrike, mais la panne logicielle a eu des répercussions toute la journée, affectant l'organisation des vols des lignes régulières, les paiements électroniques, les services d'urgences, etc.

Panne informatique mondiale de juillet 2024

L'écran bleu de la mort apparaît sur les appareils touchés par la panne mondiale, ici à l'Aéroport LaGuardia de New York.



Thème très sensible !



Augmentation des attaques via des fournisseurs tiers : Durant le troisième trimestre de 2024, l'Identity Theft Resource Center (ITRC) a observé une augmentation de 203 % des cyberattaques visant les fournisseurs tiers par rapport au trimestre précédent. 91 organisations ont été impactées, les services financiers et la santé demeurant les secteurs les plus touchés, avec respectivement 141 et 123 violations durant cette période, sur les 672 au total. dcmag.fr

Adobe Acrobat-Dokumen

CLUSIS

5 à 7

Gestion des prestataires externes

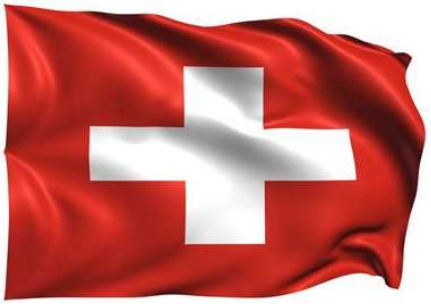
Les fournisseurs cible de choix des attaquants

Attaques de la supply chain

- large portée
- difficulté à être détectées
- potentiel important qu'elles ont de provoquer des effets catastrophiques en cascade.
- Favorisées par la dépendance croissante à l'égard des services informatiques externalisés, de la chaîne d'approvisionnement et des défis en matière de cybersécurité, en particulier pour les PME

Les attaques de la chaîne d'approvisionnement sont recensées depuis au moins 2016[1] et tiennent la première place du rapport de l'ENISA[2]

Source:
[1] https://cyber.gouv.fr/tendances-les-cybermenaces
[2] https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union



La Suisse au cœur de l'Europe

- Les attaquants ne tiennent pas compte des frontières traditionnelles
- Relations commerciales avec l'Europe : partenaires et clients
- La position de la Suisse reste une force commerciale

Les entreprises suisses

- doivent suivre la dynamique européenne pour rester dans la course
- ne sont pas épargnées par ce type d'attaques

La stratégie de l'UE en matière de cybersécurité vise à renforcer la résilience face aux cybermenaces et à faire en sorte que les citoyens et les entreprises bénéficient de technologies numériques fiables

Renforcement de la réglementation européenne en réponse à cette hausse des attaques

Source : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Directive NIS2 (Network and Information Security)

- **Objectif** : Renforcer la cybersécurité globale au sein de l'UE
- **Cibles** : Entités essentielles et importantes de 18 secteurs (énergie, transports, santé, infrastructures numériques)
- **Pourquoi ?** : Améliorer la coopération entre États membres, renforcer les capacités de gestion des incidents, garantir un niveau élevé de sécurité des réseaux et systèmes d'information

Règlement DORA (Digital Operational Resilience Act)

- **Objectif** : Assurer l'intégrité et la disponibilité du secteur financier.
- **Cibles** : 21 types d'entités financières (banques, assurances, infrastructures de marché).
- **Pourquoi ?** : Garantir la résilience face aux cyberattaques et perturbations opérationnelles, gestion des risques, notification des incidents, tests de résilience.

Cyber Resilience Act (CRA)

- **Objectif** : Renforcer la sécurité des produits numériques tout au long de leur cycle de vie
- **Cibles** : Tous les produits numériques
- **Pourquoi ?** : Protéger les consommateurs et entreprises contre les cybermenaces, garantir la sécurité dès la conception et tout au long de l'utilisation des produits numériques

5 piliers fondateurs

Supply chain risk management

Assurer la continuité de la supply chain, en particulier en cas de cyber attaques

Identifier et traiter toute menace à la continuité de l'activité susceptible de se propager dans la chaîne d'approvisionnement

Fournisseurs IT, mais aussi les autres fournisseurs sont concernées

ISO 2700x.

NIST

Risk approaches (FAIR TAM)

ISO 27001

- **Objectif :**
  - Gérer les risques liés à la sécurité de l'information dans les relations avec les fournisseurs.
- **Principales Actions :**
  1. **Mise en œuvre de Politiques :** Établir des politiques de sécurité de l'information spécifiques aux fournisseurs.
  2. **Contrôle des Fournisseurs :** Surveiller et évaluer les fournisseurs pour garantir la conformité aux exigences de sécurité.
  3. **Conformité :** Assurer que les fournisseurs respectent les normes de sécurité de l'information.
- **Domaines de Concentration :**
  - **Risques Inhérents :** Prendre en compte les risques liés à l'utilisation de systèmes externes.
  - **Impact sur la Sécurité :** Évaluer l'impact potentiel sur la sécurité de l'information de l'organisation.
- **Responsabilité :**
  - La gestion de la sécurité des informations dans les relations avec les fournisseurs doit être supervisée par la direction générale.

NIST

- **Objectif :**
  - Identifier, évaluer et gérer les risques liés à la chaîne d'approvisionnement.

- **Principales Actions :**
  1. **Identification :** Les fournisseurs doivent identifier leurs systèmes et composants critiques dans un cadre de gestion des risques1
  2. **Protection :** Définir et mettre en œuvre des contrôles pour gérer l'accès et la visibilité des systèmes critiques
  3. **Détection :** Maintenir une visibilité sur les menaces nouvelles et émergentes2
  4. **Réponse :** Prendre des mesures pour contenir et minimiser l'impact des incidents de cybersécurité2
  5. **Récupération :** Restaurer les capacités ou les services touchés par un événement de cybersécurité2

- **Domaines de Concentration :**
  - **Contrôles de Sécurité :** Plus de 1 000 contrôles organisés en familles pour évaluer les risques de sécurité des fournisseurs
  - **Conformité :** Les organisations doivent établir et mettre en œuvre des processus pour garantir la conformité aux exigences de sécurité

Comment s’y prendre ?

1. Identifier vos activités ou services les plus critiques
2. Pour chacune de ces activités ou services critiques, identifier :
   - Les fournisseurs impliqués
   - Vos besoins en sécurité
   - Hiérarchiser vos fournisseurs en conséquence
3. Dialoguer avec chacun de vos fournisseurs pour établir une relation de confiance basée sur :
   - Contrats en règle, comprenant des exigences de sécurité
   - Gouvernance efficace pour respecter les exigences légales et réglementaires
   - Audits, et vérifications pour démontrer le maintien en niveau de sécurité

Les enjeux *de la gestion des sous-traitants et des tiers*

Sécurité et protection des données par défaut et par design

Intervenant / contact

Intervenant :
Frédéric Gaudun - CIGES Neuchâtel
Responsable sécurité des systèmes d'information des institutions de santé publiques neuchâteloises

Mobile : +41 79 942 4614

E-Mail : Frederic.Gaudun@Ciges-ne.ch

Au menu aujourd'hui :

- Un peu de contexte
- Principes sur la sécurité des tiers
- TOMS - sous-traitants et tiers
- Quelques conseils pratiques
- Un exemple concret

Laissez ses clés de maison à un voisin

Différents contextes

Accès aux données internes par des externes

Externalisation des données

Accès VPN

Gouvernance, Risque et Compliance (GRC)

Pour les dirigeants

Identification des risques systémiques

IMAGE de votre société

Conformité / réglementation

Responsabilité éthique

Entrons dans le vif du sujet

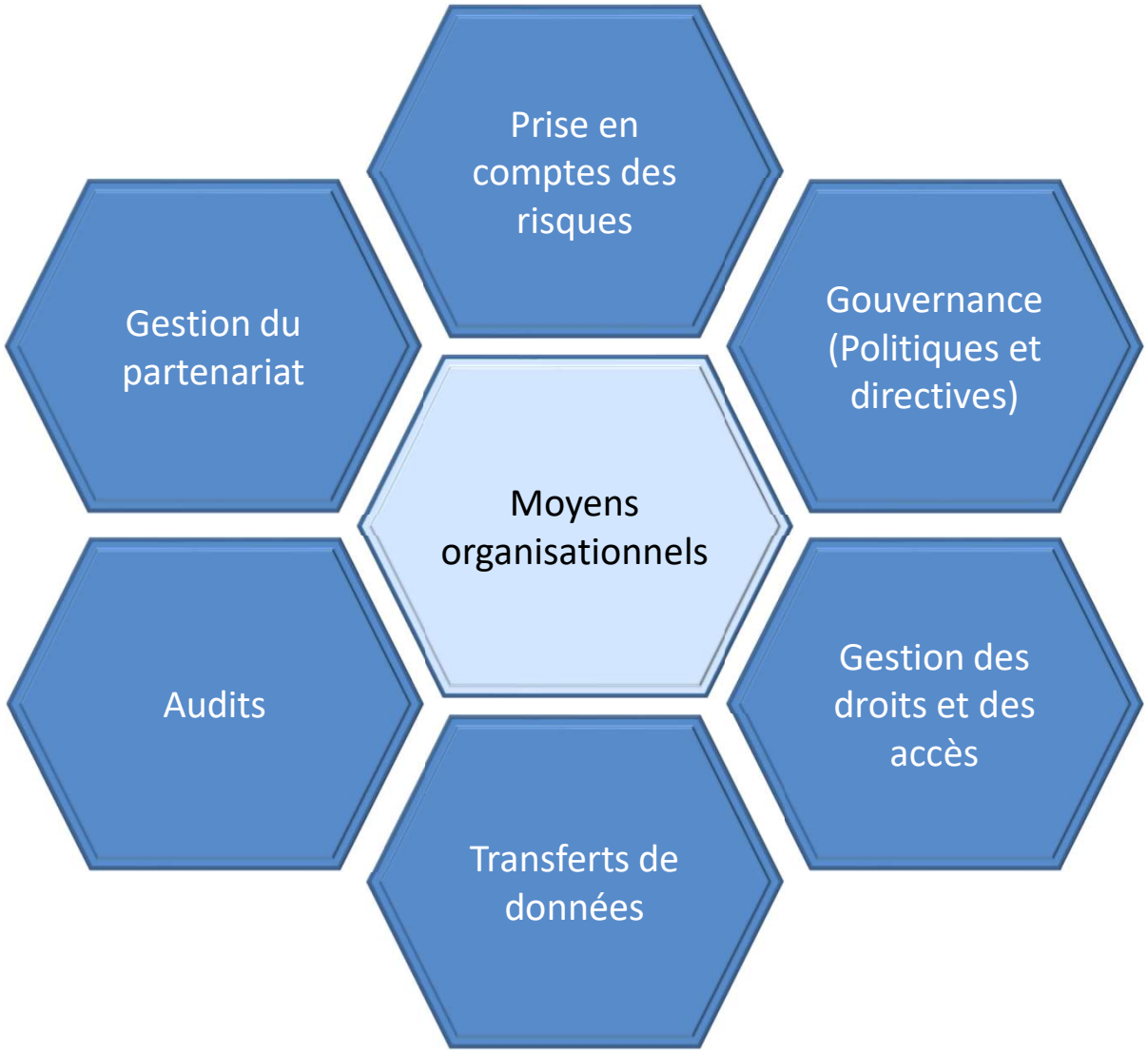
TOMS adaptés à la gestion de risque

Gestion de risque et évaluation du contexte

Moyens techniques

Moyens organisationnels

Focus sur les moyens organisationnels (Non exhaustif)



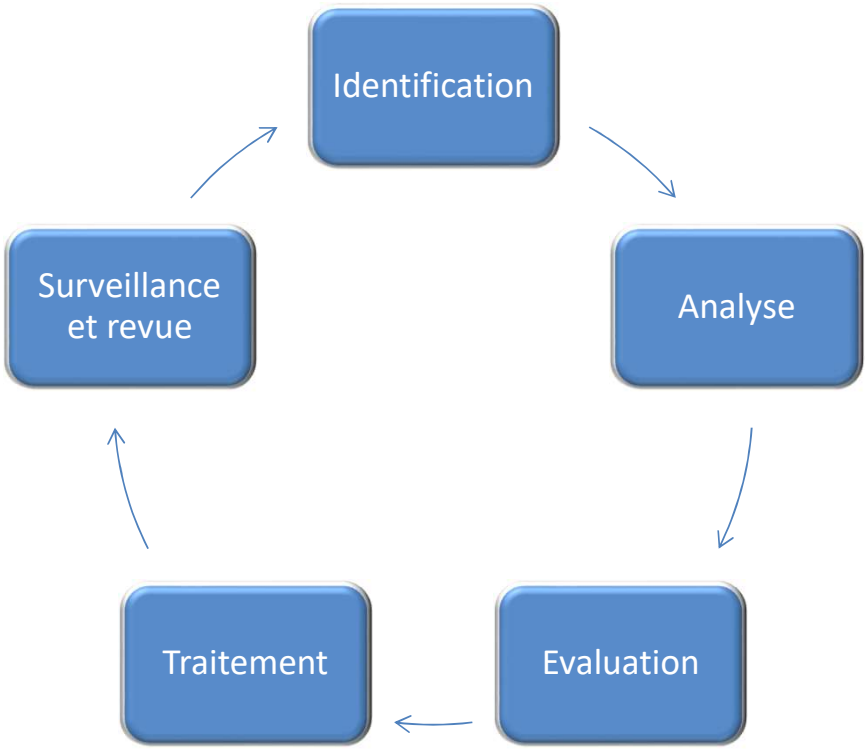
Gestion de risque

Etablissement du contexte :

Définition de l'appétence au risques (appréciation et acceptation)

Exigences de base (Normes, législation)

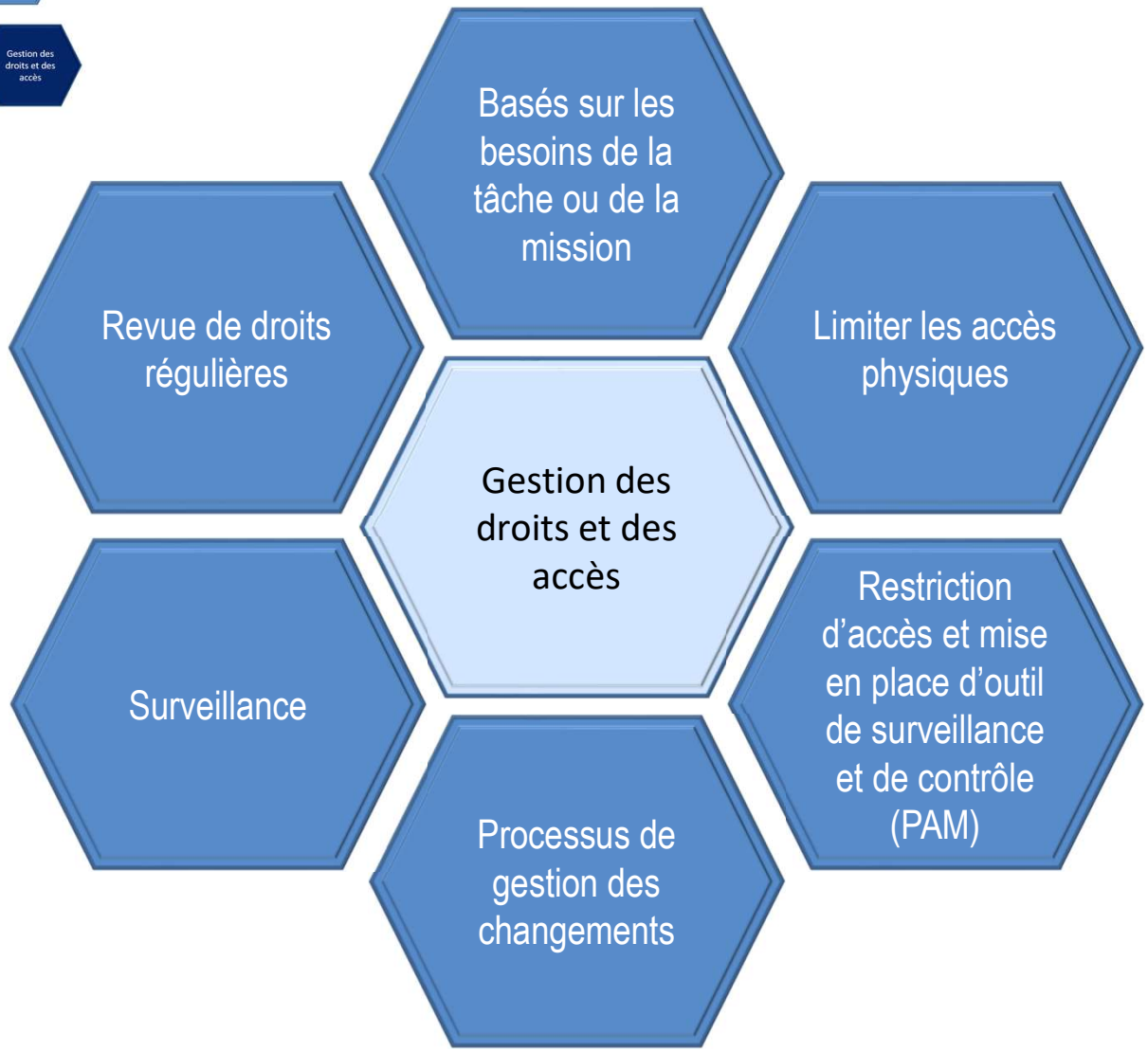
Identifier les exigences SIPD



Démarche itérative : A conduire régulièrement

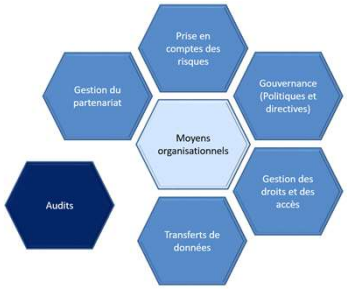
Gouvernances et directives

Gestion de droit et des accès



Transfert des données

Audits


Prise en comptes des risques
Gestion du partenariat
Gouvernance (Politiques et directives)
Moyens organisationnels
Gestion des droits et des accès
Audits
Transferts de données


S'assurer du contexte légal
Définir un cycle de revue
Existe t'il des documents à disposition
Audits
Pentest
Respect du safety and privacy by design
Revue de code / revue de process

Gestion du partenariat et cycle de vie

Amélioration continue

Planification → Due Diligence → Revue du contrat → Négociation → Cycle de la vie de la relation → Désengagement

Construction du partenariat

Quelques «take away»

Le fournisseur ne doit pas être le maillon faible de votre SI

Les réglementations sont exigeantes sur le risque «Supply Chain»

Pas de recette magique

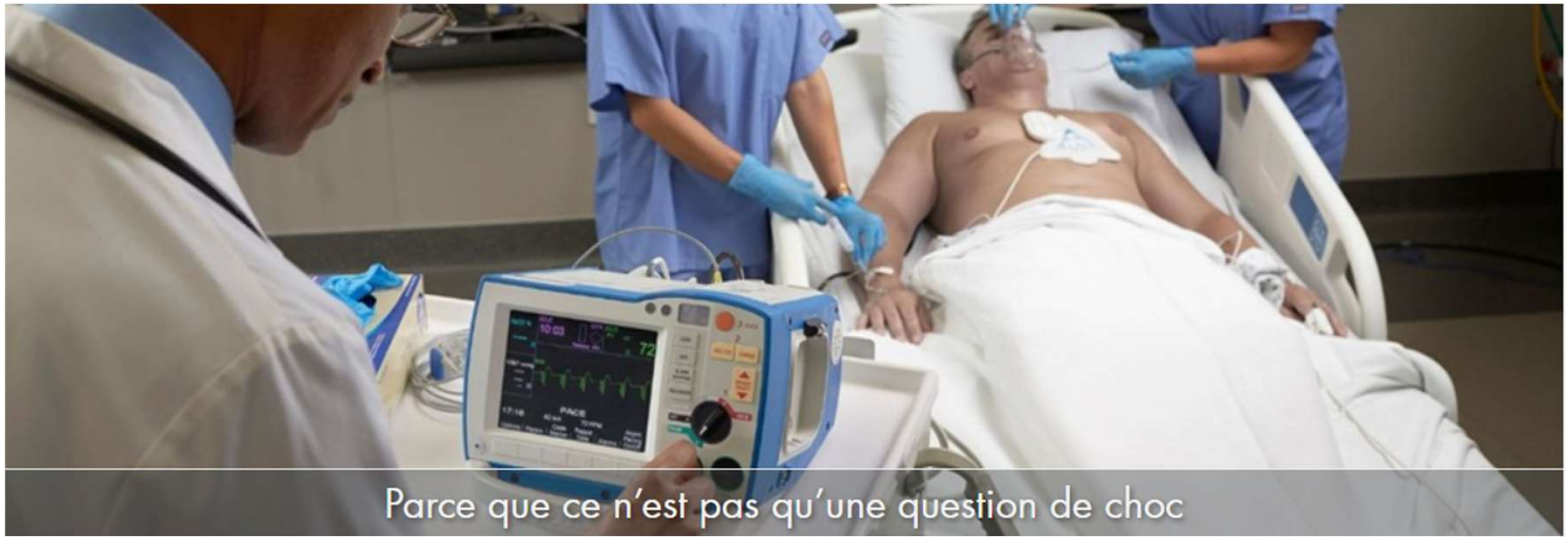
Approche holistique physique et logique

Les coûts doivent être proportionnels aux risques

Le soutien du management est essentiel

Un exemple concret

Un exemple concret : Défibrillateurs



Défibrillateurs : Les enjeux

Données de santé : Confidentielles et sensibles

Sécurité des canaux de communication

Stockage dans un cloud à l'étranger

Etat du patient – Inconscient ?

Défibrillateurs : Les solutions

Anonymisation et effacement des données après quelques jours

Chiffrement des transmissions. Certification ISO et résultats d'audits

Chiffrement des données et anonymisation (PID). Suppression des données. Contrats

PID – «Bris de glace» - DEP


WWW.MESIMAGES.CH
© MICHEL JEANDUPEUX

5. Questions & Réponses

CLUSIS

5. Questions pour nos intervenants

- Est-ce que le Clusis peut nous aider a ce sujet ?
- Existe ils des solutions qui permettent d'automatiser cela ?
- Lesquels nous recommanderiez vous ? si je suis une PME avec 6 prestataires par exemples ou alors une PME de 80 employés avec plus d'une 20 de prestataires est ce que je peux gérer cela de la même manière ?
- Dans tous vos slides je ne vois rien relatifs avec la protection des données, je dois quand même faire attention a cet aspects suivant ce que mon prestataire traite comme données , a quoi dois je faire attention ?
- Comment démarrer dans une entreprise qui a déjà des fournisseurs ?
- Peut-on faire simple ?
- Comment faire avec des « gros » fournisseurs (ex. Google, Microsoft…) ?

6. Take Aways

Quelques «take away

Comment s'y prendre ?

1. Identifier vos activités ou services les plus critiques
2. Pour chacune de ces activités ou services critiques, identifier :
   1. Les fournisseurs impliqués
   2. Vos besoins en sécurité
   3. Hiérarchiser vos fournisseurs en conséquence
3. Dialoguer avec chacun de vos fournisseurs pour établir une relation de confiance basée sur :
   1. Contrats en règle, comprenant des exigences de sécurité
   2. Gouvernance efficace pour respecter les exigences légales et réglementaires
   3. Audits, et vérifications pour démontrer le maintien en niveau de sécurité

Le fournisseur ne doit pas être le maillon faible de votre SI

Les réglementations sont exigeantes sur le risque «Supply Chain»

Pas de recette magique

Approche holistique physique et logique

Les coûts doivent être proportionnels aux risques

Le soutien du management est essentiel

Un dernier mot de nos intervenants ?

6. Take Aways

1. Il existe des solutions techniques pertinentes et locales pour vous aider;

2. Faites-vous accompagner si besoin, beaucoup d'experts sécurités sont disponibles pour vous aider, regarder notamment les sponsors ….

3. Beaucoup de littérature existe sur le sujet comme vous l'ont référencé Anne et Frédéric

4. L'état de Vaud donne des conseils : https://www.vd.ch/dcirh/dgnsi/cybersecurite/bonnes-pratiques/bonnes-pratiques-de-cybersecurite-envers-un-fournisseur-de-prestation-informatique

5. Exigences concernant la sécurité informatique de système tiers https://www.hplus.ch/fr/politik/cyber-security

6. Le Canada : https://www.cyber.gc.ca/fr/orientation/cybersecurite-chaine-approvisionnement-pour-petites-moyennes-organisations-itsap00070

7. Conclusion

1. Thème d'actualité hypersensible et critique c'est devenue la priorité des entreprises; exemples : plusieurs entreprises dans le luxe se mettent à prendre en charge la sécurité de leurs sous –traitants.
2. Les futurs indicateurs tels que le Threat Radar de Swisscom qui sortira fin mai 2025 positionnera sûrement ce risque encore plus critique qu'actuellement
3. Il y a des outils et des professionnels pour vous aider !

CLUSIS

Un grand merci pour votre participation active à ce 5à7 et bonne soirée !

www.clusis.ch