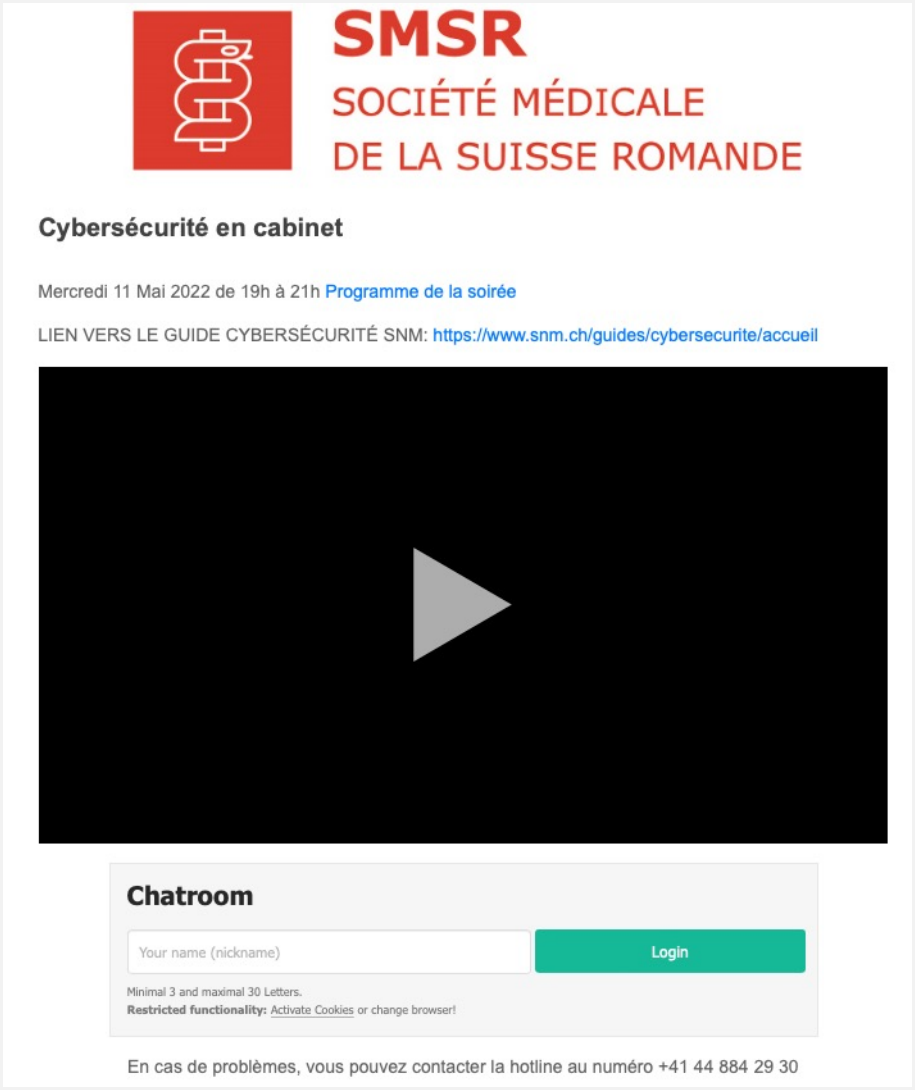
SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Cybersécurité en cabinet

Soirée SMSR 11 mai 2022

Dr Dominique Bünzli, président de la Société Neuchâteloise de Médecine



GUIDE SNM: www.snm.ch/guides

--> Guide cybersécurité en cabinet

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

OBJECTIFS ET PROGRAMME

- **1er partie**
  - Prendre conscience de la problématique: contexte, témoignage
  - Rappeler le cadre légal / communication
  - Point de vue des patients
  - Mesures immédiates/Police
- **2ème partie**
  - Principes de base de la sécurité et de l'hygiène numérique
  - Présenter des produits de cybersécurité: diagnostic/prévention
- **3ème partie**
  - Ouvrir la réflexion sur le futur (coûts, mutualisation, rôle de l'Etat ?)
  - Conclusions/Questions/Evaluation/Attestation
  - Remerciements

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

CONTEXTE

carte 1

Exemple: M. Eric Favre de l'Office Cantonal Genevois du Numérique sur les ondes RTS dans Forum le 1er avril 22:

«Les infrastructures informatiques genevoises sont sous un feu permanent. Nous détectons à peu près ***17 milliards d'événements de sécurité par année****, soit* ***5500 tentatives d'attaques ou d'événements de sécurité par seconde****»...*

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

TEMOIGNAGE

- Dre Marjorie Cosandey-Tissot, médecine interne générale

UNE CYBERATTAQUE AU CABINET

Marjorie Cosandey Tissot

11.05.2022

AVANT LA CYBERATTAQUE

- 10.2021 **Mise en application des recommandations de la FMH** pour la cybersécurité. Formation et points techniques validés par notre IT. A préciser, que nous n'avions pas les moyens de vérifier si notre IT avait bien fait ce qu'il avait dit et écrit.

- **Signature d'une charte** le 14.12.2021.

- **Avoir le sentiment de ne pas avoir été négligentes.**

LA CYBERATTAQUE

- 14.03.2022 : lundi 08h00 aucun ordinateur ne fonctionne.
- Une matinée sans agenda, sans accès aux données de notre logiciel patient (LP). Dès l'après-midi, on peut consulter notre LP.
- Mercredi 16.03.22 à midi, soit 2 jours après l'attaque nous avons pu utiliser à nouveau notre LP, mais restent encore beaucoup d'incompréhensions et de doutes.
- Jeudi 17.03.22, on apprend **le vol de données** et la menace de les **libérer sur le darknet contre rançon.**

LOCKBIT 2.0

LEAKED DATA

CONDITIONS FOR PARTNERS AND CONTACTS ›

UNTIL FILES
10D 18:48:13
PUBLICATION

29 Mar, 2022 16:57:00

onedoc.ch/fr
/cabinet-de-
[redacted]

we have some clients data of few doctors in this company

ALL AVAILABLE DATA WILL BE PUBLISHED !

LA MULTITUDE DE QUESTIONS ?

- Comment **comprendre** ce qui s'est passé, est-ce que les mesures demandées ont bien été prises par l'IT ? Notre infrastructure est-elle maintenant propre ?
- Prévenir les risques de **récidives** ?
- Comment savoir quelles données, quels patients **concernés** et **quand** les données vont-elles se retrouver sur le darkweb ?
- Payer ou non la **rançon** ?
- **Avertir les patients,** mais lesquels, à quel moment, comment ?

PLAN D'ACTION

- **Comprendre**, s'entourer d'**experts**, anticiper, **informer** les patients. Importance de bien s'entourer et savoir à qui l'on peut **faire confiance**.

- Vendredi 01.04.2022, accès aux données publiées, mesure de l'ampleur de la cyberattaque.

- Communiqué de presse, 2ème ligne téléphonique, page sur le site SNM et **stratégie de communication face aux médias**.

CE QUI NOUS A AIDÉES

- **Police** : démarches et informations utiles, **rançon**.
- **Ingénieurs en cybersécurité** : communication avec les hackeurs, rançon, penser le futur de notre sécurité informatique.
- **Préposé fédéral à la protection des données** : communication transparente aux patients.
- **Avocat spécialiste en cybercriminalité** : très aidant et compétent pour toutes nos démarches.
- **Médecin cantonal** : communication en temps de crise.
- Soutien actif du président de la **SNM**.

CE QUI NOUS A MANQUÉ

Manque d'informations et de communication de la part des informaticiens en général en matière de sécurité informatique.

Ne prennent pas le temps de partager au sujet :

- **Architecture** de nos parcs informatiques et les alternatives
- **Visibilité** des attaques
- **Surface** d'attaque
- **Archivage**

Quid de la relation médecin-informaticien ?

- Solutions **trop axées sur l'achat** d'une nouvelle technologie sans passer par l'analyse => Comme si on discutait d'emblée des options thérapeutiques sans passer par l'AA, l'examen clinique et le DD.
- Comme nos patients, **droit à l'information** ? Un partenariat médecin – informaticien type prise de **décisions partagées** ?
- Service **proactif** du fournisseur, par ex, ne pas attendre pour signaler qu'un appareil représente un danger.
- Le médecin est **soumis à une autorité de surveillance** et a une formation complète…l'informaticien pas toujours…

NOS PISTES DE RÉFLEXION

- Repenser l'architecture de nos parcs informatiques afin de **limiter la surface d'attaque**.
- **Coupler** les réflexions avec **une sobriété numérique** compatible avec une vision **durable** de la santé.
- L'augmentation du **niveau de sécurité** devra passer par une **mutualisation** des prestations pour que les coûts deviennent accessibles à nos PMEs.

QUESTIONS À NOS ASSOCIATIONS

- Face au **vaste** marché de la cybersécurité et l'**augmentation** future des cyberattaques, peut-on attendre de nos associations qu'elles fassent un travail de fond **d'analyse comparée des alternatives** et éditent des **règlementations de bonnes pratiques aux IT** pour nos données sensibles ?
- Allongement de la durée de conservation des données= augmentation du risque et des coûts pour les médecins. Quelles solutions ?
- Les bases de la cybersécurité devraient-elle être enseignées en pré-, et post-graduées et formation continue ?

MERCI DE VOTRE ATTENTION

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

CADRE LEGAL

- M. Joël de Montmollin, juriste PFPDT

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence PFPDT

Cybersécurité en cabinet

Aspects de protection des données

Joël de Montmollin

Juriste auprès du Préposé fédéral à la protection des données et à la transparence PFPDT

Neuchâtel, 11 mai 2022

Médecins et protection des données

- Par rapport au dossier du patient, **médecin = maître du fichier** (art. 3 let. i LPD)

- Obligations quant à la sécurité des données contre les traitements (art. 3 let. e LPD) non autorisés (art. 7 LPD)
  - Qui a accès?
  - Qui peut faire quoi?

➔ mesures de sécurité IT, physiques et organisationnelles

➔ concerne tant le vol/fuite/etc. de données que leur intégrité

Devoir d’information - fondements

- Informer les patients sur l’incident, les données concernées et les mesures prises pour y remédier

- Fondé sur le principe de la bonne foi (art. 4 al. 2 LPD)

  ➔ je traite des données patient -> j’ai été piraté -> je sais que ça peut exposer mon patient à des risques -> la bonne foi m’impose de le prévenir

- Disposition spécifique dans nLPD: art. 24 al. 4 et 5

Devoir d’information – questions pratiques 1/2

- Enjeux pour le patient: se **protéger** des conséquences du piratage
- Enjeux pour le médecin: maintenir la **confiance**, réduire les risques de **dommage** que peuvent subir ses patients (et potentiellement engager la responsabilité du médecin)

- Tous les patients devraient être directement informés
  - plusieurs milliers de patients
  - coordonnées pas nécessairement à jour, pas d’adresse email, etc.
    - ➔ difficultés pratiques à toucher directement toute la patientèle

Devoir d'information – questions pratiques 2/2

- Pas de «seuil de suffisance» quant aux moyens
  - ➔ plus les données sont sensibles, plus il faudra être diligent
  - ➔ action en responsabilité ≠ PFPDT mais **juge civil**
  - ➔ art. 63 nLPD: dans certains cas, possibles sanctions pénales pour non-respect intentionnel d'une obligation d'informer

NB: ce n'est pas parce que le patient n'ouvre pas action contre le médecin qu'il ne subit pas de dommages/désagréments

Exemples de risques: usage abusif des adresses emails (fausses factures, virus, etc.), chantage, perte du dossier patient

Cybersécurité en cabinet

Take home message: soyez à jour !

Merci de votre attention

Site internet PFPDT: www.edoeb.admin.ch

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

COMMUNICATION AUX MEDIAS

- Dr Claude-François Robert, médecin cantonal NE

Cybersécurité en cabinet

communication aux médias

lors d'un piratage informatique de cabinet médical

Dr CF. Robert

11 mai 2022

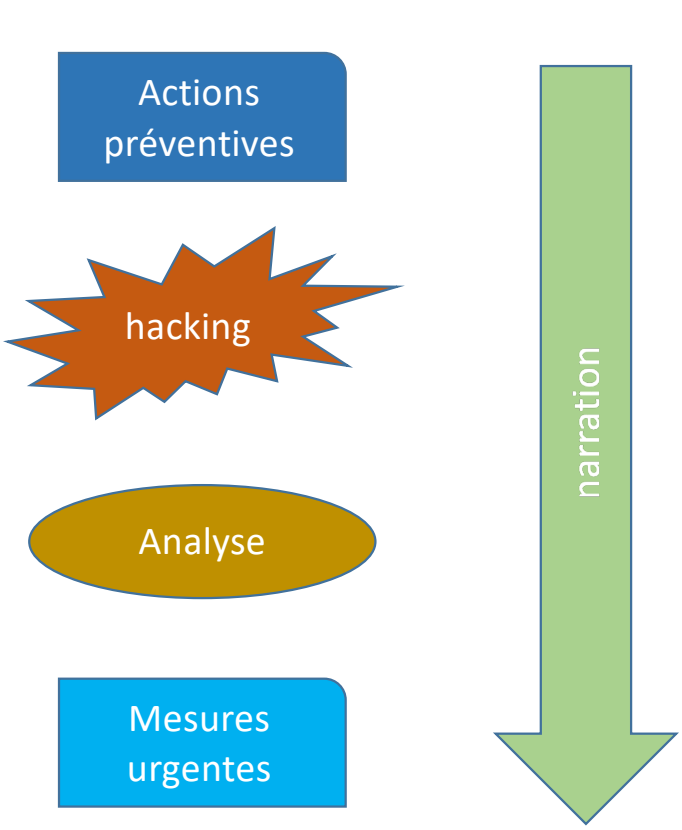
Piratage d'un cabinet : impact et réponse par une communication active

- atteinte des infrastructures, crise de communication → Impact sur le fonctionnement du système de santé
- **Objectifs de la réponse** : *préserver la confiance des patients envers les soignants*
- Rupture potentielle du respect du droit des patients, notamment du secret professionnel
- Atteinte systémique → information de l'autorité de surveillance

Check-list pour une communication active

1. Désigner un porte-parole
2. Se faire conseiller par une personne externe
3. Définir les objectifs de la communication
4. Construire la narration
5. Elaborer 3 messages clés
6. Etayer les messages par des faits (tableau 3X3)
7. Définir les moyens et le calendrier de la communication, par exemple un point presse dans 6 heures, un communiqué, répondre ou non à des interviews, anticiper les réactions à chaque communication, préserver l'égalité d'accès des médias

Eléments de la narration : épisodes, scène, acteurs



La scène du crime

Acteurs	Rôles possibles
Hackers	Obtenir une rançon, nuire Se protéger
Médecin	Protéger des données sensibles Former son personnel Garder la confiance de ses patients Maintenir son activité
Prestataire informatique	Assurer la sécurité informatique
Patients	Garder la relation de confiance avec le médecin Quitter son médecin, attaquer en justice

Elaborer les messages clés (Tableau 3X3)

Piratage du cabinet X : Communiqué du …

Faits

Message clé 1	Message clé 2	Message clé 3
Nous tenons à être transparents et confirmons que notre cabinet a subi un piratage informatique	**Cette attaque est regrettable et nous avons agi rapidement pour prendre toutes les mesures nécessaires**	**En pratique, tous nos patients concernés ont été informés et ont reçu des conseils**
Faits 1.1	**Faits 2.1**	**Faits 3.1**
Selon notre fournisseur informatique, cela s'est produit le... Les pirates se sont emparés des données sensibles. Elles pourraient être publiées sur le darknet…	Nous avons informé la police et déposé une plainte pénale	Nos anciens patients qui n'auraient pas été contactés peuvent nous téléphoner ou envoyer un e-mail à une adresse sécurisée
Faits 1.2	**Faits 2.2**	**Faits 3.2**
La cause est une probable intrusion sur un poste dédié au télétravail	Suivant les conseils de notre société informatique, nous avons pris les mesures suivantes … pour préserver les données et renforcer la sécurité.	Le cabinet est fermé et pour les rendez-vous prévus ces prochains jours, nous annonçons …
Faits 1.3	**Faits 2.3**	**Faits 3.3**
Suite à une première analyse, les données piratées concernent … des données personnelles/sensibles de nos patients…	Une société informatique nous conseille depuis … et dès ce moment, nous avions pris toutes les mesures qui nous semblaient possibles pour prévenir une telle attaque criminelle	Nous ferons une nouvelle communication pour nos patients d'ici 48 heures…

Conclusions

- Une communication active est requise pour maintenir la confiance
- Se préparer à communiquer est la meilleure prévention

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

FEDERATION SUISSE DES PATIENTS

- M. Baptiste Hurni, président section romande

Soirée cybersécurité en cabinet

Quelques considérations du point de vue des patients

Avant un évènement

- Prendre au sérieux la problématique et proposer la solution la plus efficiente
- Eviter d'avoir des partages complets de données entre médecins
- Informer les patients du système mis en place
- Discuter avec le patient des éléments pertinent, y compris des recommandations de la FMH
- Ne pas prendre le sujet à la légère
- Rediriger vers d'autres interlocuteurs (FSP, FRC,…)

Après un évènement

- Prévenir immédiatement et personnellement (dans la mesure du possible) les patients concernés
- Dénoncer les cas aux autorités pénales
- Inviter les patients à dénoncer les cas
- Proposer un suivi personnalisé, y compris avec d'autres intervenants (FSP, FRC,…)
- Prendre le temps d'expliquer et d'éventuellement rassurer

A l’avenir, améliorer les choses

- Travailler à un projet qui met en commun les ressources pour proposer une solution répondant aux meilleurs standards
- Associer les organisations de patients à la démarche
- S’assurer que tout le système est à jour et répond toujours aux meilleurs standards possibles

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

POLICE NEUCHÂTELOISE

- M. Thierry Chuat, commissaire et chef du commissariat CRECO NE

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

SOCIÉTÉ NEUCHÂTELOISE DE MÉDECINE

-

SOIRÉE CYBERSÉCURITÉ

11.05.2022

DÉPARTEMENT DE L'ÉCONOMIE, DE LA SÉCURITÉ ET DE LA CULTURE (DESC)

police NEUCHÂTELOISE

Plan

- Quelles sont les mesures immédiates à prendre en cas de cyberattaque ?
- Pourquoi annoncer une cyberattaque à la police et que peut-elle faire ?
- Quelques chiffres
- Qui sont ces hackers et a-t-on la possibilité de les identifier ?
- Conclusion

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Mesures immédiates…

En cas de chiffrement par un ransomware, le centre national pour la cybersécurité recommande **les actions immédiates suivantes** :

- Coupez toutes les connexions Internet (web, email ainsi que l'accès à distance et les VPN site-à-site).
- Vérifiez les sauvegardes et protégez-les immédiatement. Les sauvegardes doivent être déconnectées physiquement du réseau infecté aussi rapidement que possible (“mise hors ligne”).
- Contactez la police cantonale (demander à parler aux agents en charge de la cybersécurité).
- Faites appel à un prestataire externe de services de sécurité informatique, qui peut vous aider à gérer l'incident et à effectuer les analyses appropriées.
- Informez dès que possible NCSC / GovCERT.ch si vous êtes une infrastructure critique.
- Il est vivement recommandé de ne pas contacter les auteurs soi-même.

sans tarder

Merci d'informer votre société cantonale !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Pourquoi annoncer le cas à la police ???

Conseils & appui

Détection de phénomènes émergents

Mise en marche de mesures préventives

Transmission d'informations à nos collègues de fedpol/Europol/Interpol

Récolte de données identifiantes

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Quelques chiffres…

LE TEMPS

Face aux cybercrimes, le procureur fédéral appelle à l'aide

TECHNOLOGIE Mercredi, le procureur général de la Confédération, Stefan Blättler, a demandé davantage de moyens contre le crime en ligne. Il n'existe par exemple pas de base de données centrale, a-t-il regretté

ANOUCH SEYDTAGHIA
@Anouch

Que font les autorités contre les cybercriminels? Rien, entend-on souvent. Mercredi, dans le cadre des Swiss Cyber Security Days qui se tiennent à Fribourg et dont *Le Temps* est partenaire, Stefan Blättler a tenté de tordre le cou à ce cliché… tout en exigeant davantage de moyens et d'engagements de tous contre les cyberattaques.

Selon Stefan Blättler, la justice a obtenu des succès contre les cybercriminels – mais ne les a pas détaillés. «On a aussi de gros soucis, a-t-il affirmé. Nous n'avons pas, en Suisse, de législation spécifique sur la cybercriminalité pour des enquêtes, dont l'obtention des preuves numériques est un défi majeur. De plus, le processus d'entraide internationale est lent et pas du tout adapté aux cyberdélits. L'entraide est complexe et de longue haleine, cela prend parfois des mois, voire des années, avant d'aboutir à des résultats.»

«L'entraide internationale est un véritable parcours du combattant»

STEFAN BLÄTTLER, PROCUREUR GÉNÉRAL DE LA CONFÉDÉRATION

Comme le relève Stefan Blättler, «les victimes, que ce soient des particuliers ou des entreprises, sont en Suisse. Or les présumés coupables sont à l'étranger. L'entraide internationale est un véritable parcours du combattant.» Heureusement, estime le procureur de la Confédération, «dans certains cas, il peut y avoir des contacts entre procureurs de différents pays, notamment pour la saisie de données informatiques.»

Stefan Blättler regrette un manque très peu connu en Suisse: l'absence d'une base de données fédérale sur les cybercrimes. «Elle n'existe pas… Or il en faut absolument une, car nous sentons que ces délits ne cessent d'augmenter. Il y a urgence, car cela permettra aux autorités de poursuite d'agir beaucoup plus rapidement si ces infractions sont référencées au niveau suisse.»

«Manifestez-vous!»

Le procureur de la Confédération demande, en parallèle, un autre point qu'il estime capital: «Je lance un appel aux individus et aux entreprises: si vous êtes victime d'une cyberattaque, n'hésitez pas à fournir ces informations aussi vite que possible aux autorités de poursuite pénale, une action rapide peut vraiment nous aider. Souvent, on perd du temps, entre le dépôt d'une plainte et l'ouverture d'une enquête, et trouver des traces devient très difficile.»

Pour l'heure, il n'y a quasiment aucune obligation d'annonce. En janvier, le Conseil fédéral a mis en consultation un projet de loi obligeant les infrastructures dites critiques à annoncer les attaques dont elles sont victimes. Depuis 2020, la Finma, le gendarme de la finance, oblige les établissements financiers à lui annoncer des tentatives de cyberattaques. Pour tous les autres secteurs économiques, aucune obligation de ce type n'existe aujourd'hui.

Florian Schütz, délégué de la Confédération à la cybersécurité, a annoncé mercredi que le nombre de cyberincidents qui avaient été volontairement communiqués à la Confédération avait explosé entre 2020 et 2021, passant de 10800 à 21700. «Les autorités ont fait de gros efforts de prévention. Mais nous ne recevons pas assez de notifications volontaires sur les incidents. Et beaucoup d'entreprises, notamment des PME, rechignent encore à investir dans la cybersécurité», a-t-il regretté. ■

Abo Rançons

Les cyberattaques déferlent sur les entreprises suisses

Plus d'un quart des PME suisses ont été la cible de hackers. Un phénomène accéléré par la pratique étendue du télétravail.

Ivan Radja
Publié: 07.08.2021, 22h30

7

Florian Schütz, délégué de la Confédération à la cybersécurité, a annoncé mercredi que le nombre de cyberincidents qui avaient été volontairement communiqués à la Confédération avait explosé entre 2020 et 2021, passant de 10800 à 21700. «Les autorités ont fait de

ne.ch

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Qui sont ces hackers et a-t-on la possibilité de les identifier ?

Groupe criminel **Conti**

Groupe criminel **Lockbit 2.0**

!!! Soupçons !!!

ne.ch

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Conclusion

Choisir un prestataire de service compétent

Les cyberattaques ne visent pas que les autres…

Archivage des données hors réseau

Collaboration avec la police

La sécurité informatique est l'affaire de tous !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

Thierry Chuat
Commissaire - Chef du commissariat CRECO

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL
Département de l'économie, de la sécurité et de la culture
Police neuchâteloise - Police judiciaire
Commissariat Criminalité Economique et Crime Organisé (CRECO)
Passage de la Bonne-Fontaine 36-38
CH - 2300 La Chaux-de-Fonds
Tél. +41 32 889 97 48 (direct)
Tél. +41 32 889 66 91 (secrétariat)
e-mail : thierry.chuat@ne.ch
www.ne.ch/police

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

police
NEUCHÂTELOISE

QUESTIONS ?

MERCI DE VOTRE ATTENTION

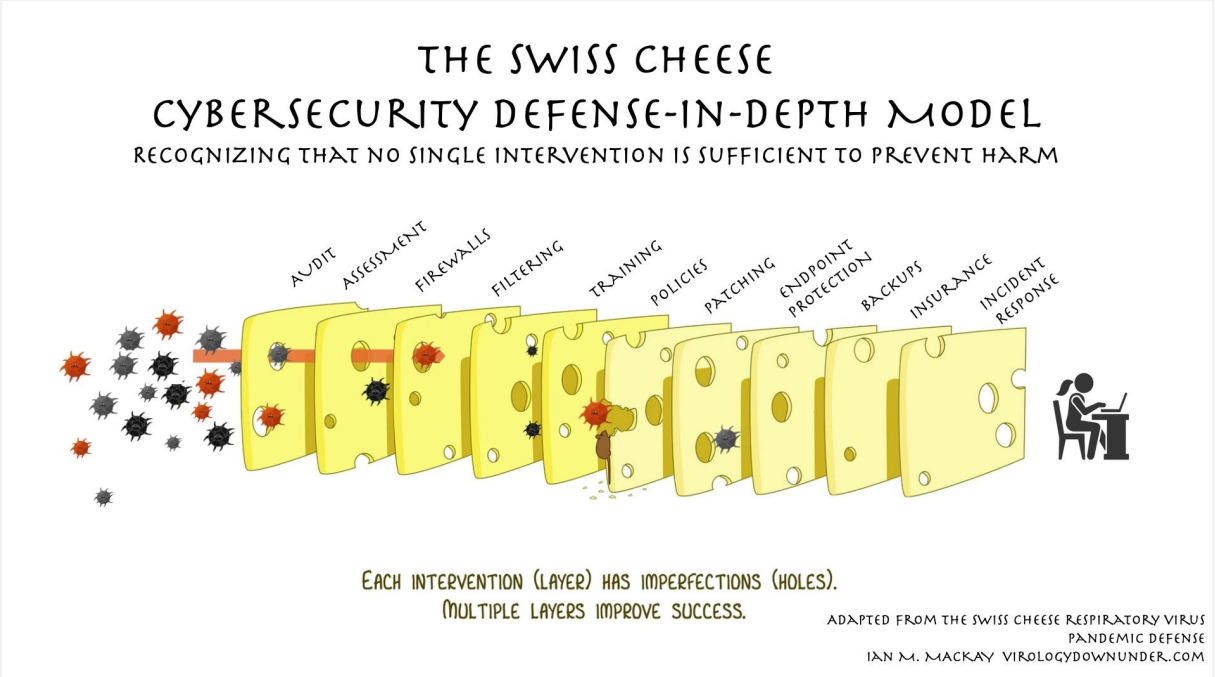
RÉPONSES !

ne.ch

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

CYBERSECURITE: 3 piliers

1. Awareness: prise de conscience, sensibilisation, bonnes pratiques
2. Analyse du parc informatique et de l'organisation interne
3. Monitoring



SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Mesures de bases

La sécurité 100% n'existe pas, mais on peut limiter les risques en compliquant la vie des hackers !

- Bonnes pratiques (p.ex: ne pas cliquer liens ou pièces jointes suspectes)
- Backup**s**: locaux mais aussi externes et isolés
- Gestionnaire de mot de passe et authentification en 2 étapes
- Mises à jour régulières (système, outils de protection, matériel)
- Chiffrement
- Avoir un scénario de crise

Lien vers le Guide SNM Lien vers les exigences minimales FMH

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

2ème partie DIAGNOSTIC / PREVENTION

- Sécurité des données locales / cryptage
- Sécurité des données via portail web / cloud
- Audit de sécurité/label
- Awareness
- Monitoring logiciel
- Monitoring humain
- Sécurité des sauvegardes dans le cloud
- Travail à distance / VPN

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

DIAGNOSTIC / PREVENTION

! Précision importante !

La qualité des prestations fournies par les associations et entreprises qui suivent ne peut être garantie et n'a pas été vérifiée par la SNM/SMSR !

Par ailleurs, la SNM/SMSR précise ne pas avoir à ce jour de partenariat actif avec les produits et entreprises présentés ci après.

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Sécurité des données locales/cryptage

- Dr Samuel Gaillard, fondateur et co-directeur LOGIVAL SA

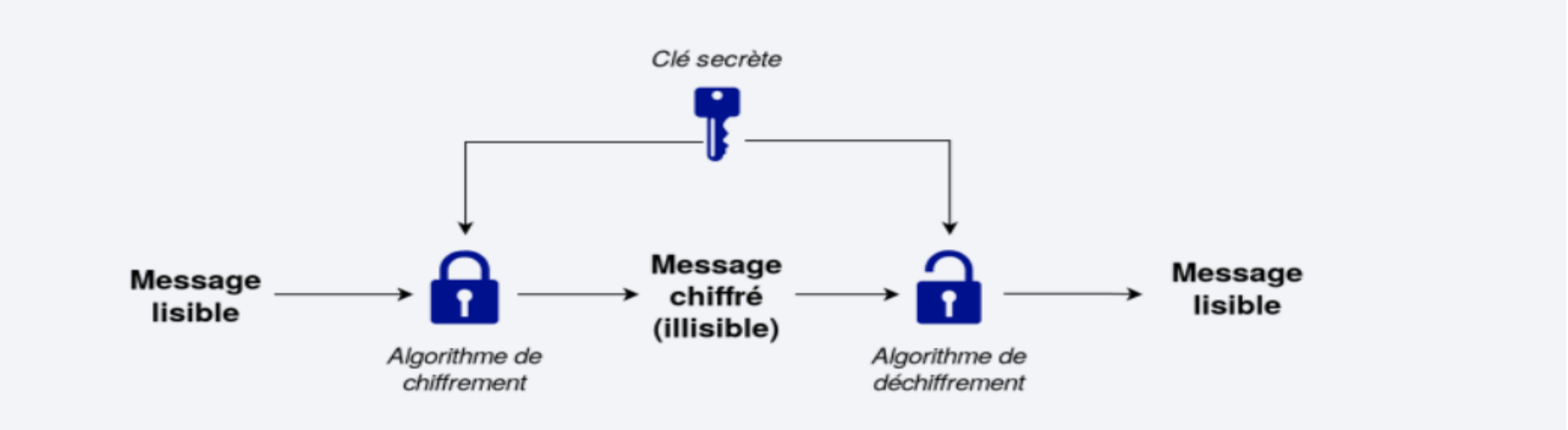
MEDIWAY

SÉCURITÉ ET CRYPTAGE DES DONNÉES

ARCHITECTURE

- Client-serveur
- Données stockées localement
- Données stockées chiffrées

CHIFFREMENT



HTA sévère
Hypercholestérolémie

```
5hZjvgCfIMlhCHkRL6DCH0dfX1Zop+CjCeEFQAiGg1DkkG7
Y8OSGFhi3pYUDkdFGzpSIQHunXdZli0h22IU6EOzP/6e1km
8DEv+rsuPGHQVHJtD/EQIWlni81MLT0HhkuEbB3Bb3hKdtM
aWY2w/P/HrrHDWBZziv8DxC5eW7Eq7qDOcE2QAZu6KSvA8p
trKc6a6fGxABv1DeIX+m2XAVJ3Ghc1QmRS/gY8xBxQD0+52
OSXcHGoC6cOTPHkFnt7rpzJSmXCFo5NJECAqwuNIGucjdsA
oXM5qoJxDuJ6Q8wUmaD3Se3IcNvDugDOFAhn1KV/mTjsxnp
exmOX0BOMIvXzK6d2lsQSZYCtGegTK8A4xVJzJokgJJhARi
```

Problèmes

HTA sévère
Hypercholestérolémie

CHIFFREMENT

- Concerne
  - Eléments saisis
  - Pièce-jointes intégrées
- Avantages
- Limites

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Sécurité des données portail web/cloud

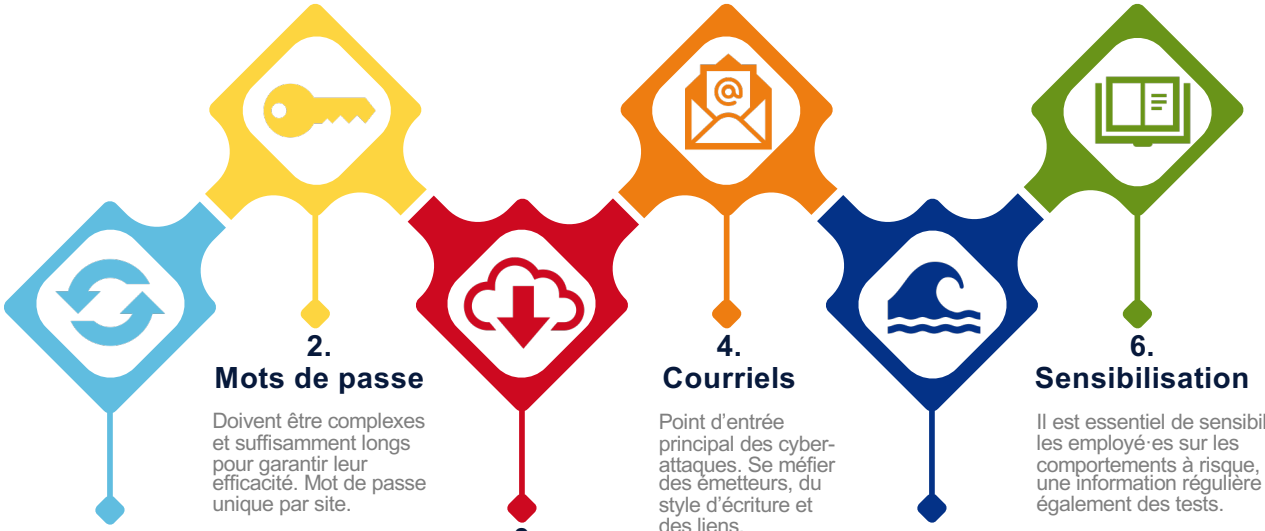
- Mme Catherine Coquart, responsable romande CAISSE DES MEDECINS

Bonnes pratiques d’utilisation d’une solution cloud

11.05.2022, CO

Au cœur de l’innovation

1. Rappel des bonnes pratiques usuelles



1. Systèmes à jour

Action préventive la plus simple et la moins couteuse à mettre en place.

2. Mots de passe

Doivent être complexes et suffisamment longs pour garantir leur efficacité. Mot de passe unique par site.

3. Sauvegardes

Sont essentielles à la reprise après un incident. Elles doivent donc être multiples, régulières et chiffrées.

4. Courriels

Point d'entrée principal des cyber-attaques. Se méfier des émetteurs, du style d'écriture et des liens.

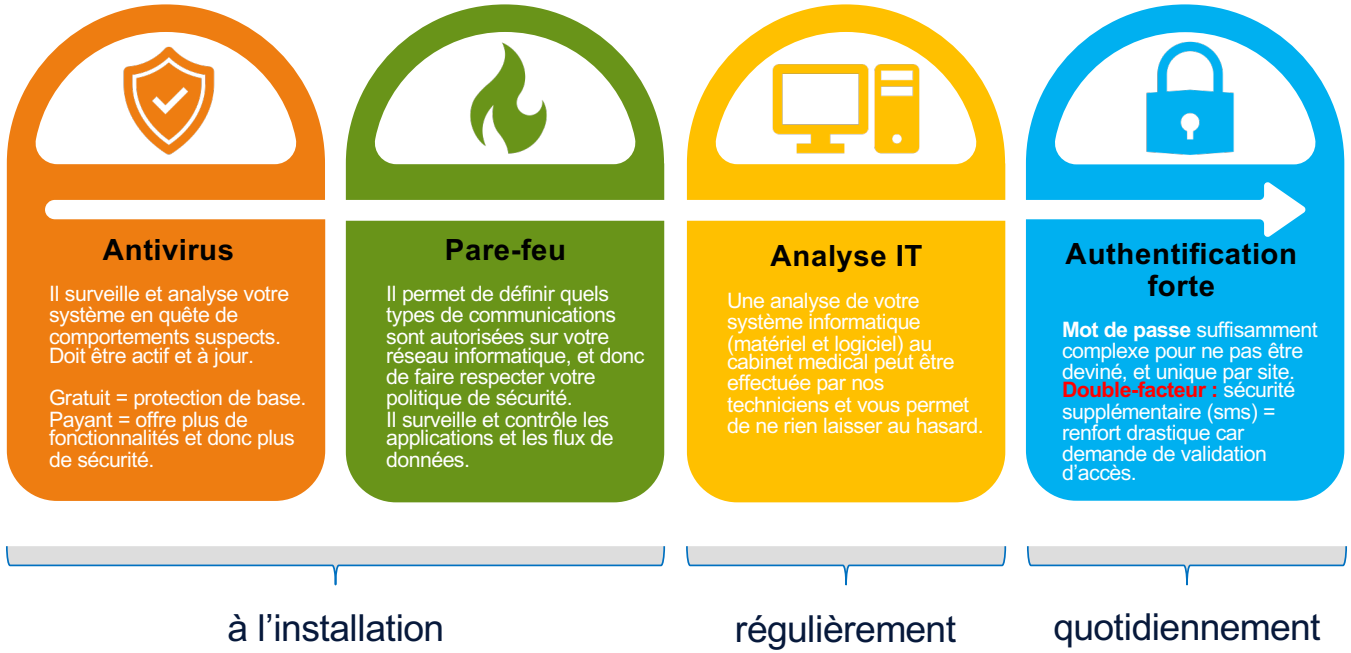
5. Événements physiques

Les catastrophes naturelles ou intentionnelles peuvent aussi menacer vos données. Contrôlez les accès à votre infrastructure contre les personnes non autorisées, les fuites d'eau, les inondations, les incendies…

6. Sensibilisation

Il est essentiel de sensibiliser les employé·es sur les comportements à risque, par une information régulière et également des tests.

2. Quatre piliers d’un environnement sécurisé



3. Accès à MediOnline : rester en lieu sûr

RISQUES

- Vol des données d'accès
- Redirection vers un site d'apparence trompeuse

CONSEILS

- Ne jamais écrire ses identifiants sur un post-it ou dans un fichier non protégé. Ne jamais les communiquer. Activer l'authentification forte (2FA).
- Utiliser des raccourcis personnels, ne jamais suivre un lien dans un e-mail inattendu

Vérification en tout temps du propriétaire d'un service Web depuis le navigateur :

La Caisse des Médecins utilise un certificat « EV SSL »

4. Sécurité des données à la Caisse des Médecins

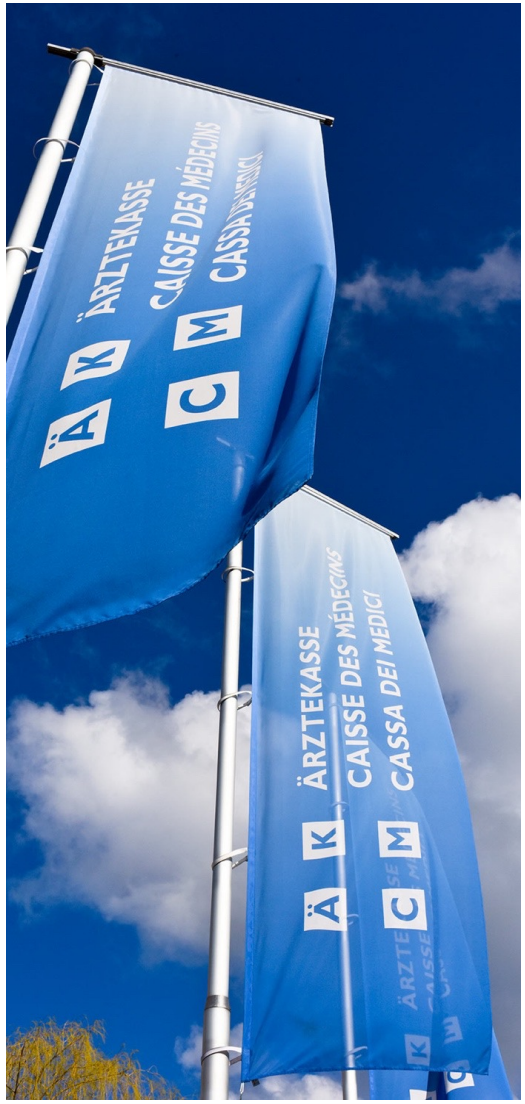
- Hébergement synchrone sur deux sites distants de 7km
- Sauvegardes sur plusieurs médias différents
- Données des patients chiffrées
- Tests réguliers d'intrusions indépendants

Merci de votre attention

https://www.caisse-des-medecins.ch/support/securite/

Caisse des Médecins
Société coopérative
Chemin du Curé-Desclouds 1
1226 Thônex

- Tel. 022 869 46 30
- romandie@caisse-des-medecins.ch



SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

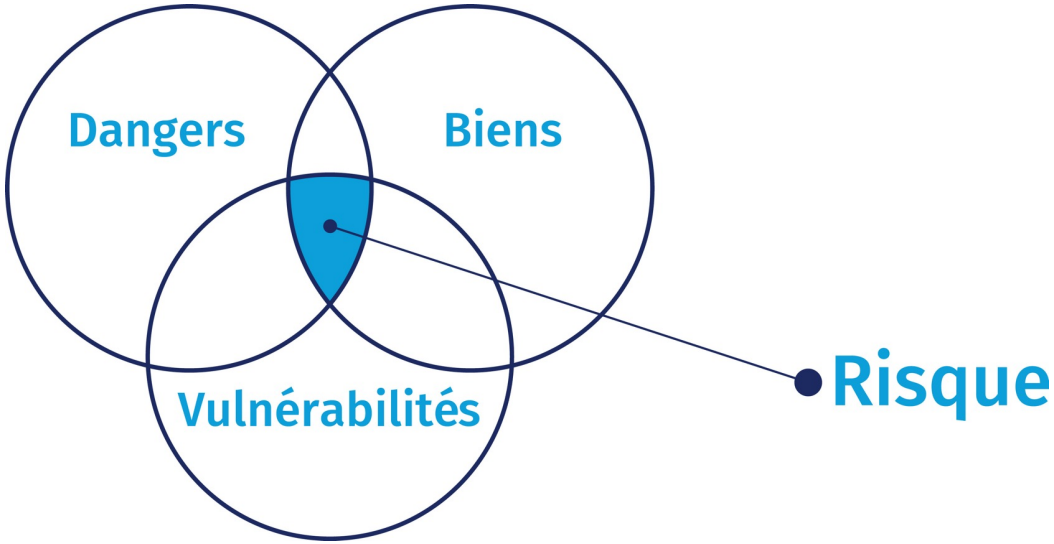
Audit de sécurité / label

- Dr Christophe Hauert, membre fondateur association CYBER-SAFE

Label cyber-safe.ch: de l'analyse de risque à la labellisation

Conférence «Cybersécurité en cabinet»
Dr. Christophe Hauert
11 mai 2022, Neuchâtel

La notion de risque cyber



Avant de choisir comment vous protéger ou vous assurer:

Quels sont les impacts en cas d'incident ?

Type de données:

- **Données administratives**
- **Données financières**
- **Données de tiers**
- **...**

Valeur des données & CIA

- **Confidentialité:**

Combien perdrez-vous si ces données sont divulguées au grand public ?
Ex: vos données de R&D

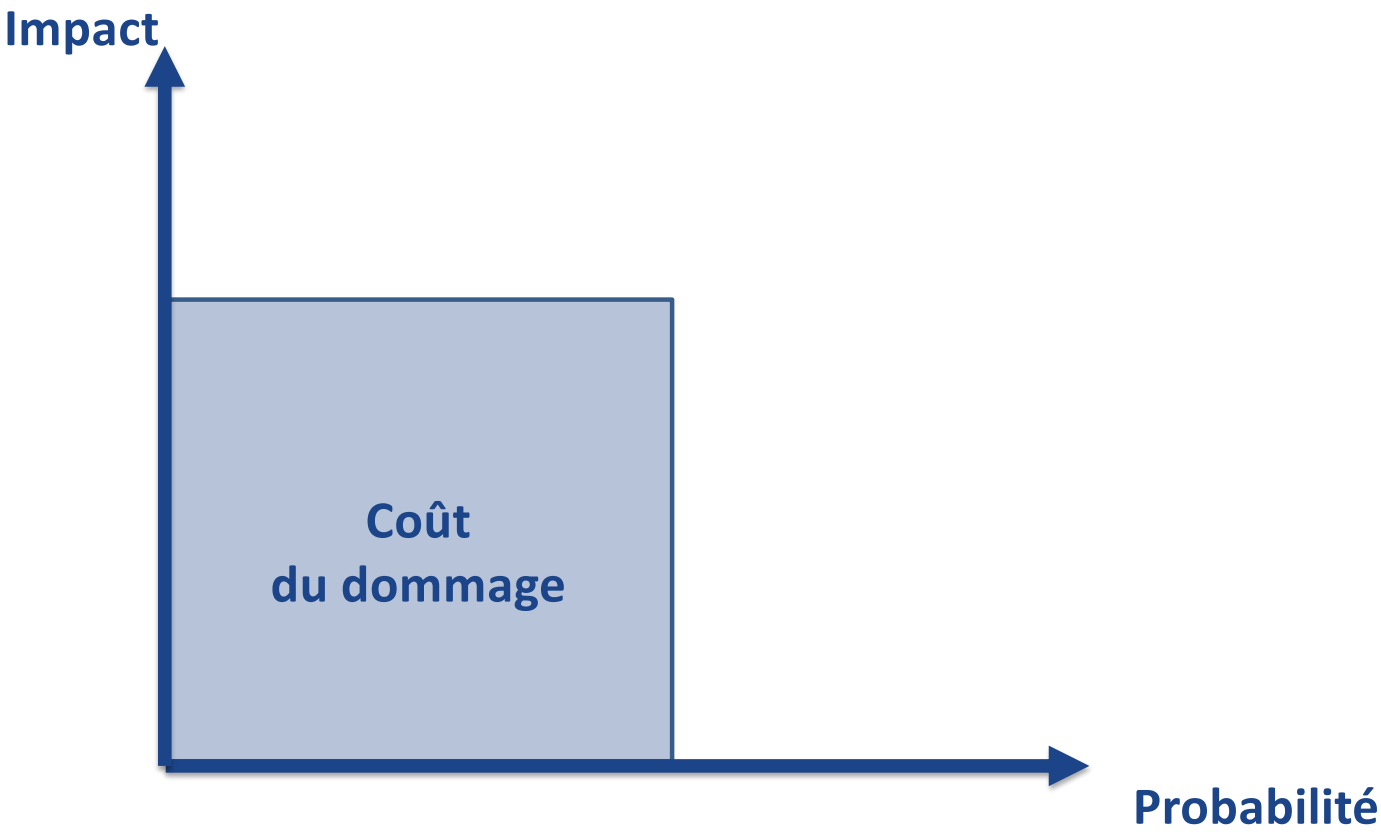
- **Integrité:**

Combien perdrez-vous si ces données sont modifiées ?
Ex: comptes de paiement

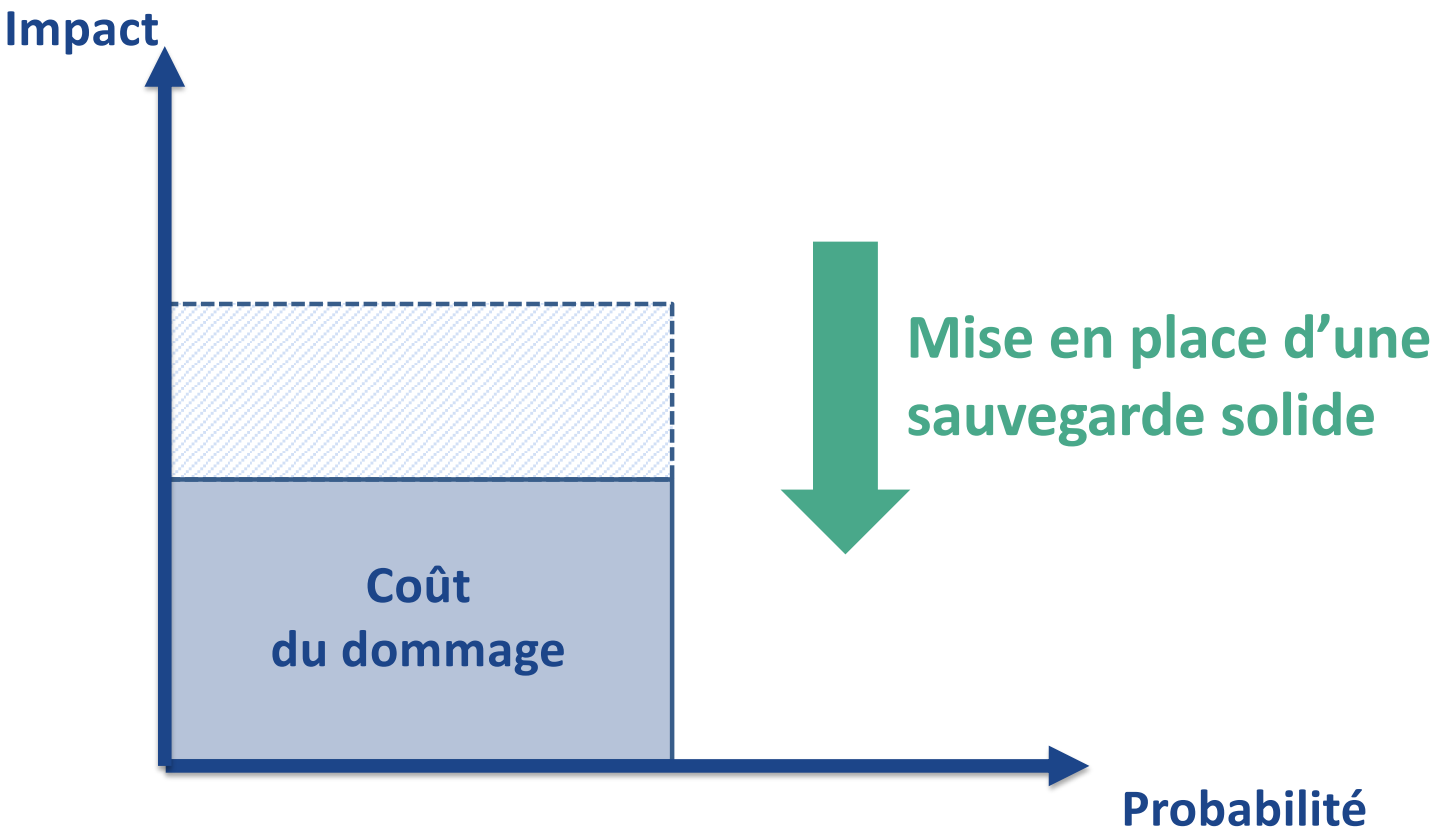
- **Accessibility (disponibilité):**

Combien perdrez-vous si ces données ne sont plus accessibles, temporairement ou définitivement ?
Ex: combien d'employés ne peuvent travailler pendant une panne de 3 jours ?

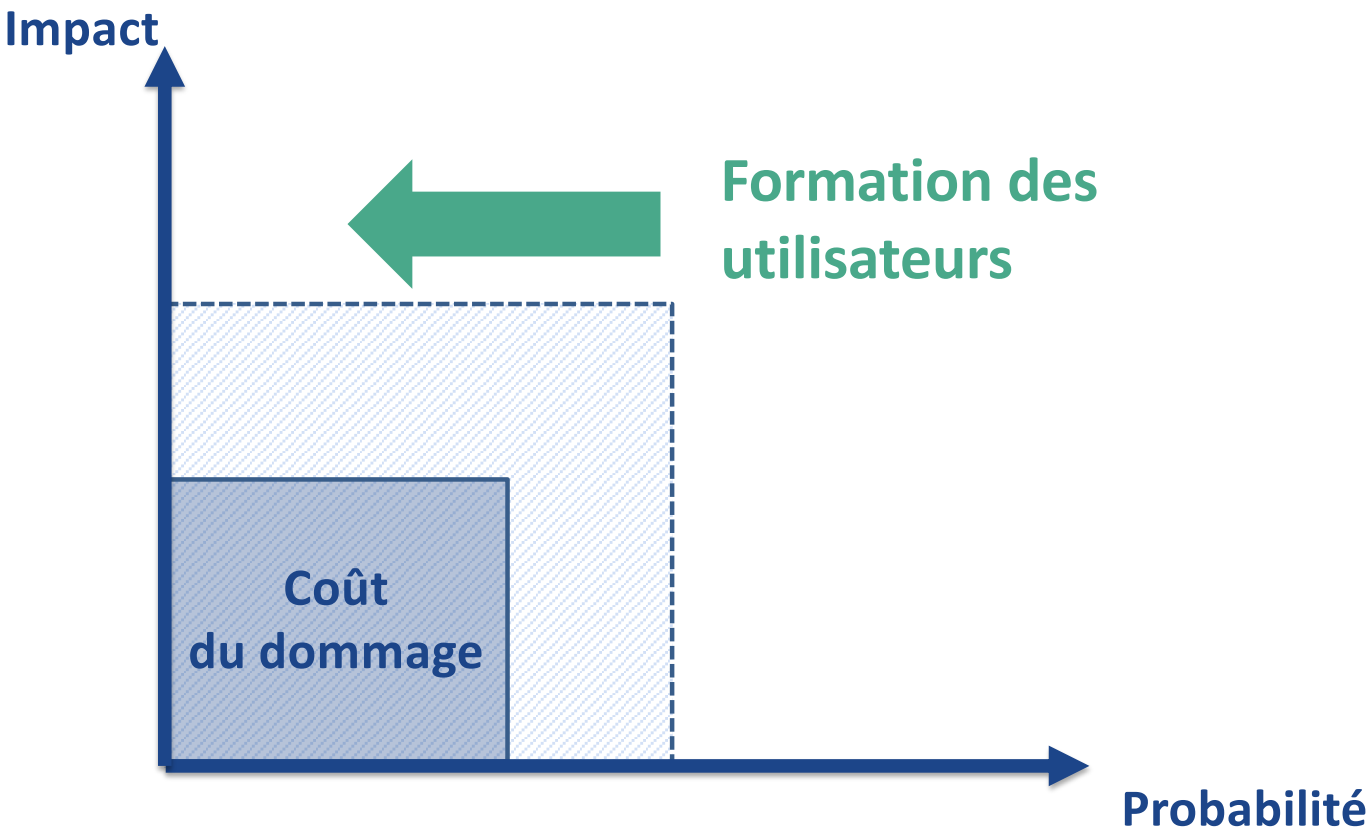
Le risque cyber: résumé



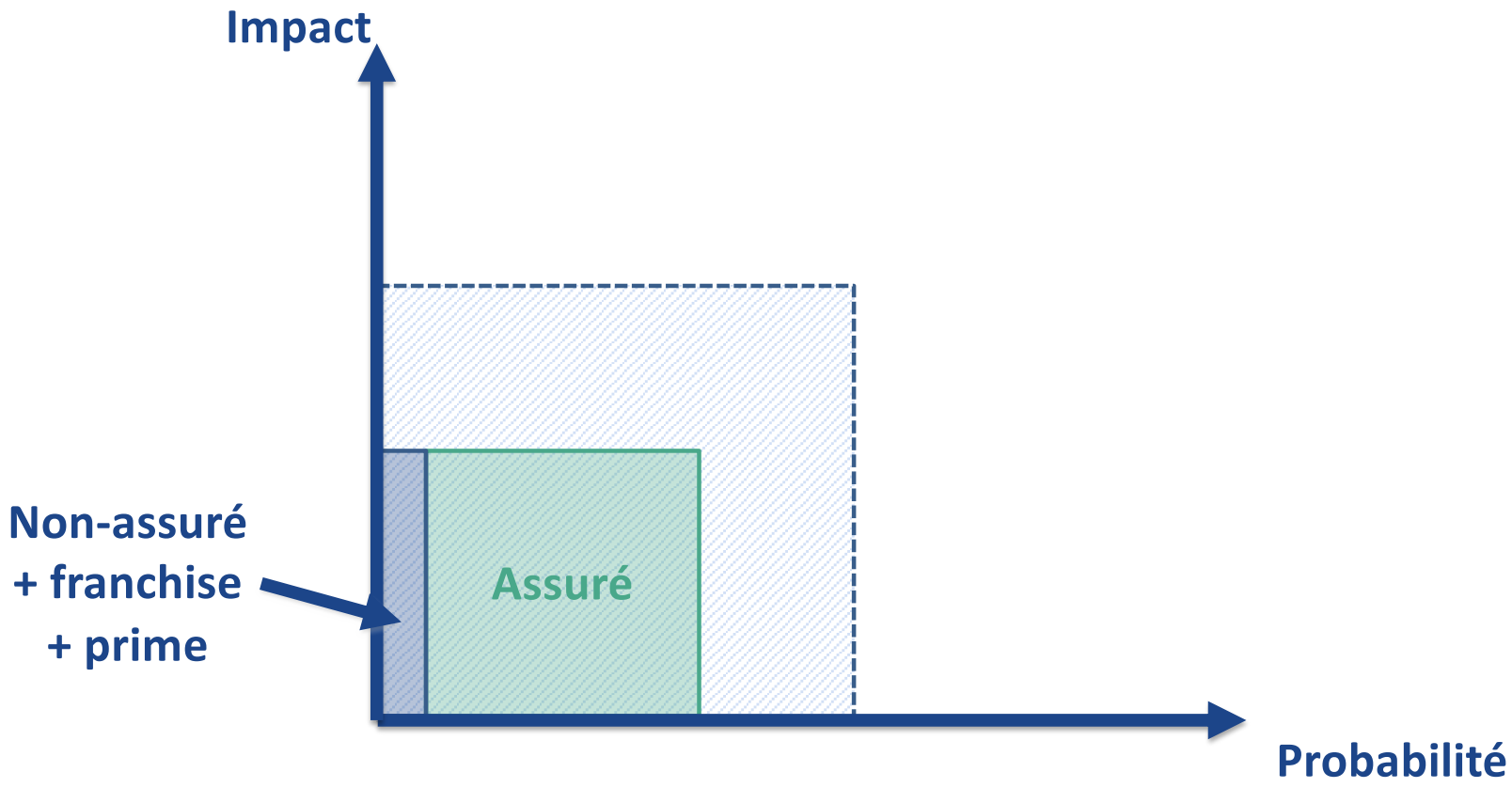
Le risque cyber: résumé



Le risque cyber: résumé



Le risque résiduel



FAIL

Vulnérabilités fréquentes

Aussi bien techniques qu'organisationnelles:

- Attribution de la **responsabilité**
- **Mises à jour** (OS et équipements)
- **Droits d'accès** et gestion des **mots de passe**
- Inventaire des données et **chiffrement**
- **Sensibilisation** à l'hameçonnage
- …

NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	1 sec	5 sec
8	IMMÉDIATEMENT	5 sec	22 min	1 heure	9 heures
10	IMMÉDIATEMENT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

*source : SCSP Community (Seasoned Cyber Security Professionnals)

Chappatte, Le Temps, 28.01.2022

CYBER SAFE

CYBER SAFE

Qui sommes-nous ?

- Monde économique, politique, académique et associatif
- 8’500 PME et >300 communes représentées
- Partenaire en CH-D

SKO ASC ASQ Association suisse des cadres

GIM-CH Groupement suisse de l'industrie mécanique SWISSMECHANIC Suisse romande

heig-vd

Hes·so

EPFL C4DT Center for Digital Trust

CVCI Chambre vaudoise du commerce et de l'industrie

FPE-CIGA Fédération Patronale et Économique

Chambre Valaisanne de Commerce et d'Industrie
Walliser Industrie- und Handelskammer

Fédération des Entreprises Romandes Neuchâtel

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

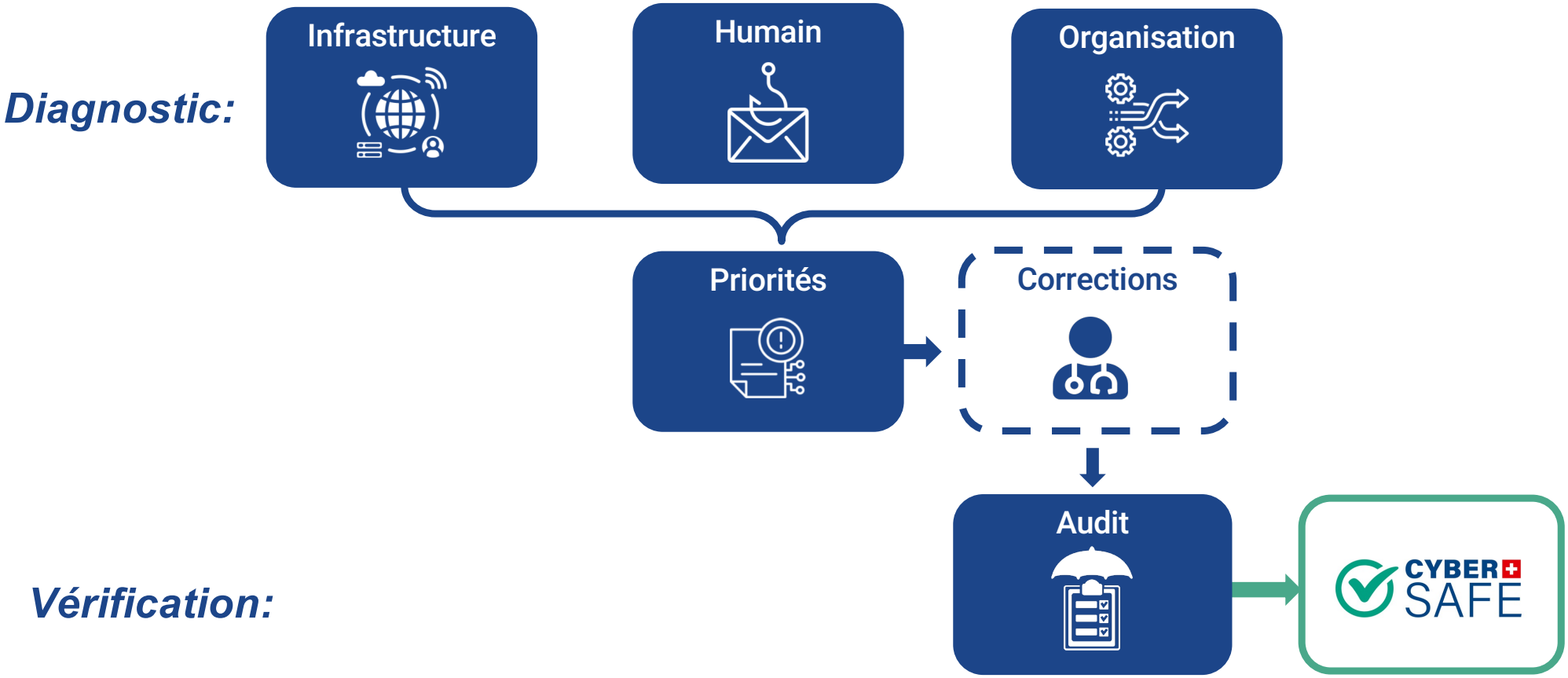
CCIG Chambre de commerce, d'industrie et des services de Genève

UNION DES COMMUNES VAUDOISES

ISSS Information Security Society Switzerland

.ICØN

Label Cyber Safe



CYBER SAFE

Données en Suisse

Prix selon #PC
Valable 2 ans

info@cyber-safe.ch

Des questions?

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Awareness

- M. Thomas Jacot, Senior Key Account Manager HIN

Awareness

Thomas Jacot, Senior Key Account Manager

Neuchâtel, 11 mai 2022, Cybersécurité en cabinet

© Health Info Net SA, Cybersécurité en cabinet [public]

Sécurité informatique

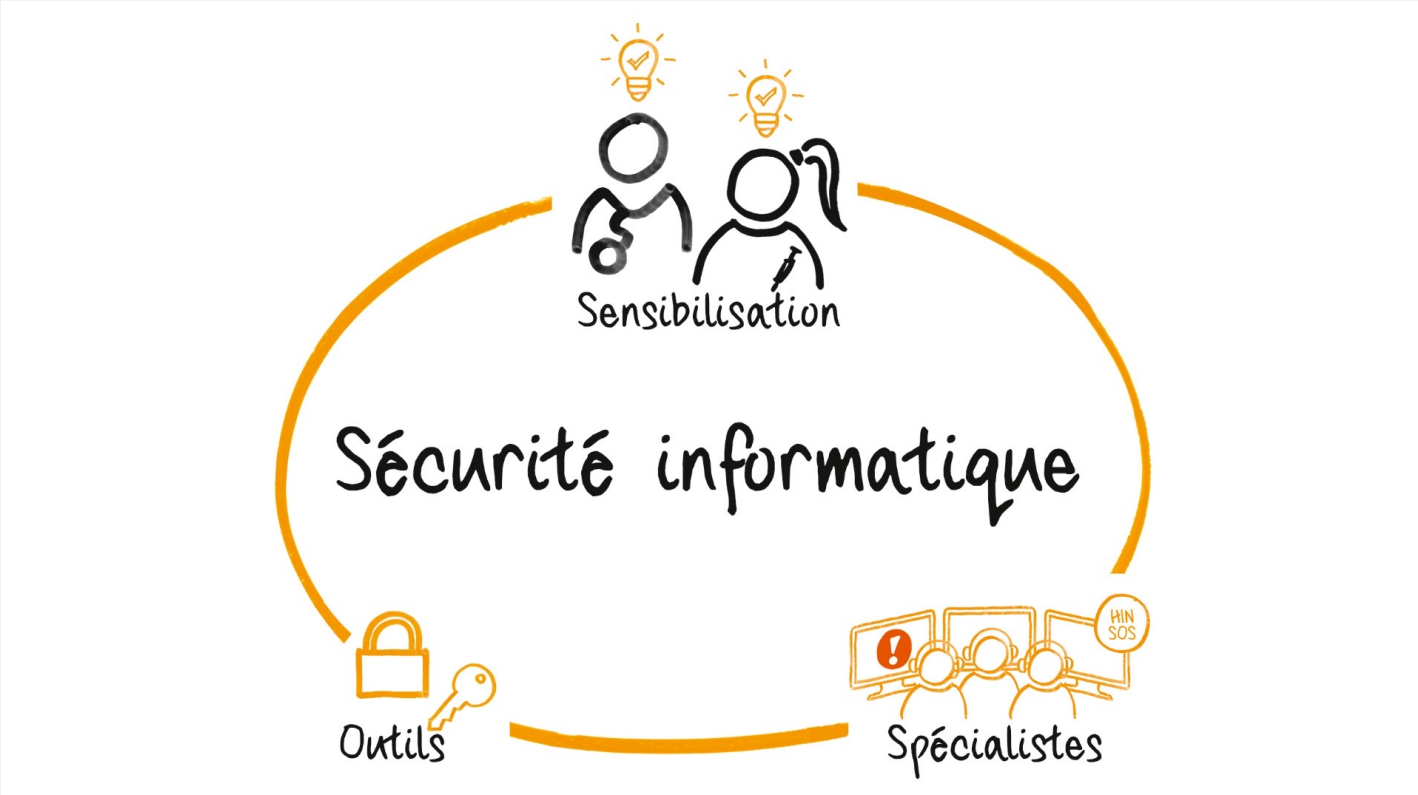
En quoi est-ce que ça me concerne?

© Health Info Net SA, Cybersécurité en cabinet [public]

La sécurité informatique – une question qui concerne aussi le traitement des données des patients

© Health Info Net SA, Cybersécurité en cabinet [public]

Nécessité d’une approche globale



© Health Info Net SA, Cybersécurité en cabinet [public]

Awareness

Qu'est-ce que la sensibilisation ?

© Health Info Net SA, Cybersécurité en cabinet [public]

Awareness …

… [en anglais], **sensibilisation**, sensibilisation éveillée (des événements internes et environnementaux), **conscience**. Elle permet la **perception** des besoins prédominants et donc une différenciation accrue entre l'organisme et l'environnement. **La pleine conscience**.

Traduction libre d'après Dorsch – Lexikon der Psychologie (2020)

... plus qu'une "simple" transmission d'informations

Les mesures de sensibilisation ne représentent pas seulement une transmission de connaissances et de contenus, mais doivent également entraîner un changement d'attitude et donc de comportement.

Awareness n'est pas synonyme de transmission d'informations !

© Health Info Net SA, Cybersécurité en cabinet [public]

HIN Awareness

Concept de sensibilisation

© Health Info Net SA, Cybersécurité en cabinet [public]

L'objectif : la sensibilisation

- Sensibiliser - aiguiser la conscience
- Déclencher la dissonance cognitive
- Motiver - activer les ressources
- **Modifier le comportement**

© Health Info Net SA, Cybersécurité en cabinet [public]

La solution …

1. Montrer la pertinence personnelle
2. Susciter la peur
3. Demander un engagement
4. Transmettre des recommandations spécifiques

© Health Info Net SA, Cybersécurité en cabinet [public]

Merci de votre attention !

Nous répondrons volontiers à vos questions.
N'hésitez pas à nous contacter :

Health Info Net SA
Avenue des Sciences 13
1400 Yverdon-les-Bains

Call Desk 0848 830 741

infosr@hin.ch

www.hin.ch

Thomas Jacot, Senior Key Account Manager

thomas.jacot@hin.ch

© Health Info Net SA, Cybersécurité en cabinet [public]

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Monitoring logiciel

- M. Thibaut Robert-Charrue, directeur FORTERESSE

FORTERESSE

Swiss IT & CyberSecurity

Présentation du monitoring logiciel

Thibaut Robert-Charrue

Directeur de Forteresse CyberSecurity

FORTERESSE
Swiss IT & CyberSecurity

Comprendre la menace

FORTERESSE
Swiss IT & CyberSecurity

24h de monitoring d'attaque sur un cabinet médical neuchâtelois

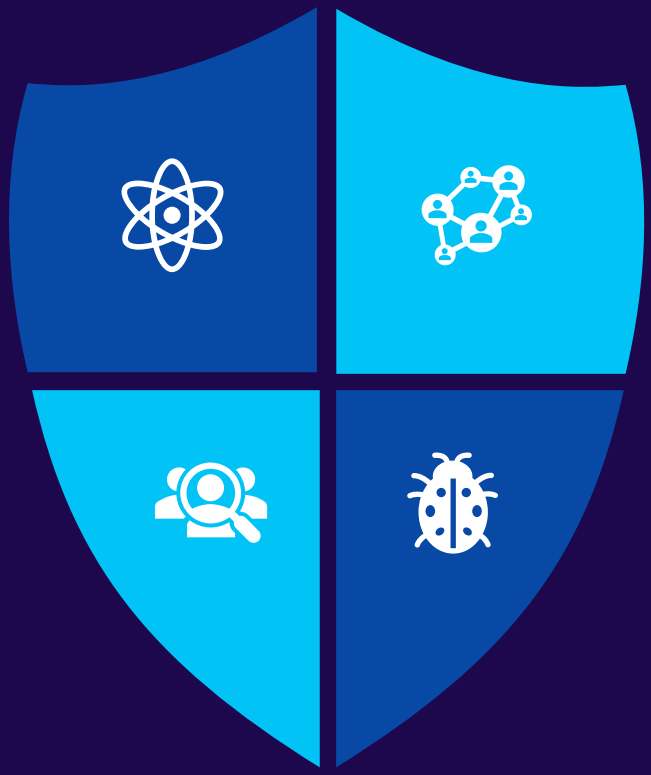
Enregistrement du 5 mai 2022

FORTERESSE
Swiss IT & CyberSecurity

Comprendre le monitoring logiciel

La fondation

L'interprétation



Les logiciels

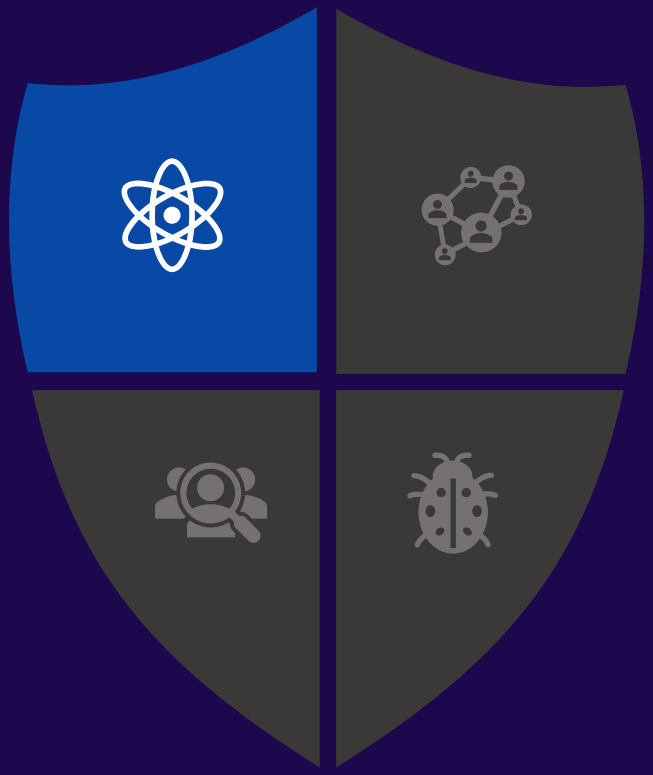
Les données

FORTERESSE
Swiss IT & CyberSecurity

Comprendre le monitoring logiciel

La fondation
(ce qui doit être surveillé)

Tous les serveurs, ordinateurs, téléphones, routeurs et objets connectés



L'interprétation

Les logiciels

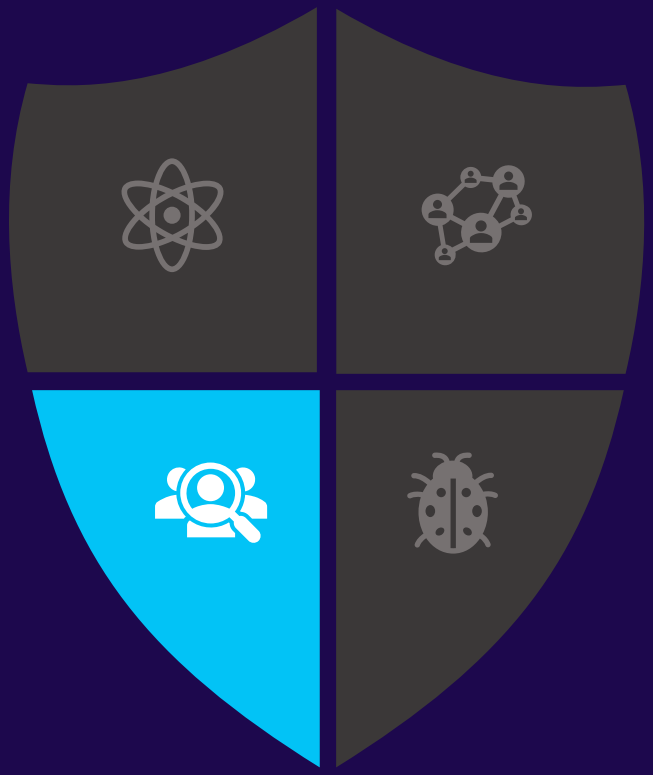
Les données

FORTERESSE
Swiss IT & CyberSecurity

Comprendre le monitoring logiciel

La fondation

L'interprétation



Les logiciels
(ce qui permet la surveillance)

Surveillance et enregistrement de ce qui se passe dans la fondation. Mais également comment cela se passe.

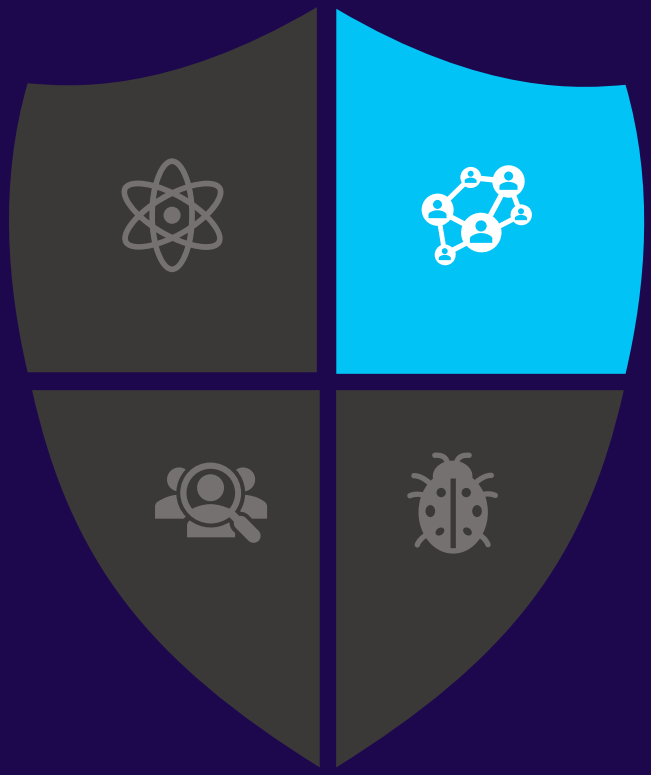
Les données

FORTERESSE
Swiss IT & CyberSecurity

Comprendre le monitoring logiciel

La fondation

Les logiciels



L'interprétation
(Analyse des données)

Analye de ce qui est remonté par les logiciels et mise en place de graphiques et statistiques, ains qu'alimentation des base de données communes.

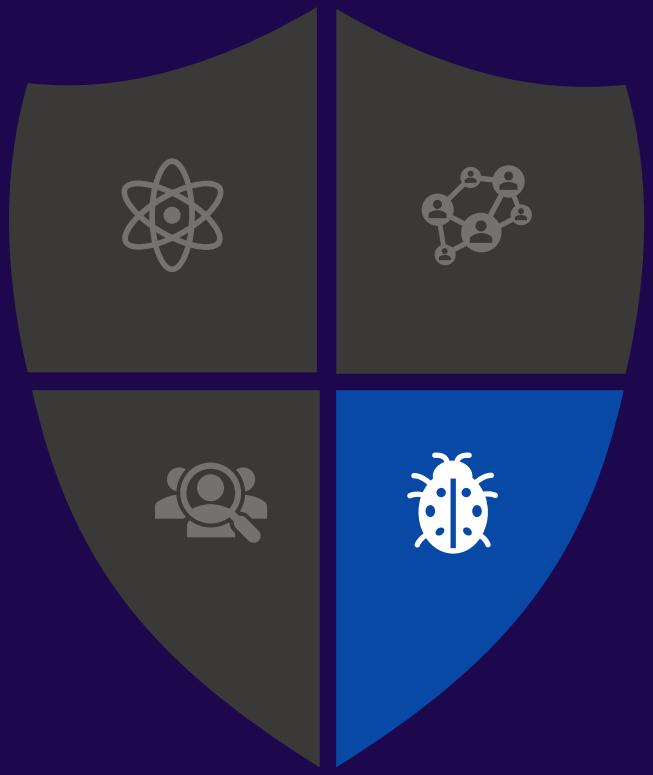
Les données

FORTERESSE
Swiss IT & CyberSecurity

Comprendre le monitoring logiciel

La fondation

L'interprétation



Les logiciels

Les données externes

(Toutes les autres données)

Surveillance des différentes sources disponibles sur le darkweb, les bulletins officiels, etc

FORTERESSE
Swiss IT & CyberSecurity

FORTERESSE

Swiss IT & CyberSecurity

Réseaux **Données** **EndPoint** **E-mails**

Christelle Moreau

Thibaut Robert-Charrue

Contact

info@forteresse.pro

www.forteresse.pro/SMSR

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Monitoring humain

- M. Julien Bressieux, Chief Operating Officer ZENDATA


SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE
ZENDATA
DON'T BE THE NEXT ONE
ZENDATA
expert Suisse cybersécurité
L'humain, un élément clé de la sécurité de demain
Julien Bressieux
Dir. des opérations - ZENDATA

Cybercriminalité et Santé

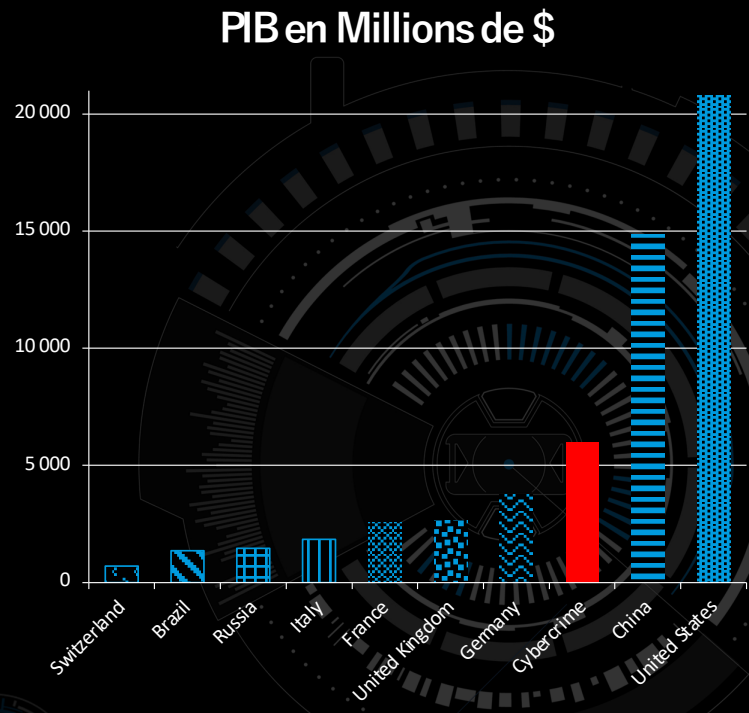
305

Attaques par semaine en Suisse dans le domaine de la santé en 2021

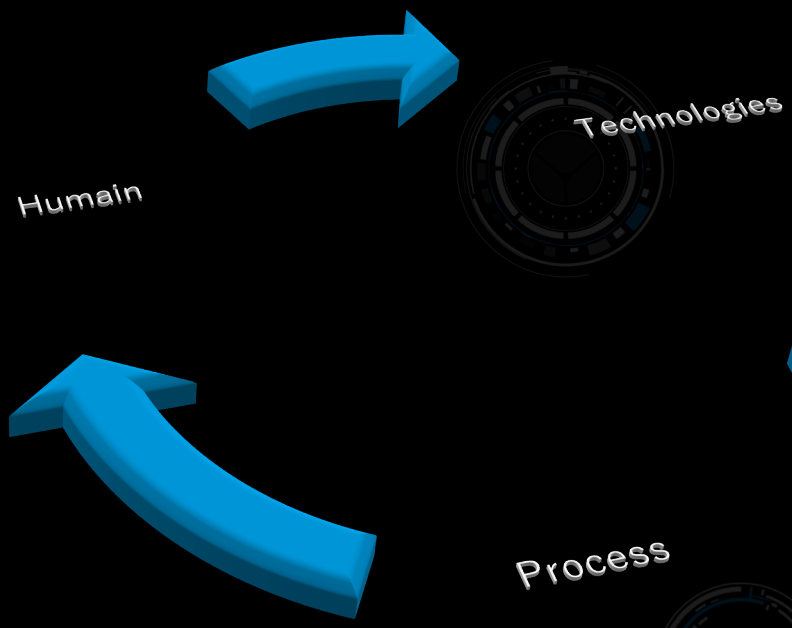
85 %

Des cyberattaques sont motivées par des raisons financières

Le reste est lié à l'espionnage et au hacktivisme



Les piliers de la cybersécurité



La cyberattaque de HSE

Health Service Executive
Feidhmeannacht na Seirbhíse Sláinte

Opening of email attachment led to HSE cyber attack, report finds

Ransomware attack could be repeated and HSE is taking steps to mitigate risk, says Reid

Fri, Dec 10, 2021, 12:05 | Updated: Fri, Dec 10, 2021, 12:08

HSE cyber-attack: Irish health service still recovering months after hack

By Michael Sheils McNamee
BBC News NI

5 September 2021

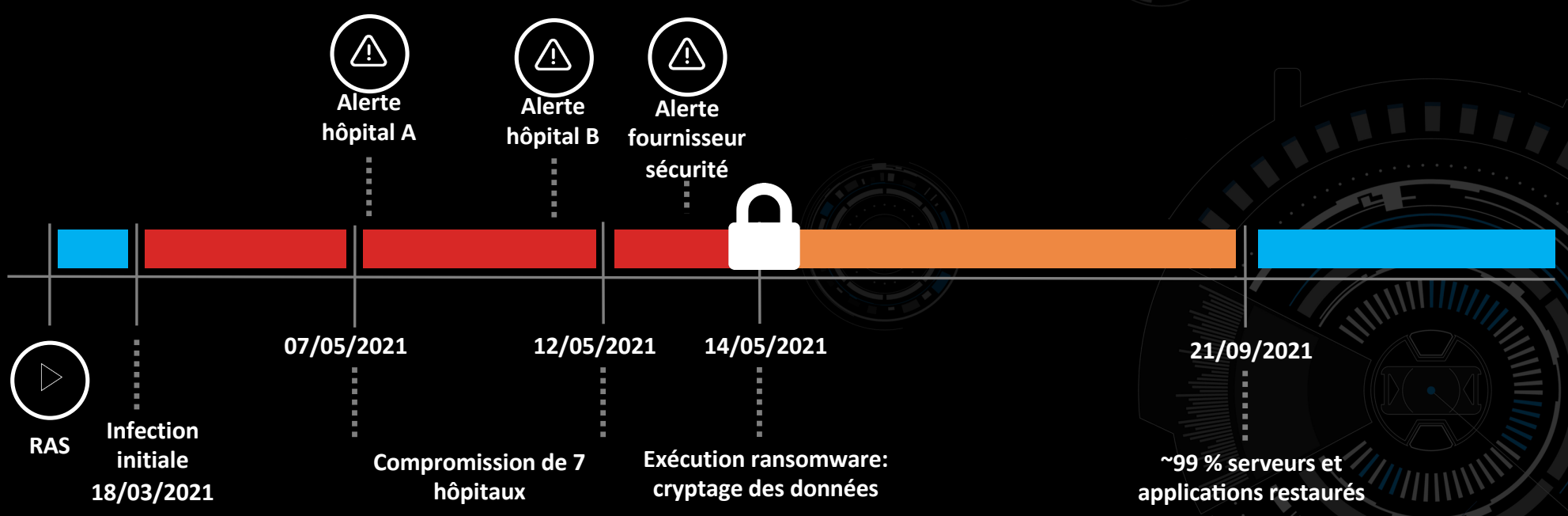
Report reveals hackers got into 'frail' IT system two months before HSE took action

HSE failed to respond to alerts of malicious activity before crippling cyber attack, report reveals

May 14 hacking left computer systems paralysed for weeks and led to mass cancellation of vital surgeries and scans

Frise chronologique de l'attaque

Health Service Executive
Feidhmeannacht na Seirbhíse Sláinte



l’atout humain

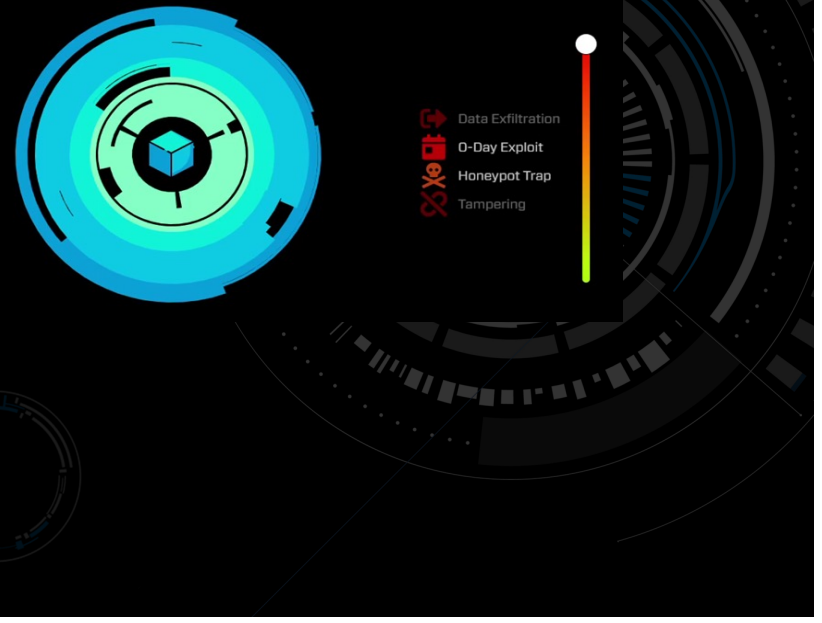
expertise

Compréhension des alertes

Comprehension des TTP des hackers

Investigation – Isolation
Remediation et correction des vulnérabilités

PRO ACTIF



contact

ZENDATA
DON'T BE THE NEXT ONE

www.zendata.ch
022 588 65 90
info@zendata.ch

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Sécurité des données dans le cloud

- M. Johnny Veillard, directeur PARTNER IT

PARTNER iT

Votre partenaire informatique

La sécurité des sauvegardes dans le cloud

PARTNER iT
Votre partenaire informatique

LES RISQUES

La 1re place

revient, avec 27%, aux **défaillances matérielles** qui comptent parmi les causes les plus fréquentes de perte de données.

L'erreur humaine (26%) occupe quant à elle la 2e place.

Une PME sur 3

a été victime d'une **cyberattaque**, sachant qu'il faut en moyenne **200 jours** pour s'en rendre compte.

43%

des cyberattaques ciblent les **PME**.

36% ont subi des conséquences financières suite à l'attaque

LES AVANTAGES D'UNE SAUVEGARDE DANS LE CLOUD

- Se prémunir d'un **vol physique** d'un serveur, d'un PC ou du NAS
  - La sécurité d'un datacenter est au même niveau qu'une banque
- Se prémunir des **dégâts matériel** sur le site
  - Incendie, inondation, bris, …
- Service **automatique**
  - Pas d'intervention humaine
- **Rétention** des données
  - Conservation de l'historique des données
- **Restauration** complète ou partielle
  - Machine complète ou fichier par fichier
- Sauvegarde de **différents systèmes**
  - Serveurs, PC, NAS, …

LA SAUVEGARDE DANS LE CLOUD MÉRITE VOTRE ATTENTION

- S'assurer que le serveur de sauvegarde est **en Suisse**
  - Confidentialité des données
- S'assurer du **cryptage** des données
  - Pendant le transfert et la sauvegarde
- Durée de la **rétention** des données
  - Attention aux virus crypto-lockers
- S'assurer de **l'intégrité** des données sauvegardées
  - Effectuer des tests de restauration de données

Merci pour votre attention

PARTNER iT

Votre partenaire informatique

CONTACT

Johnny Veillard, CEO

jv@partnerit.ch

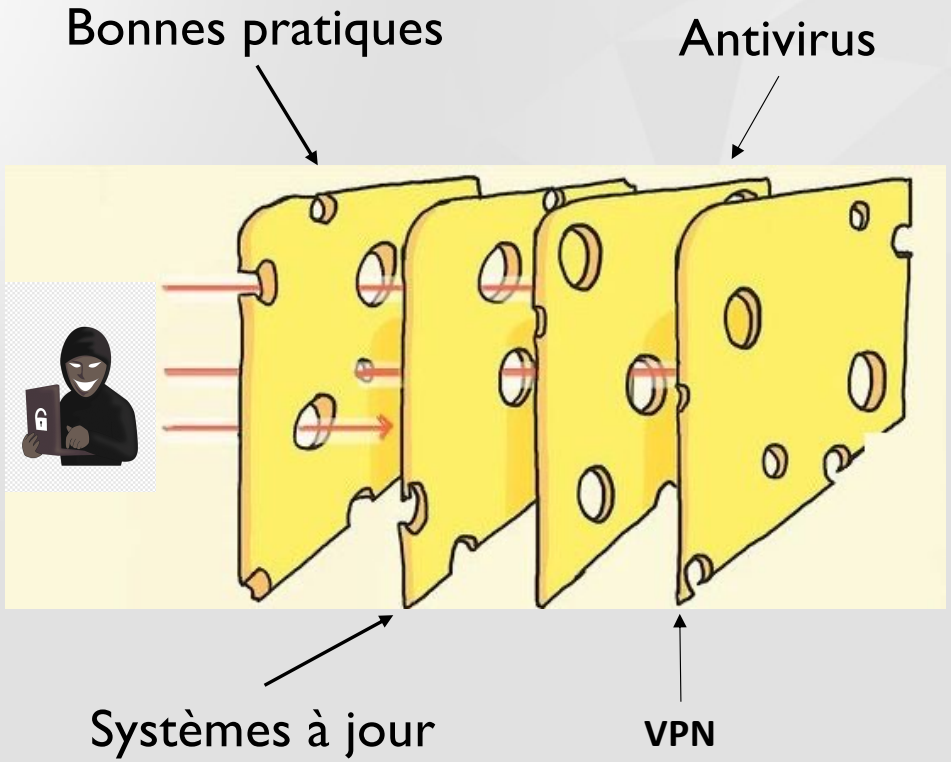
SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

VPN: Sécurisation travail à distance

- M. Marc Beauverd, département technique WIFX

MARC BEAUVERD
INGÉNIEUR SYSTÈME IT
SPÉCIALISTE VOIP

Le modèle du fromage suisse (Emmental)



VPN : DÉFINITION ET SIGNIFICATION

En informatique, un réseau privé virtuel (VPN) est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

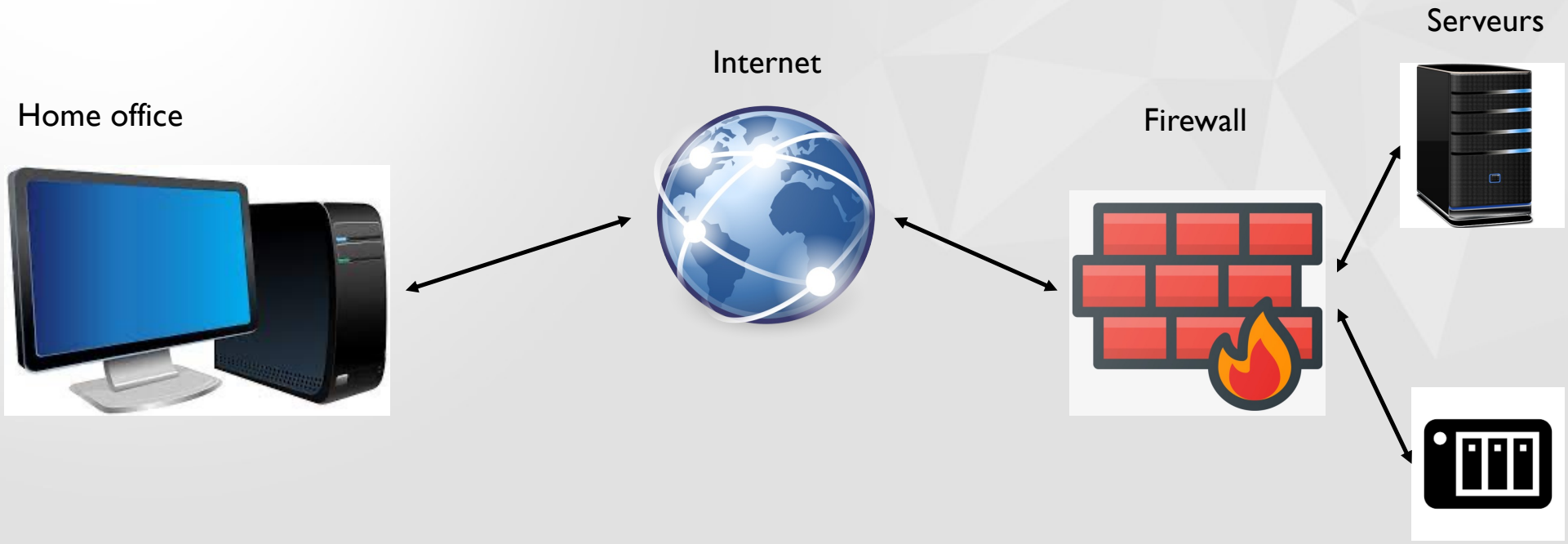
WIFX NETWORK SPECIALIST LoRa Alliance®

VPN, comment Ça marche

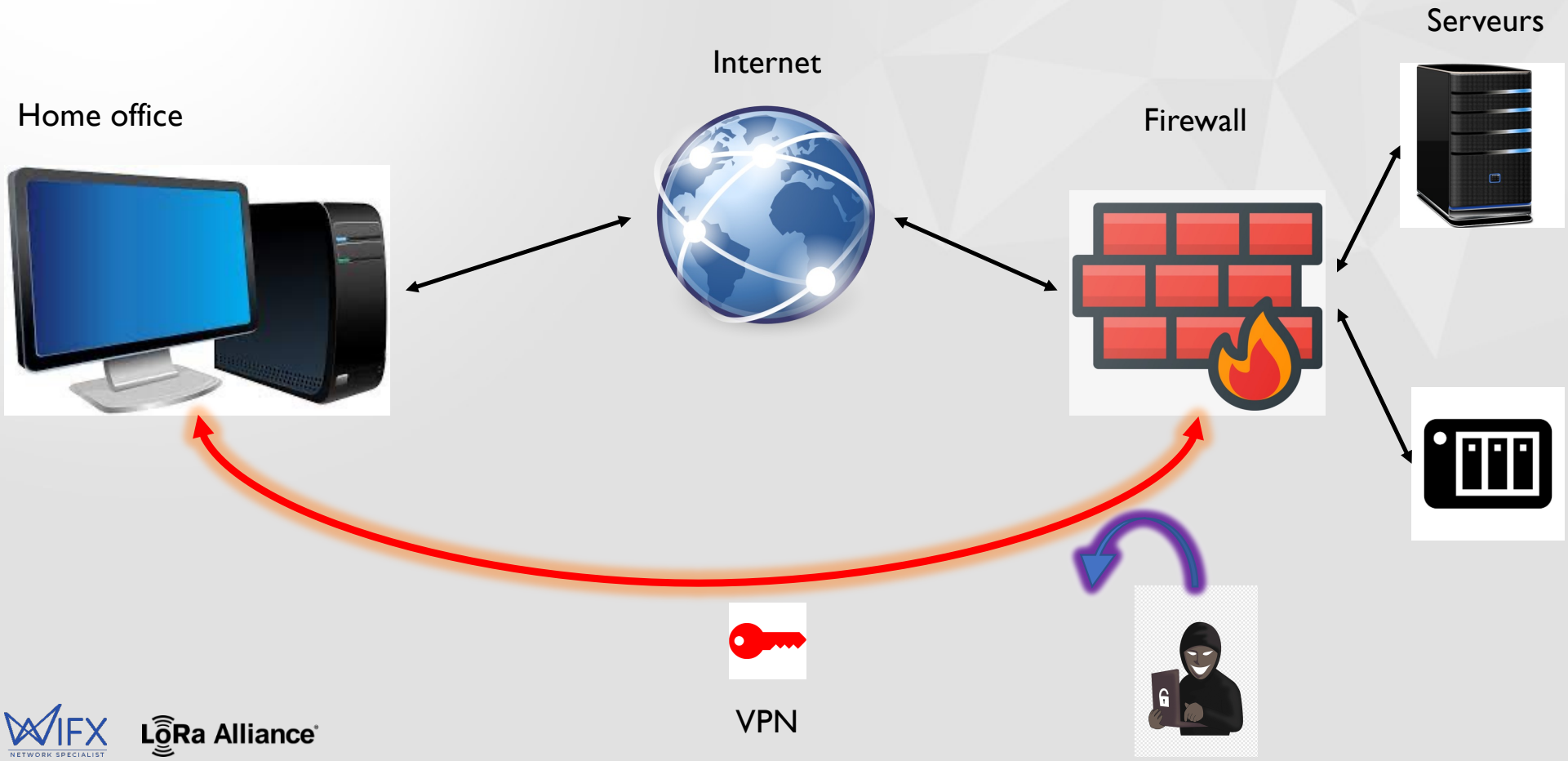
Internet

Home office

VPN, comment ça marche



VPN, comment Ça marche



MERCI DE VOTRE ATTENTION

Wifx Sàrl
Avenue des Sciences 2
1400 Yverdon-les-Bains
Phone: +41 24 550 01 70
https://www.wifx.net

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

3ème partie CONCLUSIONS/REFLEXIONS

- Hébergement des données de santé: normes et enjeux
- Point de vue de la FMH actuel et en discussion
- Conclusions de la soirée
- Questions
- Evaluation / attestation de formation

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Hébergement des données de santé: normes et enjeux

- Mme Aurélie Rosemberg, société de conseil santé et digital SYRMA

«Cybersécurité en cabinet»
Points clés de la gestion de l'hébergement

Aurélie Rosemberg

CEO & Founder Syrma Consulting

Conseils stratégiques – santé et digital

www.syrma.ch

11.05.2022
SNM

Sommaire

1. Comparatif des niveaux d'hébergement
2. L'importance de la classification dans le choix
3. La cybersécurité démarre par la gestion des contrats IT
4. Serious game en gestion des risques cyber et gestion de crise : sensibilisation & entraînement
5. Clusis : réseau d'experts indépendants

1. Comparatif des niveaux d'hébergement

Niveau Tier 1	Niveau Tier 2	Niveau Tier 3	Niveau Tier 4
• Un seul circuit électrique • Un seul circuit de distribution de refroidissement • Pas de redondance • Disponibilité de 99.67% • Interruption annuelle 28H	• Un seul circuit électrique • Un seul circuit de distribution de refroidissement • Composants redondants pour les circuits • Disponibilité de 99.75% • Interruption annuelle de 22H	• Plusieurs circuits d'alimentation électrique • Plusieurs circuits de refroidissement • Une redondance N+1 (ni intégrale, ni entièrement distincte) • Disponibilité 99,982% • Interruption annuelle 1H30 env.	• Plusieurs circuits d'alimentation électrique • Plusieurs circuits de refroidissement • Une redondance 2N+1 (deux redondances avec 1 non en pleine capacité) • Diponibilité 99,99% • Interruption annuelle 48 minutes

Syrma

2. L’importance du niveau de classification dans le choix

- Toute entreprise qui doit externaliser le stockage de ses serveurs informatiques doit choisir un prestataire ayant un niveau de qualification adapté aux conditions exigées par le contenu de ces données.
- Si les données stockées ont une importance vitale, le choix d’un data center avec le niveau Tier 4 est indispensable, car l’entreprise ne peut pas prendre le risque de voir ces données effacées à cause d’une panne d’électricité ou d’une défaillance du système de contrôle de température du data center.
- Confidentialité : respect de la loi Suisse sur la protection des données, hébergement en Suisse.
- ISDS concept à établir.
- Gestion des contrats IT : indispensable pour définir clairement les rôles et responsabilités et gérer les litiges (mises à jour, niveau des versions, certifications…).
- Difficulté : taille des cabinets (PMEs) avec des données très sensibles : regroupement pour partager les coûts d’hébergement & expertises ?

Syrma

3. La cybersécurité commence par la gestion des contrats IT

EXPERTISE CONTRAT IT AU SERVICE
DE **VOTRE** ENTREPRISE

PENDANT QUE VOUS DIRIGEZ VOTRE ENTREPRISE, UNE EQUIPE DEDIEE D'AVOCATS ET D'INGENIEURS IT EST PRESENTE POUR VERIFIER VOS CONTRATS IT (SERVICE, SOLUTION, CLOUD)

900 frs.

NOUS REALISONS
L'EXPERTISE TECHNIQUE
ET LEGALE

REPONSE GARANTIE
SOUS LES 48 HEURES
SOUS LA FORME
D'UN RESUME
STRUCTURE
POUR PRENDRE
LES BONNES DECISIONS

QUINZE COURS DES BASTIONS & SYRMA CONSULTING

S'ALLIENT AUTOUR DE CETTE OFFRE COMMUNE POUR ATTEINDRE VOS AMBITIONS

Quinze Cours des Bastions

Syrma

4. Serious game de gestion des risques cyber & crise

Qui est concerné ?

- Comité de direction
- Médecins, soignants
- Équipe de la DSI (chefs de projet)
- Equipe RSSI et DPO
- Services techniques et logistique

Sensibilisation – Entraînement – Gestion de crise

Comment cela se passe ?

3 intervenants experts (selon le public) :

- Expert Serious Game
- Expert SI hospitalier
- Expert Cybersécurité

- Durée prévisionnelle d'une session :
  - entre 45 minutes à 1h, puis 30 minutes de débriefing.
  - Session soit en présentiel ou distanciel
- Par groupe de 6 à 8 joueurs maximum

Un concept de Doshas propulsé en Suisse par

4. Ils ont déjà joué à MEDIRISK : serious game de gestion des risques cyber & crise

Groupement Hospitalier de Territoire Nord Ouest Vexin Val-d'Oise
- Centre Hospitalier René-Dubos
- Groupe Hospitalier Carnelle Portes de l'Oise
- Groupement Hospitalier Intercommunal du Vexin

Groupe hospitalier Sud Île-de-France

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
Liberté
Égalité
Fraternité

institutCurie

Centre Hospitalier Régional Universitaire de Lille

CHU Saint-Étienne

sesan
SERVICE NUMÉRIQUE DE SANTÉ

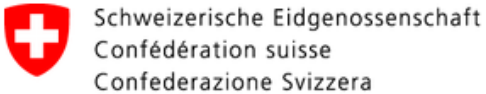
AGENCE DU NUMÉRIQUE EN SANTÉ

MIPIH

doshas consulting

Un concept de Doshas propulsé en Suisse par Syrma

Ils nous ont fait confiance sur des missions santé & IT



Syrma

CLUSIS

www.clusis.com

Syrma

L'Association

- Constituée le 15 mars 1989
- +200 Membres
- Promotion de la sécurité de l'information
- + Évènements en ligne et en présentiel
- Publications d'articles

Les Activités

Par des conférences ciblées et pointues ainsi qu'un site interactif dynamique, le Clusis partage son savoir et son expertise avec les acteurs économiques de la société de l'information.

- Plateforme d'échanges entre experts;
- Conférences;
- Réseau professionnel.

Parce qu'ils sont membres du Clusis, les professionnels de la sécurité de l'information gagnent la confiance de leurs clients et partenaires.

MERCI DE VOTRE ATTENTION !

Syrma Consulting

Aurélie Rosemberg
CEO & Fondatrice
Place de la gare, 12
1006 Lausanne
+78 714 82 78

www.syrma.ch

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

Point de vue actuel de la FMH

- Dr Alexander Zimmer membre du comité central et responsable du département numérisation/e-health

- Dr Reinhold Sojer, département digitalisation/e-health

La sécurité informatique du point de vue de la FMH

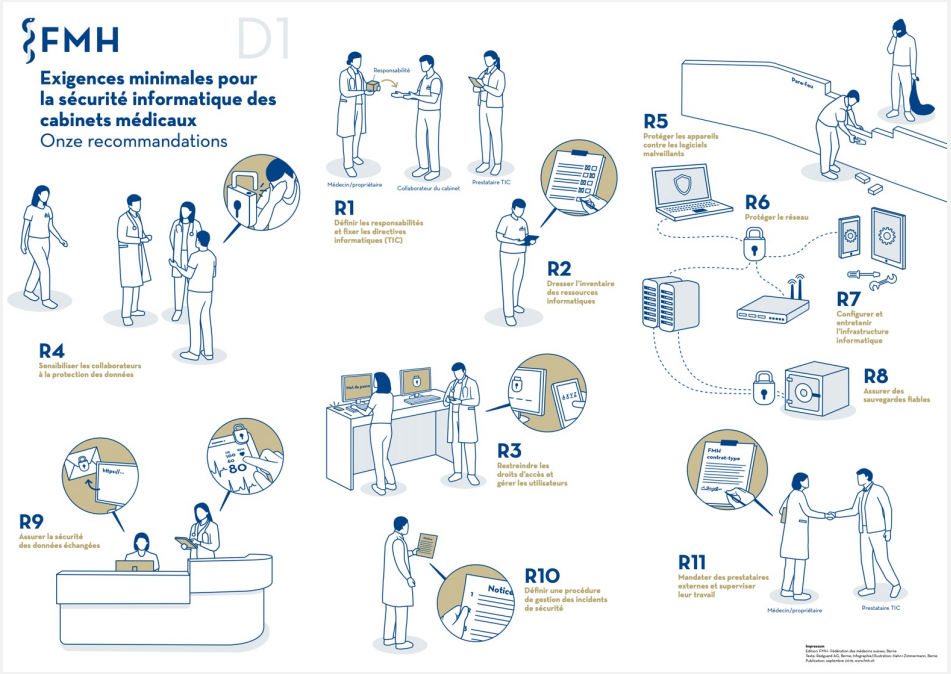
© FMH

Sécurité informatique

Exigences minimales pour la sécurité informatique des cabinets médicaux

[Exigences minimales pour la sécurité informatique des cabinets médicaux]

La FMH a élaboré les exigences minimales pour la sécurité informatique des cabinets médicaux dans le but de soutenir les propriétaires de cabinet et parce qu'aucune recommandation n'existe pour l'instant au niveau fédéral. Ces exigences sont de facto des recommandations assurant un niveau minimum de sécurité pour les données, les informations et les infrastructures informatiques (TIC).



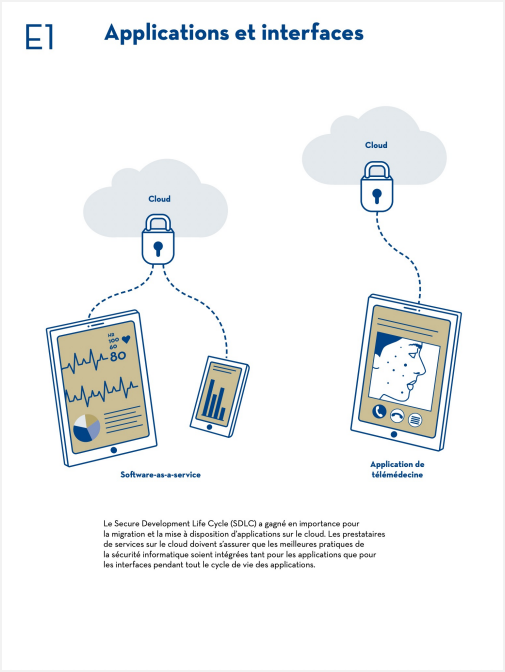
© FMH

Sécurité informatique

[Exigences techniques et organisationnelles pour les services sur le cloud]

Exigences techniques et organisationnelles pour les services sur le cloud

Les exigences techniques et organisationnelles ont été élaborées pour garantir la protection et la sécurité des données lors du traitement de données de patients sur le cloud. Ces exigences visent à réduire les risques associés à l'utilisation de services sur le cloud et à garantir une utilisation sûre de ces services pour les médecins.



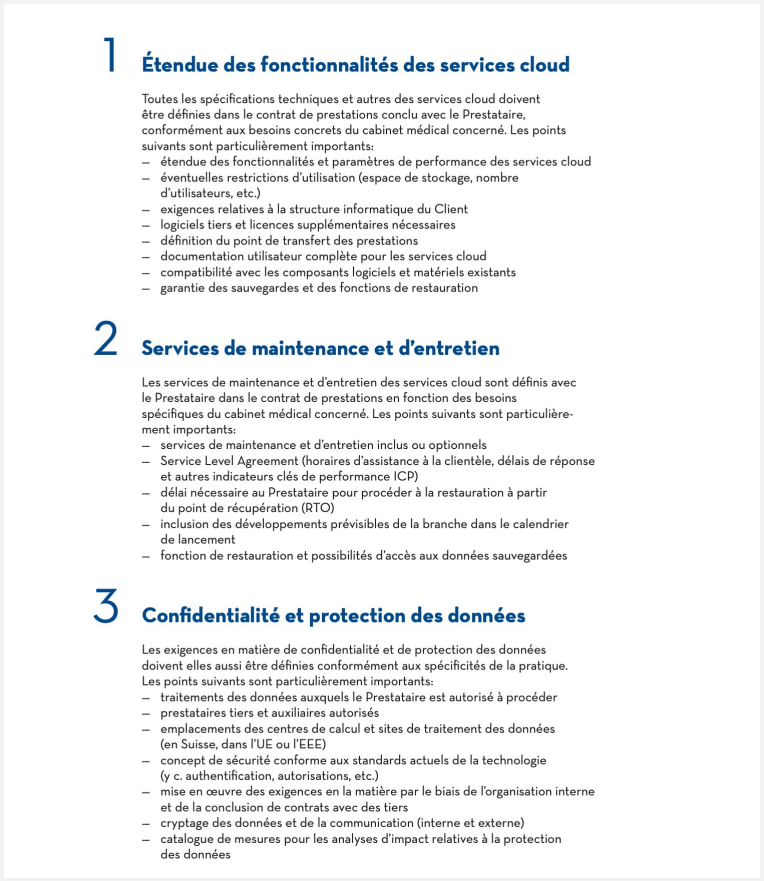
© FMH

Sécurité informatique

Exigences techniques et organisationnelles pour les services sur le cloud

La FMH s'est attelée à la rédaction d'exigences minimales relatives à la conclusion de contrats d'hébergement et de services sur le cloud. Les médecins et les cabinets de groupe qui choisiront de recourir à ce type de services auront avantage à s'appuyer sur ces exigences minimales pour leurs négociations avec les prestataires.

Contrat-cadre de services en nuage (services cloud)



1 Étendue des fonctionnalités des services cloud

Toutes les spécifications techniques et autres des services cloud doivent être définies dans le contrat de prestations conclu avec le Prestataire, conformément aux besoins concrets du cabinet médical concerné. Les points suivants sont particulièrement importants:

- étendue des fonctionnalités et paramètres de performance des services cloud
- éventuelles restrictions d'utilisation (espace de stockage, nombre d'utilisateurs, etc.)
- exigences relatives à la structure informatique du Client
- logiciels tiers et licences supplémentaires nécessaires
- définition du point de transfert des prestations
- documentation utilisateur complète pour les services cloud
- compatibilité avec les composants logiciels et matériels existants
- garantie des sauvegardes et des fonctions de restauration

2 Services de maintenance et d'entretien

Les services de maintenance et d'entretien des services cloud sont définis avec le Prestataire dans le contrat de prestations en fonction des besoins spécifiques du cabinet médical concerné. Les points suivants sont particulièrement importants:

- services de maintenance et d'entretien inclus ou optionnels
- Service Level Agreement (horaires d'assistance à la clientèle, délais de réponse et autres indicateurs clés de performance ICP)
- délai nécessaire au Prestataire pour procéder à la restauration à partir du point de récupération (RTO)
- inclusion des développements prévisibles de la branche dans le calendrier de lancement
- fonction de restauration et possibilités d'accès aux données sauvegardées

3 Confidentialité et protection des données

Les exigences en matière de confidentialité et de protection des données doivent elles aussi être définies conformément aux spécificités de la pratique. Les points suivants sont particulièrement importants:

- traitements des données auxquels le Prestataire est autorisé à procéder
- prestataires tiers et auxiliaires autorisés
- emplacements des centres de calcul et sites de traitement des données (en Suisse, dans l'UE ou l'EEE)
- concept de sécurité conforme aux standards actuels de la technologie (y c. authentification, autorisations, etc.)
- mise en œuvre des exigences en la matière par le biais de l'organisation interne et de la conclusion de contrats avec des tiers
- cryptage des données et de la communication (interne et externe)
- catalogue de mesures pour les analyses d'impact relatives à la protection des données

© FMH

Sécurité informatique

Services en cours de planification

Recommandations pour l'utilisation de Microsoft Office 365 (M365) dans les cabinets médicaux (publication prévue à l'automne 2022)

Documents et aides pour la nouvelle loi sur la protection des données (accords de confidentialité, listes des traitements, etc. publication prévue pour fin 2022)

© FMH

Sécurité informatique

Services en cours de planification

Newsletter Cybersecurity – publication sur ce service dans le Bulletin des médecins suisses en juin 2022

© FMH

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

FMH futur ?

Standards pour audits ?

Contrats avec conseillers ?

Autres ?

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

CONCLUSIONS

- Mutualisation probablement nécessaire à moyen-long terme
- Rôle actif du médecin mandant mais guidance nécessaire
- Conséquences sur nos coûts (**n'oubliez pas de remplir ROKO** !!)
- Problématique qui devra être reprise et rediscutée dans nos différentes sociétés
- Rôle de l'Etat ?
- Autres ?

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

QUESTIONS SALLES / CHAT

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

EVALUATIONS ET ATTESTATION

- https://tinyurl.com/cybersmsr (lien sur la page www.snm.ch)

*Veuillez s.v.p. donner des notes pour chacun des éléments de la colonne de gauche

Notes: **1 = mauvais** et **5 = excellent**

	1	2	3	4	5
Qualité des présentations	○	○	○	○	○
Thèmes choisis	○	○	○	○	○
Qualité du support de cours (guide en ligne)	○	○	○	○	○
Informations utiles en pratique ?	○	○	○	○	○

Commentaires

Envoyer

- Une fois votre évaluation envoyée, vous pourrez télécharger votre attestation

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

REMERCIEMENTS

- M. Dominique Castella, CIGES ainsi que le RHNe pour la salle
- Dr Hervé Zender, modération des questions et organ. apéro !
- Prof Jean-Pierre Hubaux, directeur du labo «data security» à l'EPFL
- Comité SMSR et Comité SNM
- Médecine et Hygiène: site, inscriptions, page web
- Tous les intervenants
- Les participants

SMSR
SOCIÉTÉ MÉDICALE
DE LA SUISSE ROMANDE

FIN

Soirée à revoir sur https://www.smsr.ch/cybersecurite-en-cabinet
(lien à venir dans les prochains jours)

carte 1