SOCIÉTÉ VAUDOISE DE MÉDECINE

21e JOURNÉE SVM

13 OCTOBRE 2022
DÈS 14H00
ÉCOLE HÔTELIÈRE DE LAUSANNE

Laboratoire du futur

Modération:
Annick Chevillot
rédactrice en chef adjointe,
Heidi.news.

Partenaire média

HEIDI.NEWS

Cybersécurité

Relève médicale

Durabilité

UNE CYBERATTAQUE AU CABINET

Dre Marjorie Cosandey Tissot

SVM-13.10.2022

Objectifs de l’atelier

- **Sensibilisation** aux cyberattaques : Cela n’arrive pas qu’aux autres….
- D’une expérience difficile en tirer des apprentissages, **prévenir** de futures attaques, **susciter** une mobilisation collective.
- Vous **rassurer :** s’intéresser à la sécurité informatique, ce n’est **pas « si compliqué »** pour les médecins : Connaître quelques aspects **juridiques**, **bonnes pratiques, relation de confiance** avec son équipe informatique, **contrats** solides.

Avant la cyberattaque

- 10.2021 **Mise en application des recommandations de la FMH** pour la cybersécurité. De la formation de l'équipe (phisching, mots de passe solides, etc..) à la validation par notre IT, point par point des 11 recommandations. Pas moyen de vérifier si notre IT avait bien fait ce qu'il avait dit et écrit.
- **Signature d'une charte** le 14.12.2021 par tous les collègues du cabinet.
- **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). Grâce à la **sauvegarde**, nos IT nous connectent à une version virtuelle dès l'après-midi, on peut consulter notre LP mais pas modifier les dossiers ni ouvrir les pdf.
- 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 des 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 !

Une cyberattaque au cabinet

Gestion de crise-Plan d’action

- **Comprendre**, **anticiper**, **informer** les patients. **Prévenir** les récidives. Importance de bien s’entourer et savoir à qui l’on peut **faire confiance**.
- Payer ou non la **rançon** ?
- 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 **prêtes à répondre aux médias**.

Ce qui nous a aidé

- **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** : soutien pour la communication transparente aux patients.
- **Avocat spécialiste en cybercriminalité** : très aidant et compétent sur 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 matière de sécurité informatique, soit :

- **Architecture** de nos parcs informatiques et les alternatives
- **Visibilité** des attaques

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 qui vise une **prise de décisions partagée** ?
- **Service proactif du fournisseur,** par ex, ne pas attendre pour signaler qu'un appareil représente un danger.

Pistes de réflexions

- 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.
- Augmentation du niveau de sécurité devra passer par une **mutualisation** des prestations pour que les coûts et les prestations des spécialistes deviennent accessibles à nos PMEs.

Questions à nos associations

- Peut-on attendre de nos associations qu'elles fassent un travail de fond **d'analyses comparées des alternatives ?** Ex Serveur au cabinet versus icloud.
- La **cybercriminalité est une réalité**. Oser le parallèle entre surveillance épidémiologique et surveillance de la cybercriminalité des données médicales ? Ex newsletter FMH
- **Mandater des experts par nos associations** : La cybercriminalité va sans cesse évoluer, il faut que l'on soit prêt, informé, réactif et soutenu par des spécialistes. **Plateforme** spécifique cybercriminalité pour les membres ?
-

Take home message

- **Contrats selon les recommandations de la FMH**, et **clause de confidentialité** à soumettre impérativement à vos informaticiens.
- Mot de passe solides, installer un **gestionnaire de mot de passe.**
- **Hygiène numérique, double authentification, sauvegardes et mises à jour professionnalisées.**
- S’assurer que sur votre serveur, votre bureau virtuel il n’y a **rien en clair**, importance du **chiffrement**, ne pas stocker de données sensibles en dehors de votre LP.
- Uniquement des **adresses électroniques sécurisées.**
- Limiter le stockage de données, séparer dossiers en cours des

Briser un tabou

- La Cybercriminalité est une réalité.
- **Pas de honte** à se faire hacker surtout si l'on n'a pas été négligent-e.
- Importance de **témoigner** pour mieux identifier les failles et protéger les données de l'ensemble de nos patients.

Conclusions

- Vivre avec cette nouvelle réalité.
- L’intégrer dans notre formation pré-,post- et continue.
- S’y intéresser plutôt que résister, c’est même intéressant et proche de la démarche médicale.
- Savoir s’entourer pour déléguer les aspects techniques.
- Ne pas se laisser décourager par cette réalité, nous avons **l’un des plus beau métier du monde….**

Merci de votre attention

ASPECTS JURIDIQUES

Le secret médical est expressément rappelé dans différentes lois :

- Art. 40 lit. f LPMéd
- Art. 11 du Code de déontologie FMH ;
- Art. 35 LPD ;
- Art. 398 al. 2 CO ;
- Art. 28 CC.
- Le devoir de diligence.
- CP

Quelques références de la FMH

- https://www.fmh.ch/files/pdf24/exigences-minimales-securite-informatique-cabinets-medicaux-d3.pdf
- https://www.fmh.ch/files/pdf7/instructions-relatives-au-contract-cadre-reglant-la-fourniture-de-services-cloud.pdf
- https://www.fmh.ch/files/doc3/contrat-cadre-de-services-en-nuage-services-cloud-word.docx
- https://www.fmh.ch/files/doc3/contrat-de-sous-traitance-du-traitement-des-donnees-word.docx
- https://www.fmh.ch/files/pdf24/liste-de-controle-pour-le-services-en-nuage-services-cloud.pdf

Guide de la SNM sur la cybersécurité

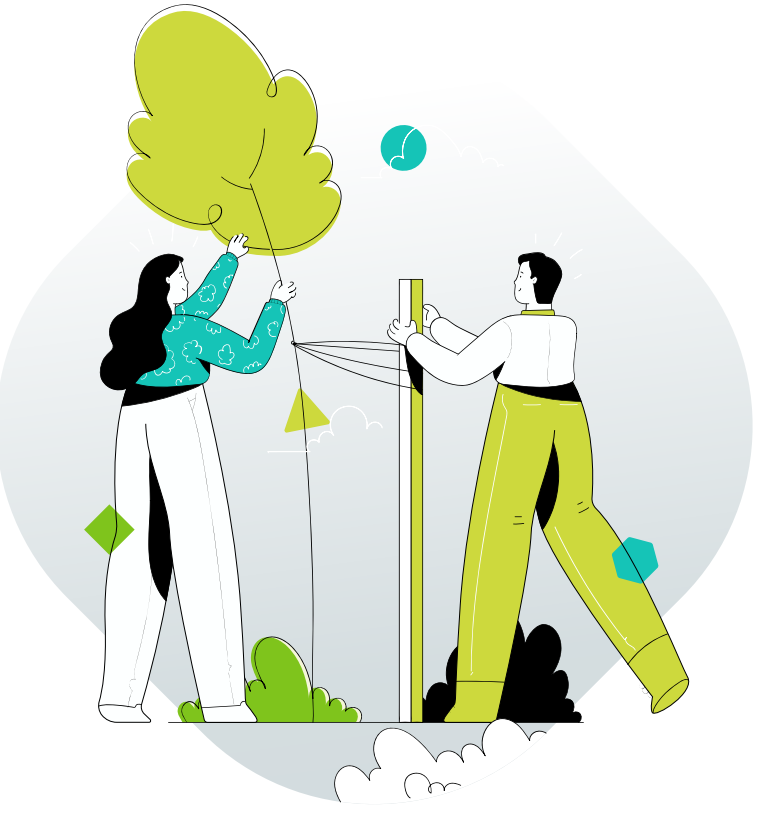
- https://www.snm.ch/guides/cybersecurite/accueil

Cybersécurité au cabinet

SVM

Philippe Oechslin

13.10.2022



Agenda

- Votre responsabilité
- Techniques de hacking
- Petite visite du darknet
- Bonnes pratiques
- Questions: les nôtres
- Questions: les vôtres

Cela n'arrive pas qu'aux médecins

INFORMATIQUE ABONNÉ

Quand une importante société de sécurité informatique à Genève se fait elle-même pirater

Banques privées, services de l'Etat, enquêtes judiciaires: plus de 200 entités romandes ont recouru à un prestataire de services informatiques dont nombre de données confidentielles se sont retrouvées sur le darknet

Le Temps, 27.7.22

Vous n’êtes pas les seuls

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Search

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Zomo Health	TX	Business Associate	1359	09/30/2022	Unauthorized Access/Disclosure	Network Server
	FMC Services, LLC	TX	Healthcare Provider	233948	09/23/2022	Hacking/IT Incident	Network Server
	Anesthesia Associates of Maryland LLC	MD	Healthcare Provider	12403	09/23/2022	Hacking/IT Incident	Network Server
	Cynthia Paul, M.D., LLC d/b/a The Coeur Group	NE	Healthcare Provider	2020	09/23/2022	Hacking/IT Incident	Email
	WellMed Medical Management	TX	Healthcare Provider	10506	09/23/2022	Unauthorized Access/Disclosure	Electronic Medical Record, Network Server
	Seattle Children's Hospital	WA	Healthcare Provider	6750	09/21/2022	Hacking/IT Incident	Network Server
	Bonita Springs Retirement Village, Inc.	FL	Healthcare Provider	554	09/19/2022	Hacking/IT Incident	Email
	Easterseals-Goodwill Northern Rocky Mountain, Inc.	MT	Healthcare Provider	3886	09/16/2022	Hacking/IT Incident	Email
	Tessie Cleveland Community Services Corp	CA	Healthcare Provider	9747	09/16/2022	Hacking/IT Incident	Network Server
	Country Doctor Community Clinic	WA	Healthcare Provider	38751	09/16/2022	Hacking/IT Incident	Network Server
	Landmark Management Services	FL	Healthcare Provider	501	09/15/2022	Hacking/IT Incident	Network Server
	Neurology Center of Nevada	NV	Healthcare Provider	11700	09/15/2022	Hacking/IT Incident	Electronic Medical Record
	Centerstone of Tennessee, Inc.	TN	Healthcare	3675	09/12/2022	Hacking/IT Incident	Email

Registre US des cas où des informations médicales ont été dérobées

Votre responsabilité

La nouvelle loi sur la protection des données (9. 2023)

- Les données sont sensibles et vous en êtes responsables (art 5)
- Ceci inclut la sécurité informatique (art 8)
  - Les responsables du traitement … **doivent assurer**, par des mesures organisationnelles et techniques appropriées, **une sécurité adéquate des données**…
- La responsabilité reste la vôtre même si vous déléguez l'informatique
  - art 9.2: Le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données.
  - Il faut s'assurer par des contrats que la sécurité des données est garantie.

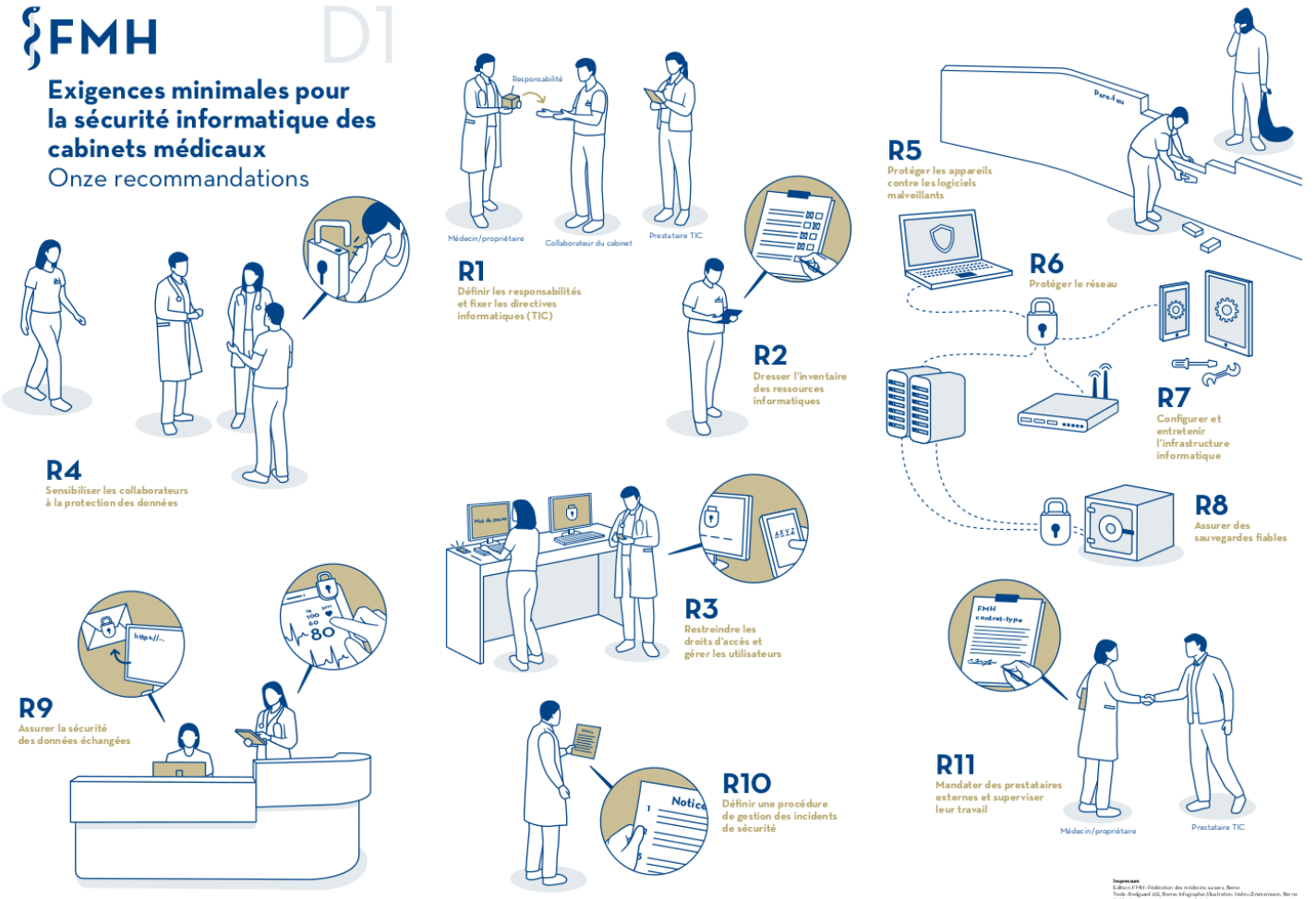
Nouveautés

- Devoir d'annonce (art 24)
  - Le responsable du traitement annonce dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données …
- Les dispositions pénales (art 61)
  - Violation des devoirs de diligence:
    - Sont, sur plainte, punies d'une amende de 250 000 francs au plus les personnes privées qui, intentionnellement:
      - … ne respectent pas les exigences minimales en matière de sécurité des données …

Une sécurité *adéquate* des données

- Le terme 'adéquat' est assez vague
  - L'ordonnance de la loi donne quelques pistes.

- Vous avez de la chance: la FMH a défini une **liste de 11 mesures de sécurité** à mettre en place
  - si vous appliquez ces mesures, on ne peut pas vous reprocher de ne pas avoir une sécurité adéquate



Exigences minimales FMH

Quid des nuages?

- Les données personnelles ne peuvent être traitées que dans des pays avec un niveau de protection compatible
  - p.ex. en Europe, mais pas aux US

- Si la société est us-américaine, le traitement, même en Suisse, est problématique
  - Les autorités us-américaines peuvent exiger l'accès aux données
  - Le PFPDT a critiqué la SUVA qui voulait utiliser Office 365, hérbergé en Suisse
  - Les américains sont en train d'adapter la loi pour devenir compatibles
    - ➡ affaire à suivre

- La FMH a préparé un contrat cadre et des instructions pour l'utilisation du cloud

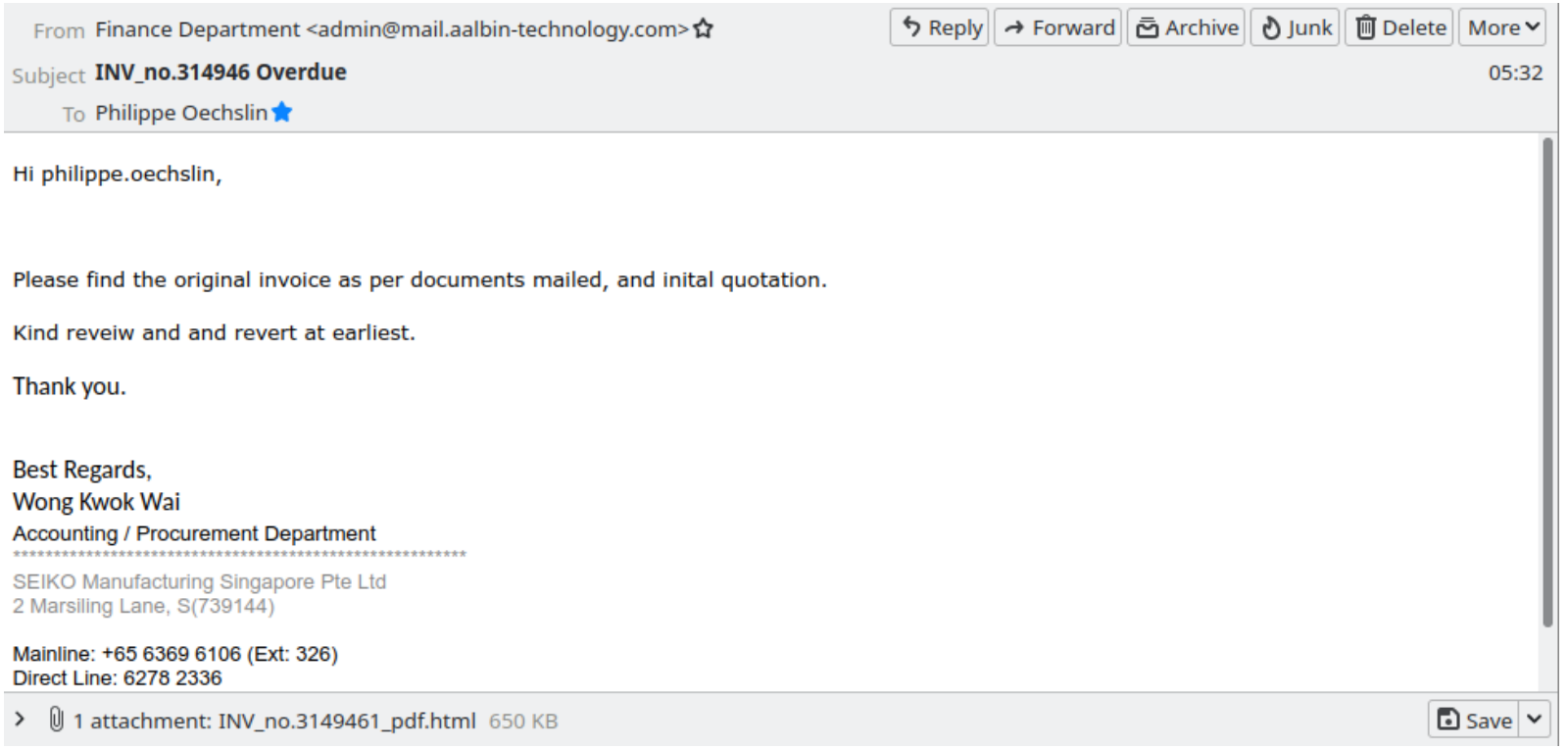
www.fmh.ch/fr/themes/ehealth/informatique-cabinet-medical.cfm

Techniques de hacking

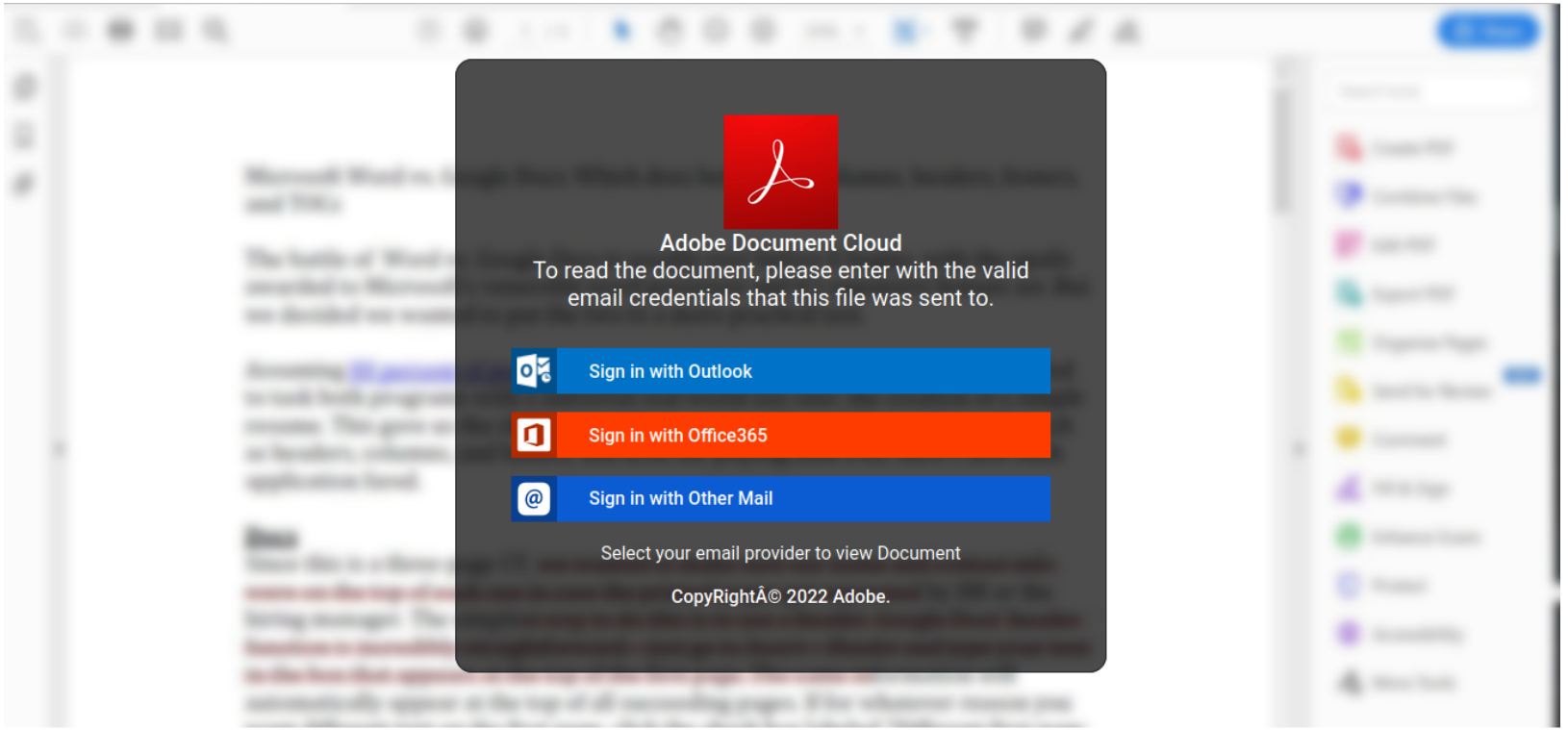
Comment font-ils?

Phishing

- On peut obtenir un mot de passe en demandant poliment



Phishing


Adobe Document Cloud
To read the document, please enter with the valid email credentials that this file was sent to.
Sign in with Outlook
Sign in with Office365
Sign in with Other Mail
Select your email provider to view Document
CopyRightÂ© 2022 Adobe.

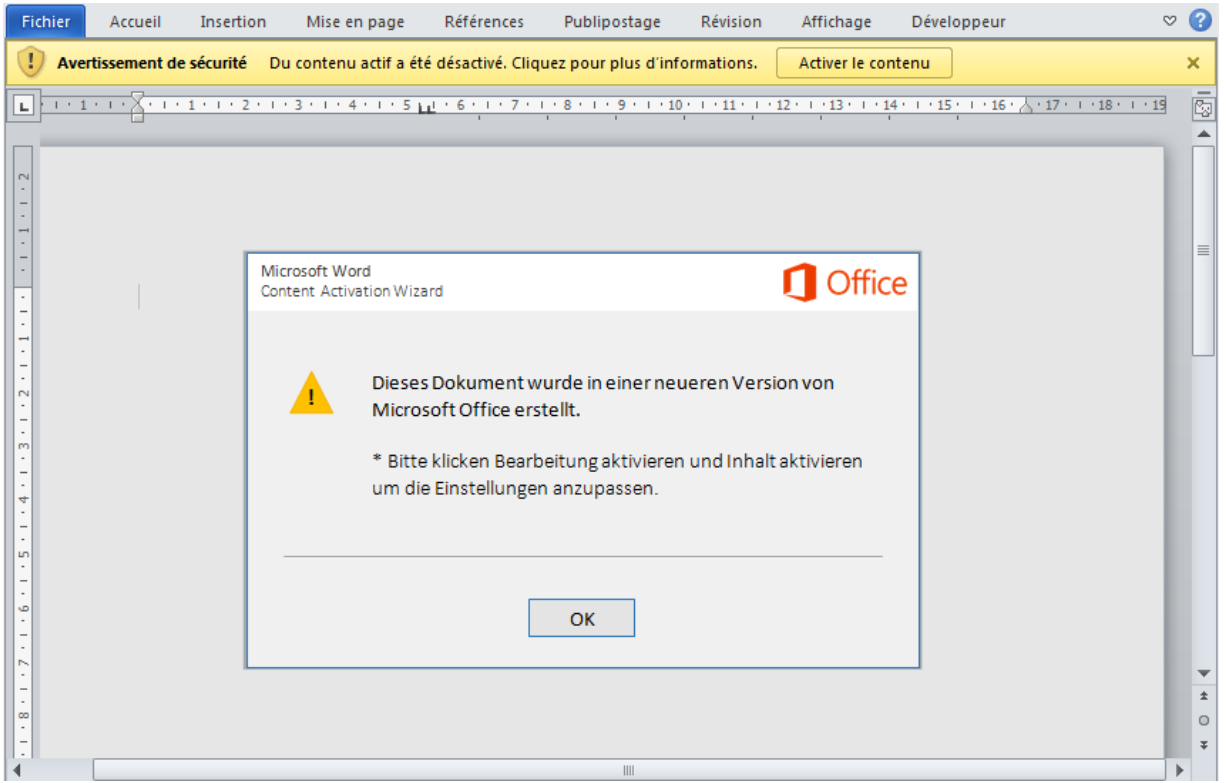
Failles de sécurité

- Logiciels
  - Les logiciels que vous utilisez peuvent contenir des failles qui permettent aux pirates de s'introduire dans votre ordinateur (navigateur, office, ...)
  - ➡ Mettre à jour les logiciels
- Equippements
  - Les équipements réseau peuvent aussi avoir des failles!
  - ex. routeur, pare-feux (*firewall*), WiFi
  - ➡ Mettre à jour le logiciel des équipements

  - 2021: Failles sur le pare-feu Fortinet
  - 2020: Failles sur accès à distance par Citrix

Malware

Ce document a coûté 30’000.-

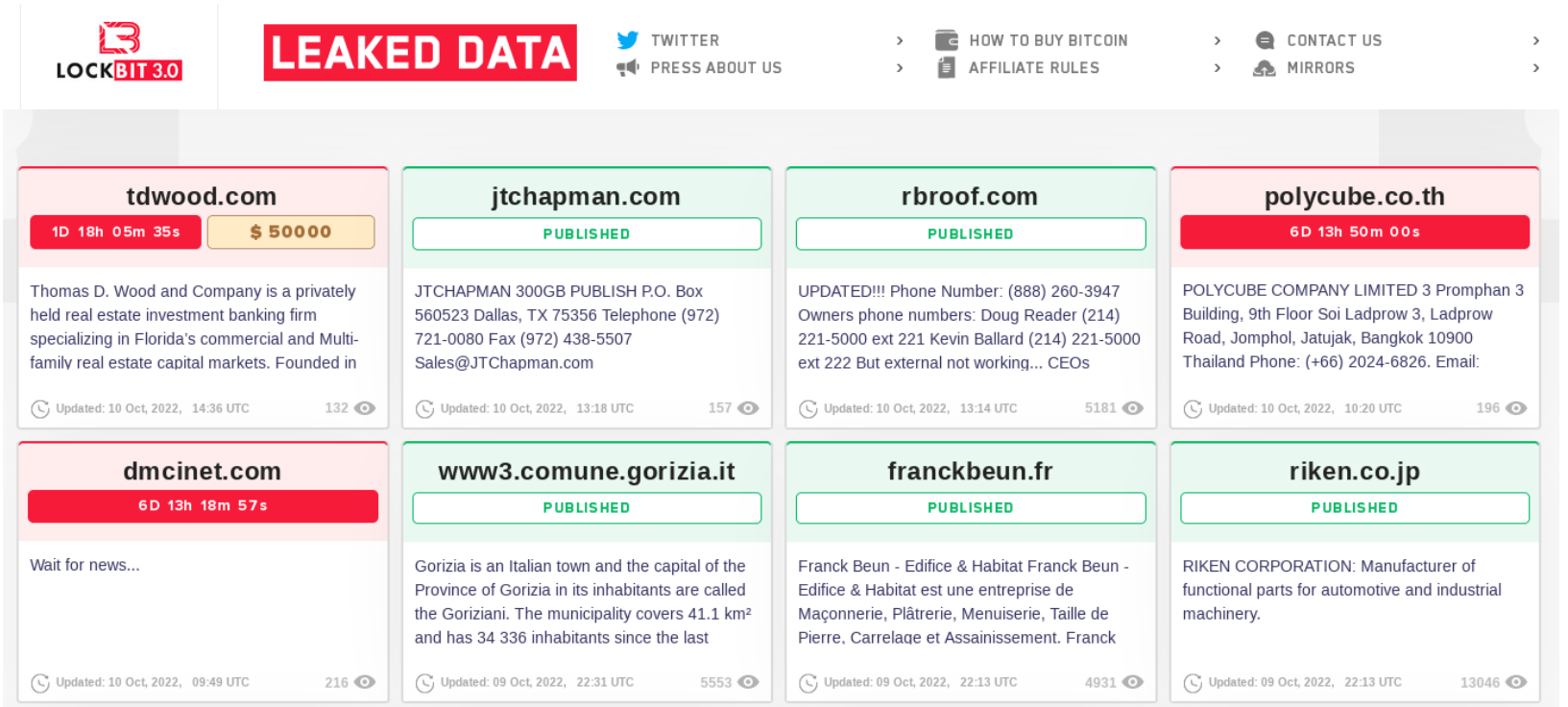


Les virus très récents ne sont pas reconnus par les anti-virus

Démo cheval de troie

Petite visite du darknet

Les sites des ransomware (rançongiciels)



Lockbit

Bonnes pratiques

Chiffrement

- Si les données sont chiffrées, on ne peut pas y accéder sans connaître la clé/le mot de passe

- Exemples de données chiffrées:
  - Votre logiciel métier chiffre les données médicales (probablement)
    - Vous devez taper un mot de passe à son lancement
    - Si ces données sont publiées, et si vous avez un bon mot de passe, les données ne pourront pas être lues

  - On peut chiffrer un document Word ou Excel en le protégeant par un mot de passe
    - si le mot de passe est bon, le pirate ne pourra pas lire le document

  - Votre messagerie HIN chiffre les documents avant de les transmettre
    - il gère automatiquement les clés de chiffrement

Données en clair

- Exemples de données médicales en clair
  - Petites quantités
    - Correspondance/notes rédigées à l'extérieur de votre logiciel métier
    - Fichiers PDF téléchargés ou reçus en attachement
  - Grandes quantités
    - export des données de votre logiciel métier,
      p.ex. lors d'un changement de version, de système ou de praticien
- Ne gardez pas de données en clair dont vous n'avez plus besoin.

Mots de passe

- Quel est le meilleur mot de passe?
  - **Maison2+** ou **mai+2son**
  - **CristianoRonaldo2020** ou **MionelLessi4**
  - Les pirates connaissent nos habitudes
- Un bon mot de passe est **long** et **original**
- Il faut des mots de passes **différents** pour tous les comptes importants
  - Les pirates vont utiliser un mdp volé sur un site pour accéder à d'autres sites
- Utilisez un **gestionnaire de mots de passe**!
  - ➡ démo
- Un bon mot de passe ne vous protège pas forcément contre le phishing
  - Utilisez un **deuxième facteur** pour les comptes sensibles

Questions: les nôtres

Question à vous poser

- Savez-vous quelles données médicales sont stockées en clair dans vos systèmes ?
  - logiciel métier
  - correspondance
  - autres
- Avez-vous des accès à distance à des données médicales sans deuxième facteur ?
- Avez-vous des mots de passe identiques pour le professionnel et pour le privé ?
- Votre prestataire informatique est-il au courant des recommandations de la FMH ?

Questions: les vôtres