Cyberrisques, couvertures, services et sinistres

Valéry-Philippe WEGMANN, Senior Underwriter AXA

Webinaire AAC, 6. mars 2024

Ordre du jour

60 min.

1. Cyberrisques	Pourquoi toutes les entreprises sont-elles concernées? Pourquoi tout gestionnaire de fortune externe peut-il être concerné? Enquêtes, statistiques
2. Quelles sont les couvertures d'assurance possibles?	
3. Services	
4. Dommages	Exemples de sinistre
5. Questions et discussion	


1
Cyberrisques

1.1 Pourquoi toutes les entreprises sont-elles concernées?

Objectif de l’entreprise: sécurité de l’information

La cybersécurité s’entend comme une gestion des risques à l’échelle de l’entreprise.
En théorie, chaque problème majeur de sécurité informatique est résolu, et c’est quand même un désastre!

Propriété intellectuelle
Avantage concurrentiel

Protection des données et confiance des clients

Sécurité juridique
Responsabilité de la direction

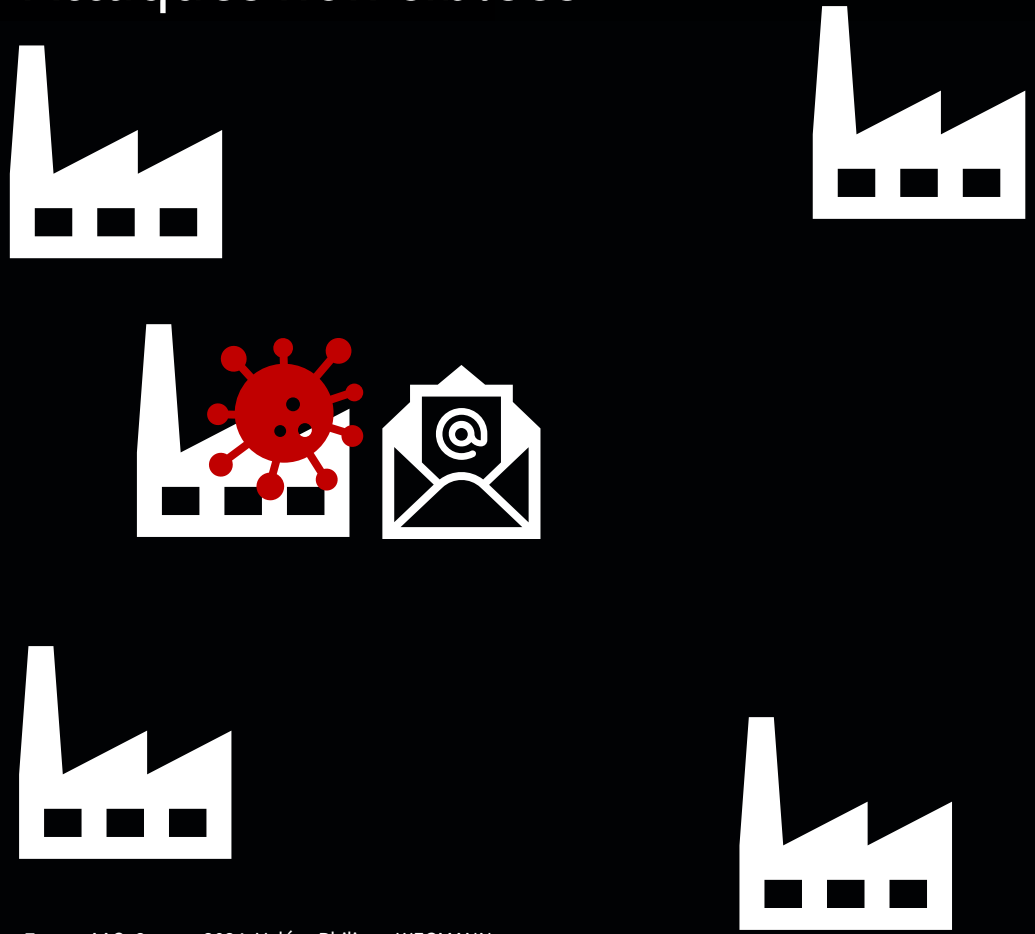
Prévention des dommages
Réduction des coûts

Capacité de livraison
Disponibilité des marchandises

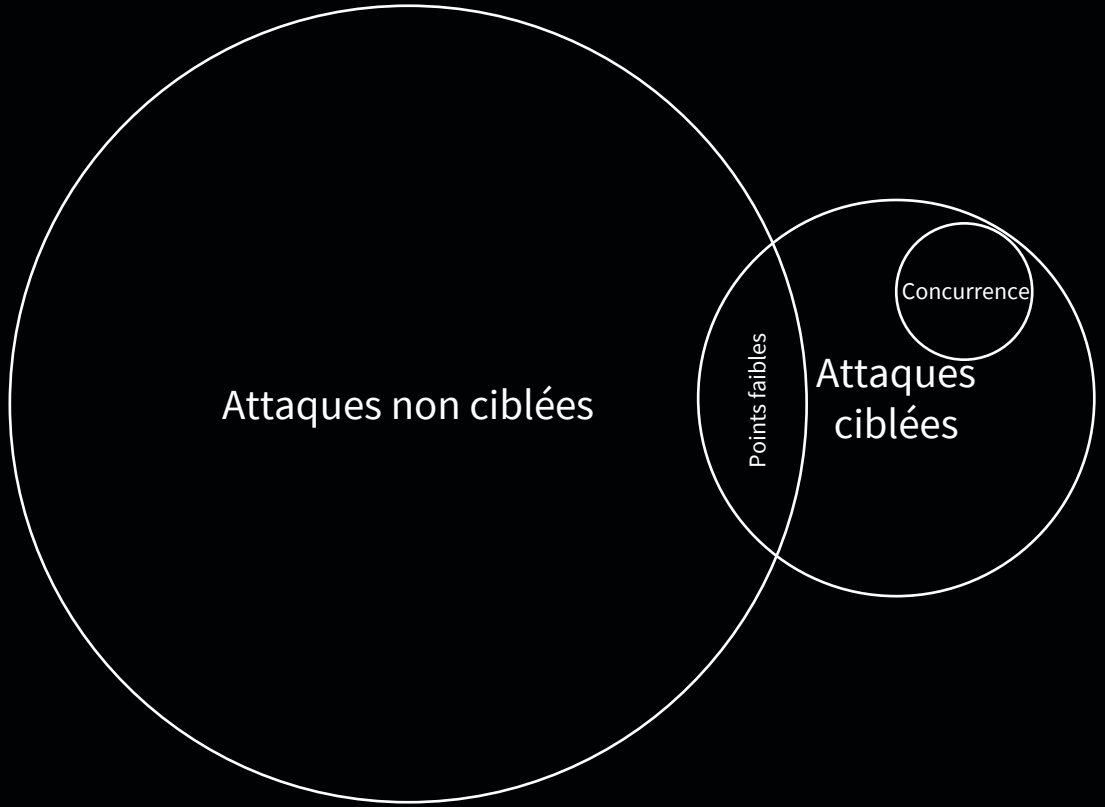
Fixation
Objectifs de risque

Attaques ciblées

Attaques non ciblées



Attaques non ciblées



Facteur humain

Recommandations du BACS (anciennement NCSC)

du 29 janvier 2024 (rapport anti-phishing 2023, partiellement raccourci)

- Signalez **à BACS** les e-mails ou sites Internet suspects sur antiphishing.ch.
- **Soyez sceptique:** aucune banque ni aucun institut de carte de crédit ne vous demandera par e-mail ou SMS de modifier votre mot de passe ou de vérifier vos données de carte de crédit.
- **Authentification multifactorielle (MFA):** si possible, activez l'authentification multifactorielle (MFA) sur vos comptes en ligne tels que les e-mails ou les réseaux sociaux.
- **Utilisation multiple de mots de passe:** n'utilisez jamais le même mot de passe pour plusieurs comptes en ligne. Utilisez un gestionnaire de mots de passe pour gérer vos données d'accès.
- Décompte de **carte de crédit:** vérifiez régulièrement vos décomptes de carte de crédit afin de déceler toute anomalie, et contactez immédiatement l'organisme émetteur de votre carte de crédit en cas de transaction inconnue.
- **Utilisation des favoris:** utilisez la fonction favoris («Bookmarks») de votre navigateur Web pour accéder régulièrement à des comptes en ligne tels que l'e-banking, les médias sociaux ou les e-mails.
- **Spoofing:** gardez à l'esprit que les expéditeurs d'e-mails et de SMS, mais aussi les numéros d'appel des appels entrants, sont faciles à falsifier. En cas de doute, exigez de pouvoir rappeler l'appelant.

1.2 Pourquoi tout gestionnaire de fortune externe peut-il être concerné?

Gestionnaires de fortune externes et cybersécurité

- Informatique et cybersécurité
  - → est jugé par la grande majorité des gestionnaires de fortune externes en Suisse comme très important et nécessitant une intervention dans un délai de 12 mois à trois ans.
  - → est confiée le plus souvent à des prestataires externes (env. 60%)
    - – Statu quo de la digitalisation et de l'organisation interne des gestionnaires de fortune externes, étude de Tatiana Agnesens, Lucerne, janvier 2024
- Cybercriminalité et gestion de fortune
  - → Les gérants de fortune externes ont souvent un accès direct à la fortune des clients. Des criminels tentent d'en profiter
  - → Il suffit d'un mauvais clic pour installer un logiciel malveillant permettant d'accéder à l'e-banking.
  - → Des criminels se font passer pour des membres du Directoire et poussent un collaborateur à effectuer un paiement ou un ordre qui ne sont pas justifiés commercialement (fraude au CEO).
  - → Les collaborateurs et collaboratrices ne sont pas suffisamment formés à la détection du phishing (contenus Internet falsifiés).
    - – Article de la newsletter AAC d'Andreas Corradini (AXA), décembre 2022

Le gestionnaire de fortune externe dans la presse

- «Un gestionnaire de fortune suisse connu a été piraté – des données ont été divulguées dans le darknet» (titre du 7 février 2023 chez Watson)
  - → Des criminels ont pu s'introduire dans les serveurs de Finaport SA et voler de grosses quantités de données. On parle de 1,2 téraoctet.
  - → Entreprise a confirmé que les données volées des serveurs ont été publiées sur le Darknet
  - → Finaport a informé les autorités dans les 24 heures
  - → Toutes les données concernées ont fait l'objet de sauvegardes.
  - → Les attaques continueront. La quantité, la qualité et la complexité augmentent.
  - → L'obligation de déclaration des personnes soumises à la surveillance vis-à-vis de la FINMA est un outil important pour la détection des cyberincidents.
  - → Selon la presse, Finaport ne s'en est pas tiré indemne. Aucune autre information n'a été publiée.


1.3 Enquêtes, statistiques

Étude Cyber d'AXA et statistiques policières sur la criminalité

15% des entreprises ont été victimes d'une attaque en 2021.

14% des petites PME

29% des grandes PME

Chaque

10.

L'entreprise a été victime d'attaques répétées

33'345

Infractions dans le domaine de la cybercriminalité en 2022

+10%

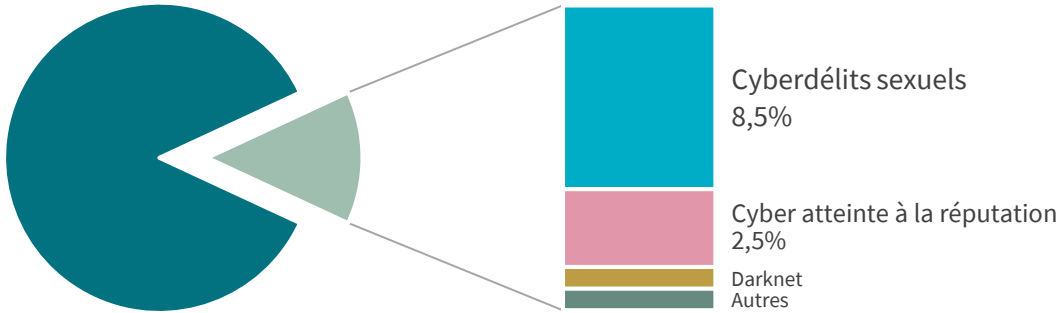
Augmentation de 2021 à 2022

Sources: étude d'AXA Suisse, août 2022, statistiques policières de la criminalité 2022, 2023

Cybercriminalité (criminalité numérique)

En 2022, 33 345 infractions à composante numérique ont été enregistrées.
(+ 10% par rapport à 2021) – le taux d'élucidation est de 34,3%.

Domaines de la criminalité numérique



Cybercriminalité économique: 89,0%, soit 29 677 infractions (p. ex. utilisation abusive de systèmes de paiement, fraude au CEO, fraude numérique)

Source: Statistique policière de la criminalité, rapport annuel 2022, Neuchâtel 2023

Cybercriminalité (criminalité numérique)

Quelles ont été les infractions les plus fréquentes de la cybercriminalité économique en 2022?

- Phishing: 2236
- Piratage: intrusion violente dans un système informatique 246
- Piratage: intrusion dans un système informatique avec des données d'accès tierces 796
- Maliciel et rançongiciel 307
- Malware – e-banking Troie 49
- Maliciels et logiciels espions 15
- Maliciels – Rogueware/Scareware 45

Source: Statistique policière de la criminalité, rapport annuel 2022, Neuchâtel 2023

«Le risque existe, mais cela ne concerne pas mon entreprise»

Une fausse croyance dangereuse

Parmi les personnes interrogées qui ne présentent qu'un faible risque pour leur propre
Voir les entreprises, dire…

60%
Mon entreprise est trop petite

81%
Nos systèmes informatiques bénéficient d'une protection complète

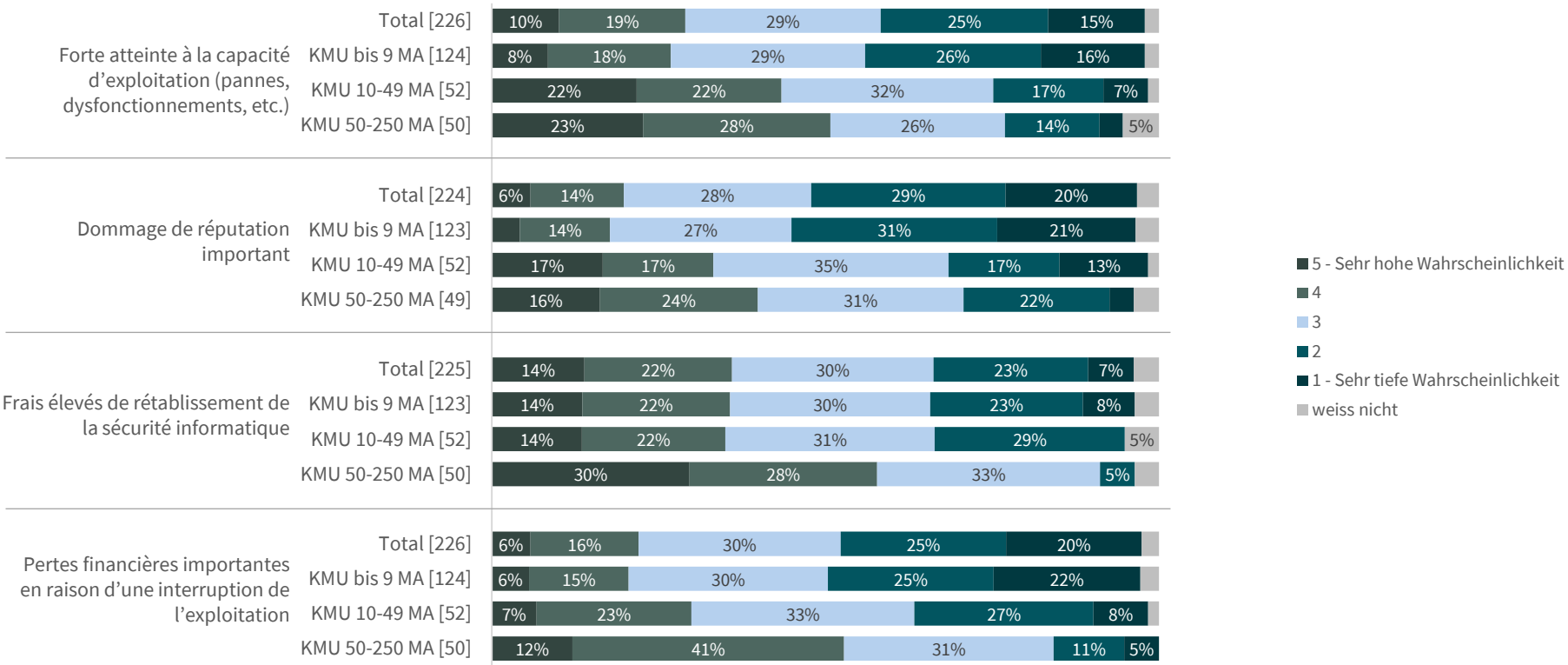
58%
Nous n'avons encore jamais été victimes d'une cyberattaque

70% de
nos données ne sont pas intéressantes

Source: Cybersecurity for SMES, Challenges and Recommendations, ENISA, juin 2021

Étude Cyber d'AXA

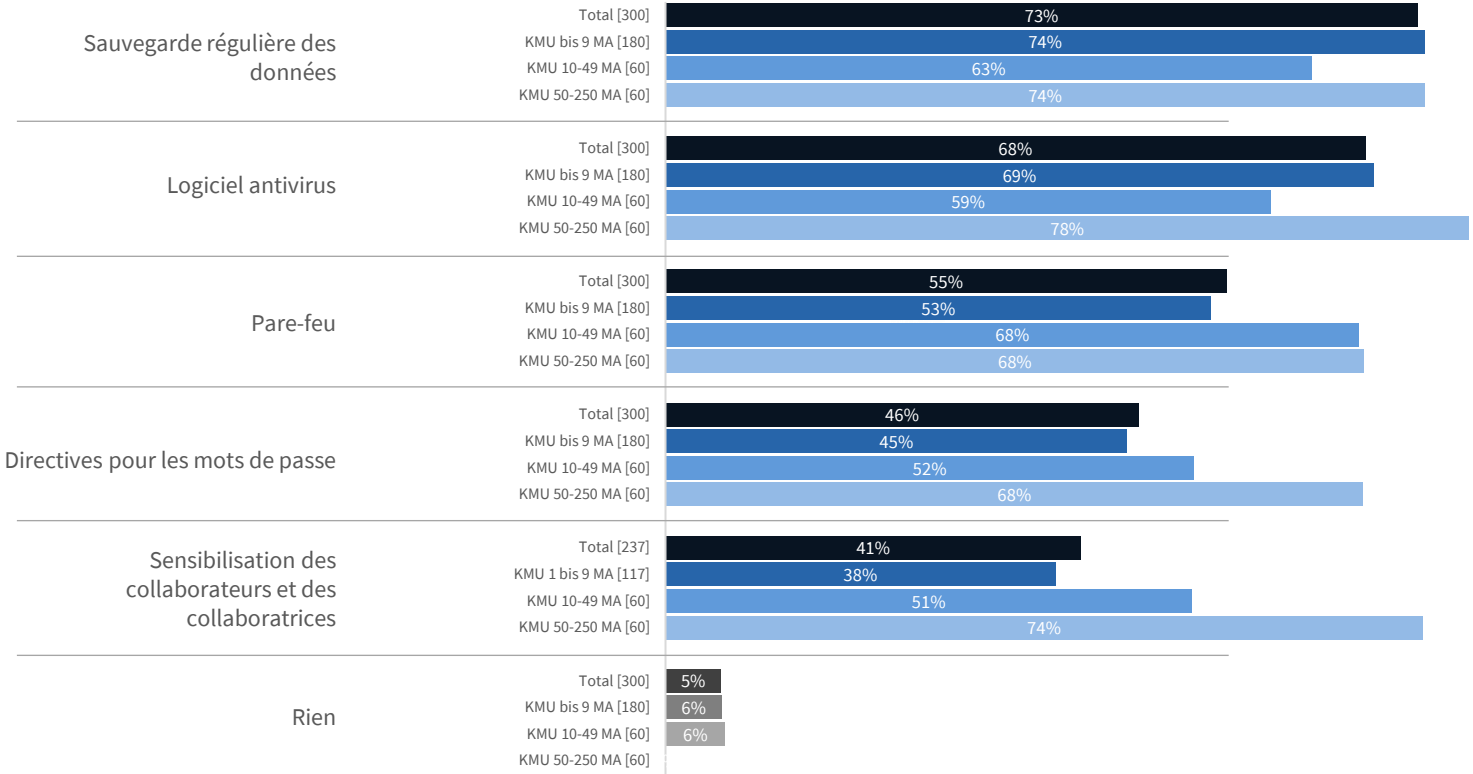
Quelles sont les conséquences probables?



Source: étude d'AXA Suisse, août 2022

Étude Cyber d'AXA

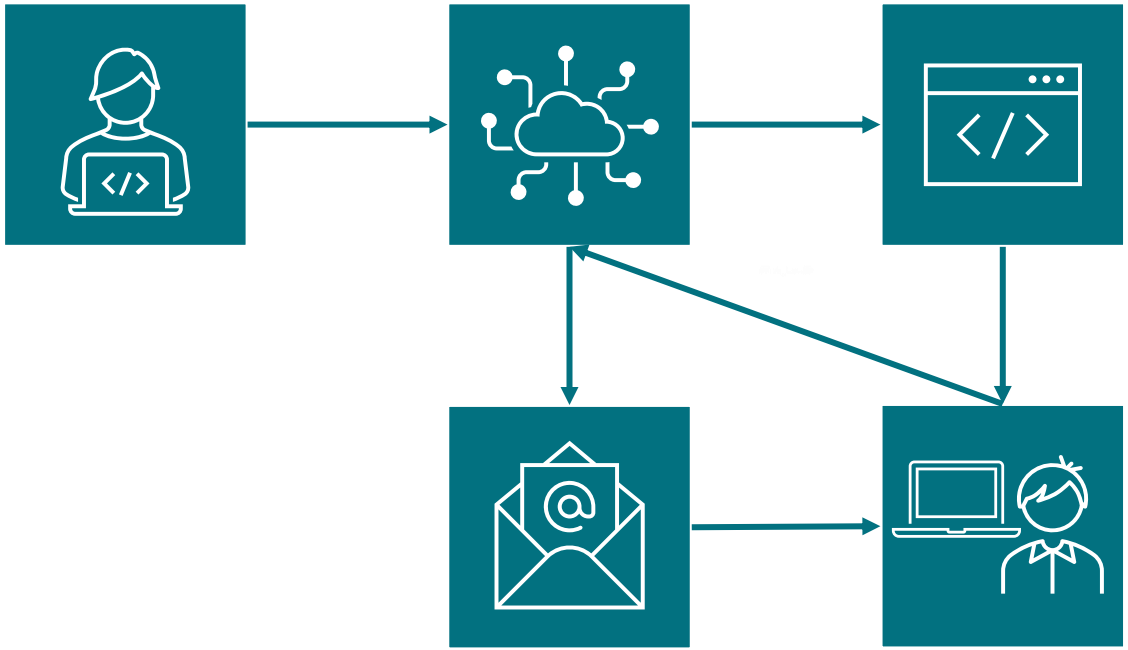
Mesures prises par les entreprises



Source: étude d'AXA Suisse, août 2022


2
Quelles
sont les couvertures
d’assurance possibles?

Principes généraux – Cyberévénement

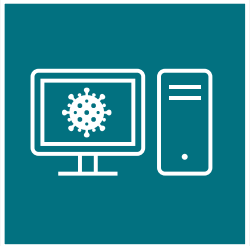
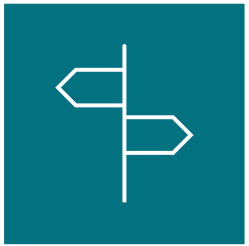


«… un acte intentionnel, une attaque dommageable…»

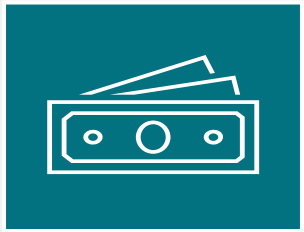
«…au *système informatique* du *preneur d'assurance* ou aux *systèmes de cloud computing*…»

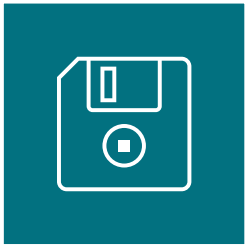
E2-E4 CGA

Bases – Couvertures

Cyberévénement causant un dommage	Cyberévénement engageant la	Gestion de crise	Couvertures complémentaires
			   
• Frais de reconstitution • Pertes d'exploitation • Violation de la protection des données	• Indemnisation des prétentions justifiées • Défense contre les prétentions injustifiées	• Mesures d'urgence • Conseil en cas de crise • Communication de crise	En ligne Services bancaires Piratage télépho nique Ingénierie sociale Demande de rançon
CGA B1	B2 CGA	B3 CGA	B4 à B6 CGA

Bases – Couvertures complémentaires

Manipulation E – banque, boutique en ligne ou envoi de marchandises	Piratage téléphonique	Ingénierie sociale	Demande de rançon
			
• Paiements non autorisés de l'e-banking • Vol de fonds de tiers • Manipulation lors de la livraison de marchandises • Pour les dom. pr. et la RC	• Utilisation de l'installation téléphonique par des tiers après un cyberévénement causant un dommage propre	• Escroquerie • Prise de contact personnelle par l'escroc • Exploitation de la bonne foi, etc.	• Y c. Frais de négociation
B4 CGA	B5 CGA	B6 CGA	CGA C1.12



Sauvegarde

- min. Tous les 7 jours (hors ligne)
- Test de reprise recommandé (non exigé par les CGA)

Systèmes de sécurité

- Antivirus
- Pare-feu, etc.

Mises à jour

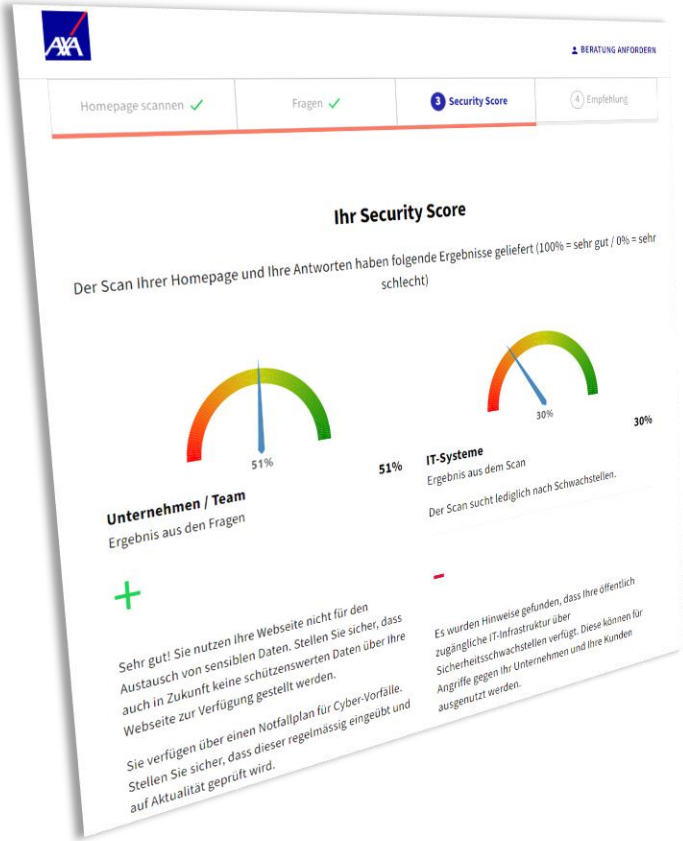
- Systèmes d'exploitation, de sécurité et autres
- Rapidement

*«…qu'*il s'agisse de les mesures destinées à protéger les *données* assurées contre les risques assurés….»

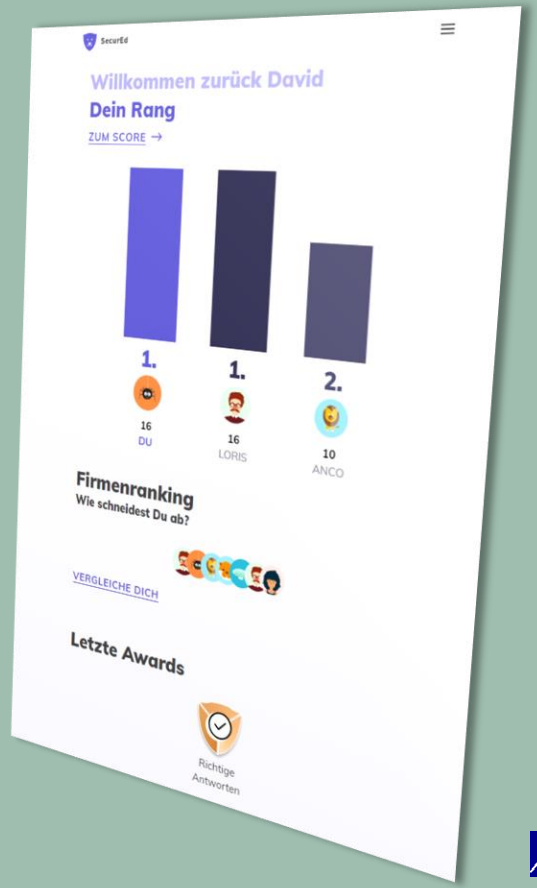
CGA A11


3
Services

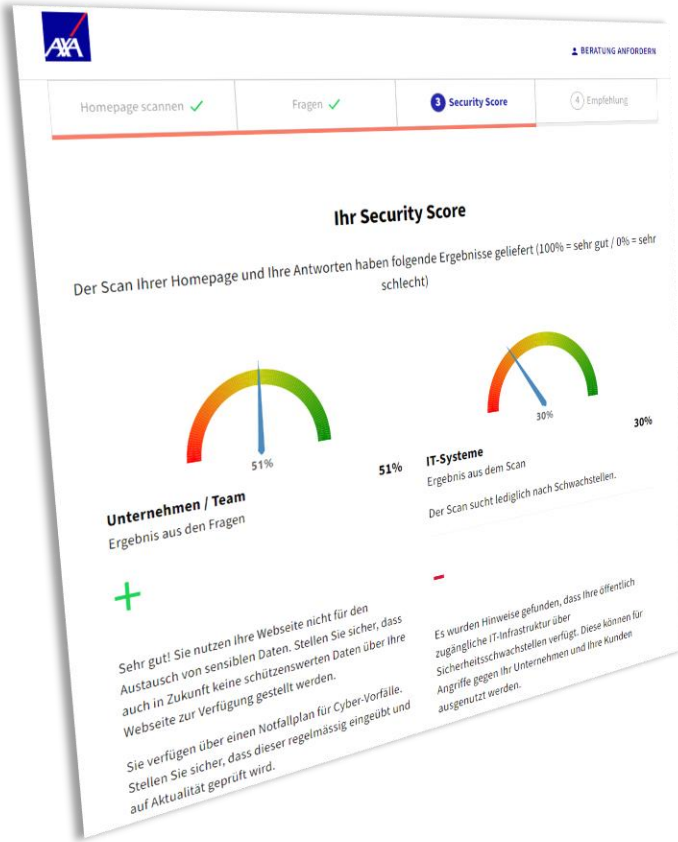
Cyber-Check et protection



Service de cyberprévention



Cyber-Check et protection



cyber-check.axa.ch

- ✓ Bref test d'autotest pour les PME sur le thème de la cyberassurance
- ✓ Sensibilisation
- ✓ Scan de la page d'accueil au moyen d'un test de vulnérabilité

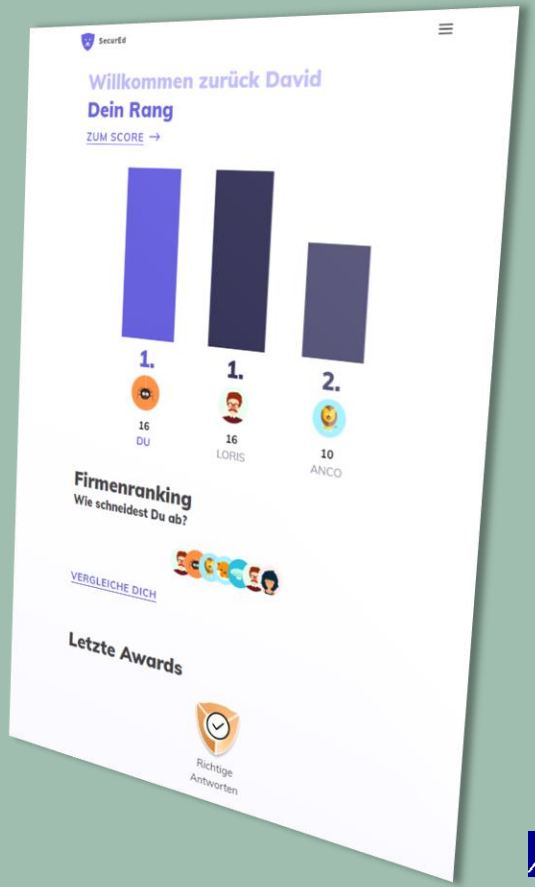
- ✓ **Le client peut également établir des offres.**

Service de cyberprévention

www.scrd.ch

- ✓ Plate-forme de formation pour les collaborateurs
- ✓ La ludification pour plus de motivation
- ✓ Blog Cyber présentant les dernières failles de sécurité
- ✓ Vulnerability Scan – Vue de l'extérieur de l'infrastructure informatique

- ✓ **Gratuit pour tous les clients Cyber d'AXA**
- ✓ Inscription sous www.axa.ch/cps




4
Dommages

Les trois lignes de défense

L’assurance Cyber est la 3e ligne de défense

Mesures techniques

- Protection contre les virus
- Pare-feu
- Backup (y c. tests)
- Scanner des failles
- Tests de pénétration

Mesures organisationnelles

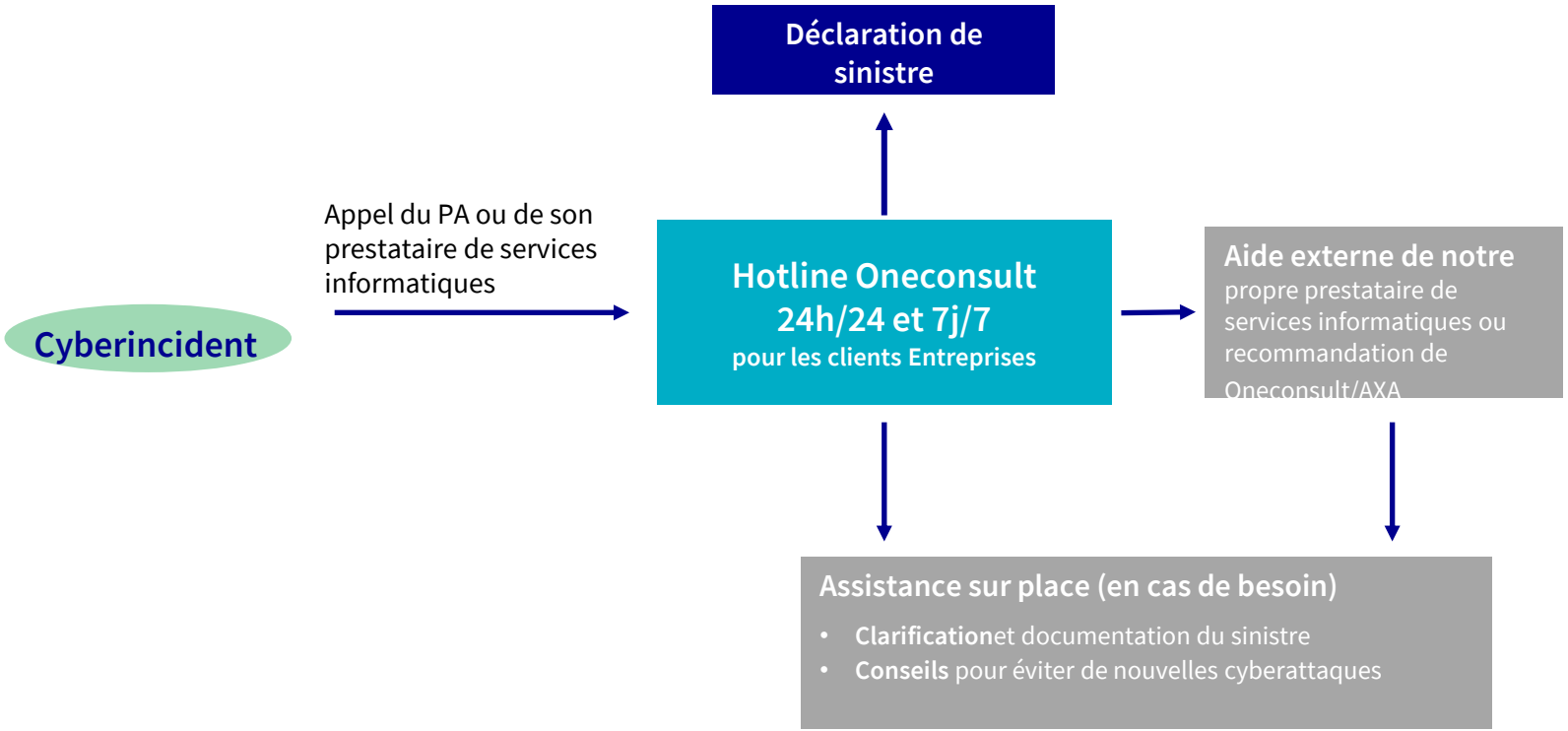
- Plan d’urgence avec désignation des responsables
- Exercices de crise
- Business Impact Analysis
- Formations pour les collaborateurs
- Évaluation des risques

Assurance Cyber

- Aide immédiate 24h/24 et 7j/7 et gestion des sinistres
- Transfert de risques
- Soutien du Risk Management
- Partenaire en matière de prévention
- Gestion de crise avec un réseau d’experts

Processus de déclaration de sinistre

Procédure en cas de sinistre chez les clients Entreprises



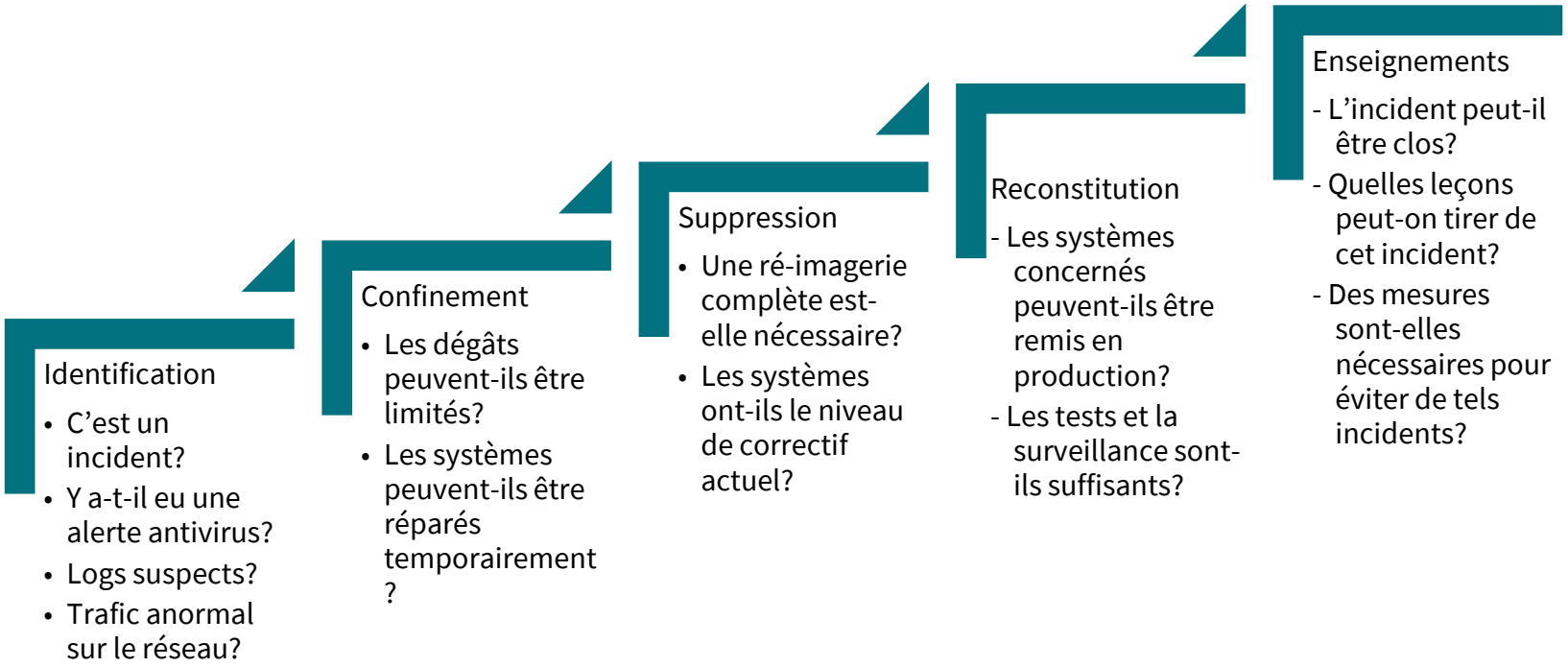
Assistance immédiate en cas de sinistre Cyber

par Oneconsult SA

- Appréciation de l'expert sur la situation décrite
- Recommandation de mesures immédiates pour limiter le dommage
- Recommandation de mesures immédiates pour déterminer la cause
- Première évaluation des mesures mises en place

- Les frais relatifs à l'aide immédiate ne sont soumis à aucune franchise et ne sont pas déduits de la somme d'assurance.
- Cela vaut également s'il s'avère qu'il ne s'agit pas d'un sinistre couvert.
- L'aide immédiate est limitée à CHF 5000. Ce laps de temps devrait permettre à Oneconsult d'évaluer s'il s'agit d'un événement assuré.

Phases de l’Incident Response



Exemple de sinistre Müller et Meier

Introduction à l’exemple de sinistre Müller & Meier

Müller et Meier
Gestion de fortune

- Gestionnaire de fortune externe
- 5 collaborateurs avec poste de travail
- 780 000 CHF de chiffre d’affaires
- La couverture de base de l’assurance Cyber vient d’être conclue.

Exemple de sinistre Müller et Meier

Phase 1 BEC (Business Email Compromise)

Von: Nicole [redacted]
Gesendet: Dienstag, 31. Mai 2022 09:26
An: Gaetano [redacted]
Cc: Buchhaltung [redacted]
Betreff: Aw: Guten Morgen, fällige Rechnung

Hallo Gaetano,

Kannst du heute eine internationale Bankueberweisung machen? Sag mir bescheid, dann kann ich dir die Bankdaten und die Rechnung senden.

Mit Freundliche Grüße

Nicole [redacted]
Geschäftsführerin
[redacted]

Hallo Nicole

Ja, kann ich. Schick mir die Rechnung und Bankkoordinaten

Freundliche Grüsse

Gaetano [redacted]

Buchhaltung / Personal

[redacted]

Von: Nicole [redacted]
Gesendet: Donnerstag, 2. Juni 2022 08:18
An: Buchhaltung [redacted]
Betreff: Re: AW: AW: Guten Morgen, fällige Rechnung

Hallo Gaetano,

Senden Sie mir eine Zahlungsbestätigung.

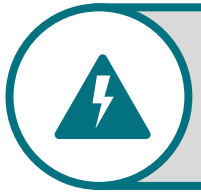
Mit Freundliche Grüße

Nicole [redacted]
Geschäftsführerin
[redacted]

Exemple de sinistre Müller et Meier

Phase 1 BEC

- Un e-mail falsifié a contraint la comptabilité à effectuer un paiement international.



- Versement de 25 000 euros à l'auteur
- De plus, un logiciel malveillant a été installé puis activé.

- La couverture pour les erreurs de paiement a été refusée, car l'ingénierie sociale n'a pas été conclue.

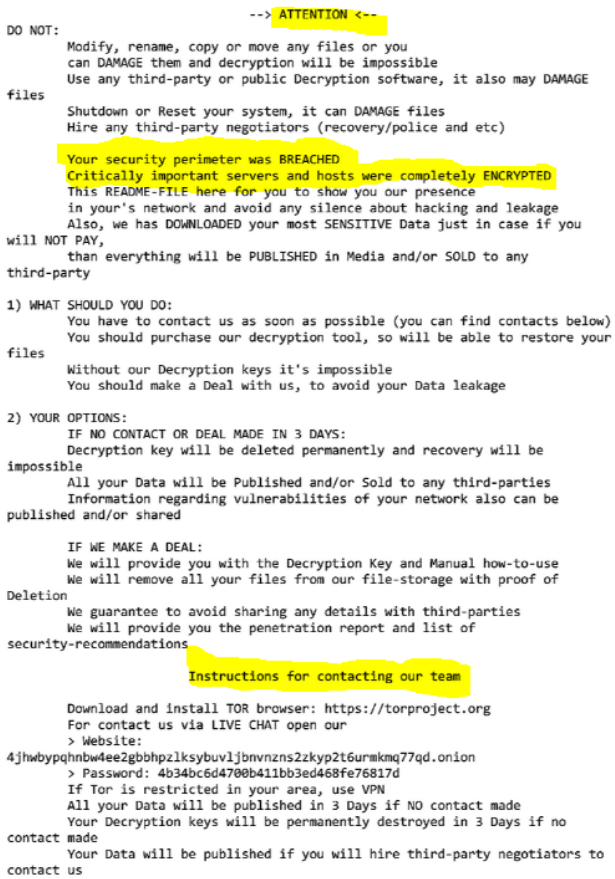
Exemple de sinistre Müller et Meier

Phase 2 rançongiciel

Le lundi matin, lorsque Monsieur Tobler de Müller et Meier veut le premier allumer son ordinateur, le message suivant s'affiche à l'écran:

Exemple de sinistre Müller & Meier

Phase 2 Ransomware

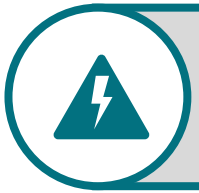


```
                    --> ATTENTION <--
DO NOT:
        Modify, rename, copy or move any files or you
        can DAMAGE them and decryption will be impossible
        Use any third-party or public Decryption software, it also may DAMAGE
files
        Shutdown or Reset your system, it can DAMAGE files
        Hire any third-party negotiators (recovery/police and etc)

        Your security perimeter was BREACHED
        Critically important servers and hosts were completely ENCRYPTED
        This README-FILE here for you to show you our presence
        in your's network and avoid any silence about hacking and leakage
        Also, we has DOWNLOADED your most SENSITIVE Data just in case if you
will NOT PAY,
        than everything will be PUBLISHED in Media and/or SOLD to any
third-party

1) WHAT SHOULD YOU DO:
        You have to contact us as soon as possible (you can find contacts below)
        You should purchase our decryption tool, so will be able to restore your
files
        Without our Decryption keys it's impossible
        You should make a Deal with us, to avoid your Data leakage

2) YOUR OPTIONS:
        IF NO CONTACT OR DEAL MADE IN 3 DAYS:
        Decryption key will be deleted permanently and recovery will be
impossible
        All your Data will be Published and/or Sold to any third-parties
        Information regarding vulnerabilities of your network also can be
published and/or shared

        IF WE MAKE A DEAL:
        We will provide you with the Decryption Key and Manual how-to-use
        We will remove all your files from our file-storage with proof of
Deletion
        We guarantee to avoid sharing any details with third-parties
        We will provide you the penetration report and list of
security-recommendations

                    Instructions for contacting our team

        Download and install TOR browser: https://torproject.org
        For contact us via LIVE CHAT open our
        > Website:
4jhwbypqhnbw4ee2gbbhpzlksybuvljbnvnzns2zkyp2t6urmkmq77qd.onion
        > Password: 4b34bc6d4700b411bb3ed468fe76817d
        If Tor is restricted in your area, use VPN
        All your Data will be published in 3 Days if NO contact made
        Your Decryption keys will be permanently destroyed in 3 Days if no
contact made
        Your Data will be published if you will hire third-party negotiators to
contact us
```

Exemple de sinistre Müller & Meier

Phase 2 Ransomware

- Infection d’un client par un clic sur un lien
- Le malware n’a pas été détecté.



- Cryptage des serveurs
- La plupart des postes inf. sont également cryptés
- Demande de rançon sous forme de bitcoins

☒ Sauvegarde régulière des données
☒ Sauvegarde locale inutilisable
☒ Le back-up hors site était intact

Conclusion: exemple de sinistre Müller & Meier

Rémunération

Analyse Sinistres, vérification du système CHF 1440

Reconstitution des systèmes CHF 7560,00

Divers Réparation après reconstitution CHF 2880

Frais externes

OneConsult Aide immédiate CHF 600

Indemnisation totale CHF 12 480,00

Commentaires de l'IT:

- Parfois, en informatique, on se sent comme un berger. Mais les moutons sont ivres. Et brûler! Et clique dessus n'importe où! (Source: Henrik@Celilander)

- Motivation = incitation/coûts (source: Linus Neumann)


5
Questions et discussion

Avantages chez AXA

Pourquoi AXA est-elle le partenaire idéal pour les assurances Cyber et les services?

Le service informatique de la PME ou son prestataire de services informatiques dispose d'un **interlocuteur spécialisé 24h/24 et 7j/7** en cas de soupçon.

Le **service de prévention** est **gratuit** pour les clients ayant souscrit une police Cyber.

L'**aide immédiate** est **gratuite** pour le client, même en l'absence d'événement couvert.

Gestion de crise par un **réseau d'experts** éprouvés (y c. couverture des frais RP)

Les membres de l'ASG bénéficient d'un **rabais de 10%** sur l'assurance Cyber.

Lien vers le calculateur en ligne ➔ L'ASG Cyber-Offre

Pour toute autre question ou remarque, veuillez envoyer un e-mail à notre BOX

AXA Assurances SA

Service spécialisé Assurances Cyber Clients Entreprises

cyber.security@axa.ch

Offres exclusives pour les entreprises membres de l'ASG | AXA


Merci de votre attention.