Cyberattaque d'une étude d'avocats… et après ?

Célian Hirsch, avocat et doctorant au Centre de droit bancaire et financier de l'Université de Genève

WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT

? What happened?

All your files have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.

? Why Me?

This is not a personal attack. You have been targeted because of the inadequate security provided by your vendor (QNAP).

? What now?

You can make a payment of (exactly) 0.030000 bitcoin to the following address:
bc1qcdve3qn83g44gmzrmqsces3rh2r6qm93j9jcul

Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [more information]

You can enter the **decryption key** below to start the decryption process and get access to all your files again.

important message for QNAP

🔑 Enter your decryption key here..

Plan

Analyse juridique sous l'angle de la nLPD

1. Définitions légales
2. Le devoir d'informer
3. Responsabilités civiles, administrative et pénale

Cybersecurity Incident Response Process

Définitions légales

Violation de la sécurité des données (*data breach*)

Art. 5 let. h nLPD

Toute violation de la sécurité entraînant de manière accidentelle ou illicite la **perte** de données personnelles, leur **modification**, leur **effacement** ou leur **destruction**, **leur divulgation ou un accès non autorisés** à ces données

Définitions légales

Violation de la sécurité des données (*data breach*)

- Perte
  - Disponibilité des données
    - Vol/perte d'un support de données
- Altération (modification ou effacement)
  - Intégrité des données
    - Suppression accidentelle de données
- Divulgation ou accès non autorisés
  - Confidentialité des données
    - Envoi d'un e-mail à un mauvais destinataire
    - Mauvaise gestion des droits d'accès au sein de l'étude

Principe de sécurité des données

Art. 8 nLPD

1. Les responsables du traitement et les sous-traitants doivent assurer, par des **mesures organisationnelles et techniques appropriées**, une sécurité adéquate des données personnelles par rapport au **risque** encouru.

2. Les mesures doivent permettre d'éviter toute violation de la sécurité des données [***data breach***].

3. Le Conseil fédéral édicte des dispositions sur les **exigences minimales** en matière de sécurité des données.

Définitions légales

Principe de sécurité des données

- Authentification multi-facteurs
- Mise en place des correctifs de sécurité (*patch*)
- Chiffrement des données

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Guide relatif aux mesures techniques et organisationnelles de la protection des données

Ordonnance sur la protection des données

Art. 3 Mesures techniques et organisationnelles

[1] Pour assurer la confidentialité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes autorisées n'aient accès qu'aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle de l'accès aux données);

b. seules les personnes autorisées puissent accéder aux locaux et aux installations utilisés pour le traitement de données (contrôle de l'accès aux locaux et aux installations);

c. les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé de données personnelles à l'aide d'installations de transmission (contrôle d'utilisation).

[2] Pour assurer la disponibilité et l'intégrité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données);

b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire);

c. les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données (contrôle du transport);

d. la disponibilité des données personnelles et l'accès à celles-ci puissent être rapidement restaurés en cas d'incident physique ou technique (restauration);

e. toutes les fonctions du système de traitement automatisé de données personnelles soient disponibles (disponibilité), que les dysfonctionnements soient signalés (fiabilité) et que les données personnelles stockées ne puissent pas être endommagées en cas de dysfonctionnements du système (intégrité des données);

f. les systèmes d'exploitation et les logiciels d'application soient toujours maintenus à jour en matière de sécurité et que les failles critiques connues soient corrigées (sécurité du système).

[3] Pour assurer la traçabilité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. il soit possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment (contrôle de la saisie);

b. il soit possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission (contrôle de la communication);

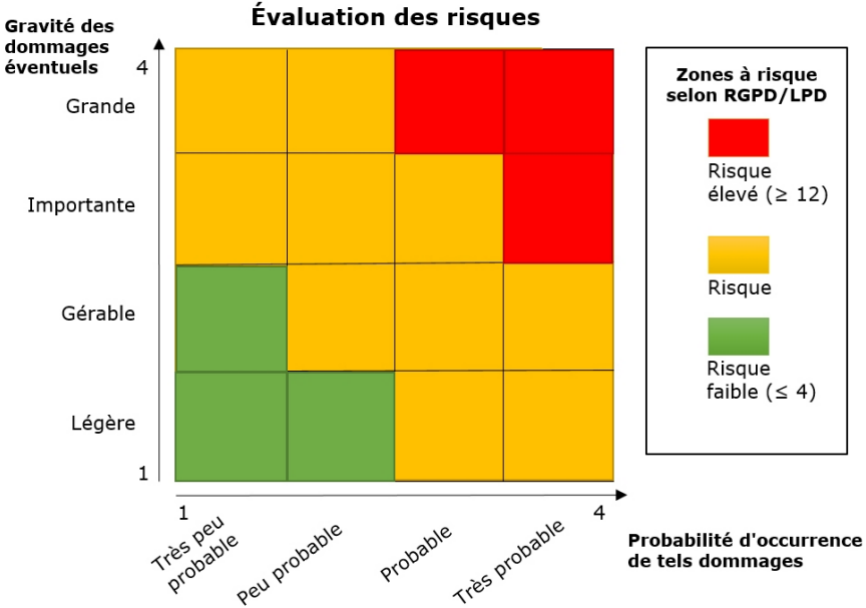
c. les violations de la sécurité des données puissent être rapidement détectées (détection) et que des mesures puissent être prises pour atténuer ou éliminer les conséquences (réparation).

Première conséquence d'une cyberattaque: il faut **informer**

	Autorité européenne compétente	PFPDT	Personnes concernées
Conditions	Dès qu'il y a une cyberattaque, sauf s'il n'y a pas de risque pour les personnes concernées	Risque élevé pour les personnes concernées	-Risqué élevé (RGPD) -Nécessaire à sa protection (nLPD) -Lorsque l'autorité l'exige (nLPD et RGPD)
Délai	72 heures	Dans les meilleurs délais	-Dans les meilleurs délais (RGPD) -La nLPD ne précise pas le délai
Contenu	La nature de la cyberattaque, ses conséquences et les mesures prises ou envisagées	La nature de la cyberattaque, ses conséquences et les mesures prises ou envisagées	Mêmes informations, mais « en des termes clairs et simples » (RGPD) / « dans un langage simple et compréhensible » (OPDo)
Sources juridiques	Art. 33 RGPD Lignes directrices du G29 Guidelines 01/2021 on Examples regarding Personal Data Breach Notification	Art. 24 nLPD Art. 15 al. 1 ODPo	Art. 34 RGPD Art. 24 al. 4 nLPD Art. 15 al. 3 OPDo

Première conséquence d'une cyberattaque: il faut informer

L'analyse du risque



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Recommendations for a methodology of the assessment of severity of personal data breaches

Working Document, v1.0, December 2013

David Rosenthal, Samira Studer/Alexandre Lombard (pour la traduction), La nouvelle loi sur la protection des données, in : Jusletter 16 novembre 2020

Première conséquence d'une cyberattaque: il faut informer

Le contenu de l'information au PFPDT

Ordonnance sur la protection des données

Art. 15 Annonce des violations de la sécurité des données

[1] L'annonce au PFPDT d'une violation de la sécurité des données comprend les informations suivantes:

a. la nature de la violation;

b. dans la mesure du possible, le moment et la durée;

c. dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées;

d. dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées;

e. les conséquences, y compris les risques éventuels, pour les personnes concernées;

f. les mesures prises ou prévues pour remédier à cette défaillance et atténuer les conséquences, y compris les risques éventuels;

g. le nom et les coordonnées d'une personne de contact.

Première conséquence d'une cyberattaque: il faut informer

Le contenu de l'information à la personne concernée

Ordonnance sur la protection des données

Art. 15 Annonce des violations de la sécurité des données

[1] L'annonce au PFPDT d'une violation de la sécurité des données comprend les informations suivantes:

a. la nature de la violation;

Dans un langage simple et compréhensible

e. les conséquences, y compris les risques éventuels, pour les personnes concernées;

f. les mesures prises ou prévues pour remédier à cette défaillance et atténuer les conséquences, y compris les risques éventuels;

g. le nom et les coordonnées d'une personne de contact.

Première conséquence d'une cyberattaque: il faut informer

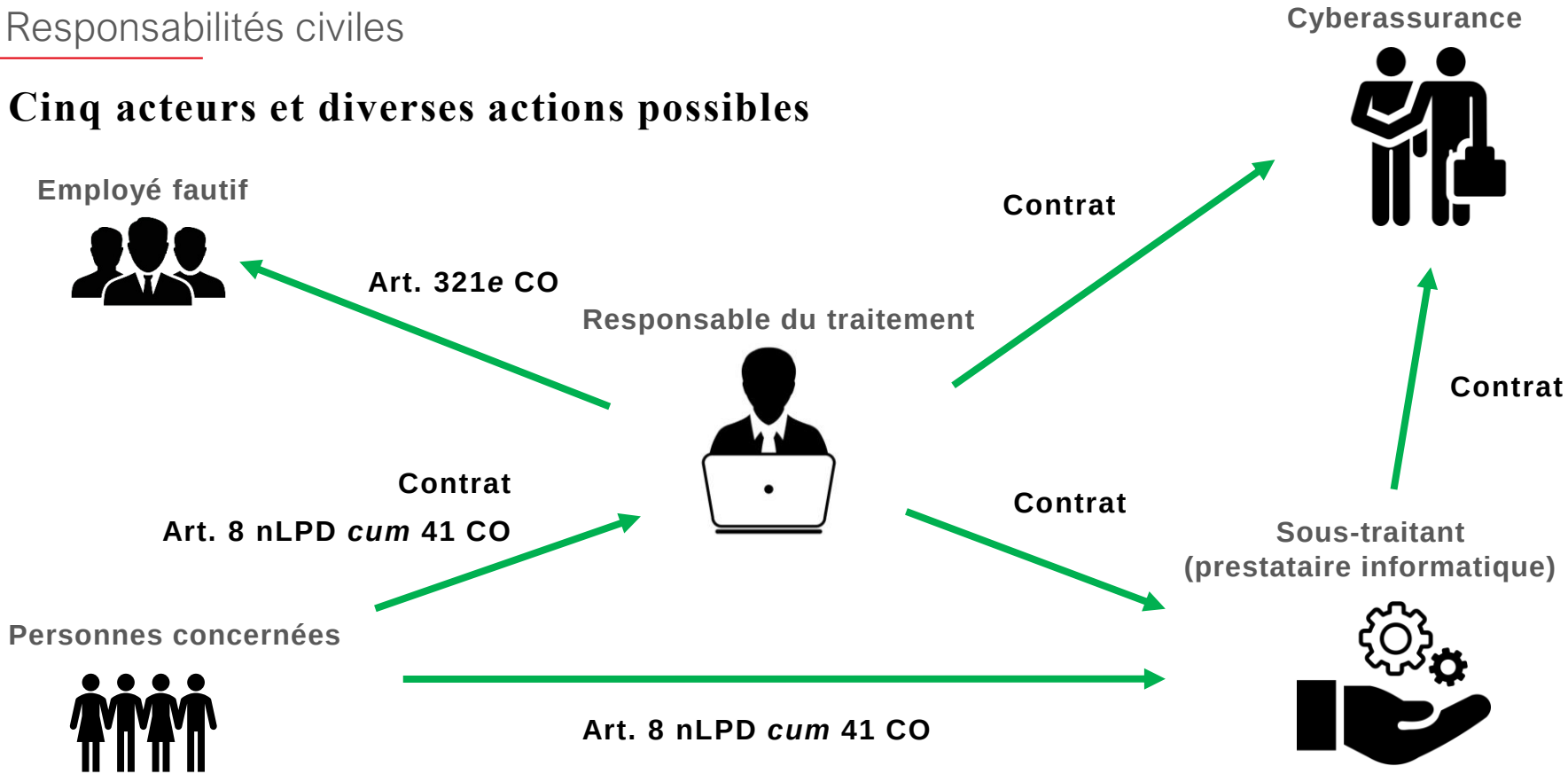
Le secret d'avocat comme limite à l'information ?

- Vis-à-vis de l'**autorité** ?
  - Non, car aucune information n'est protégée par le secret

- Vis-à-vis des **personnes concernées** ?
  - Cela dépend…
    - Non, si la personne concernée est le client (maître du secret) ;
    - Non, si le client a donné son consentement ;
    - Oui, si la personne concernée (p.ex. la partie adverse et/ou son avocat) prend connaissance, grâce à l'annonce de la violation de la sécurité, d'informations protégées par le secret.

Responsabilités civiles

Cinq acteurs et diverses actions possibles



Responsabilité administrative

Pouvoirs du PFPDT

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

- Le Préposé peut ordonner au responsable du traitement la mise en place de mesure de sécurité et d'informer les personnes concernées de la cyberattaque (art. 51 al. 3 let. b et f nLPD)…

- … mais il ne peut pas prononcer d'amende,
  - contrairement aux autorités européennes (art. 83 RGPD)

THURSDAY 10 MARCH 2022 6:51 PM

UK data watchdog fines Tuckers Solicitors £98,000 after hacker leaked legal papers onto dark web

British Airways fined £20m over data breach

16 October 2020

Piratage de cabinets médicaux en Suisse romande

31.03.2022 - La veille, il a été divulgué que plusieurs cabinets médicaux en Suisse romande avaient été visés par des pirates informatiques, lesquels ont publié de très nombreux dossiers de patients sur le Darknet. Le PFPDT est en contact avec les cabinets en question et attend à ce que les patientes et patients concernés soient informés de manière complète et transparente. Cet incident pointe une fois de plus que les données médicales sensibles en Suisse ne sont pas suffisamment sécurisées.

ICO Fines Marriott International £18.4 Million for Security Breach

Posted on October 30, 2020

Responsabilité pénale

Violation des exigences minimales en matière de sécurité des données

Art. 61 let. c nLPD **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** édictées par le Conseil fédéral selon l'art. 8, al. 3 [nLPD]

Mais quelles sont ces exigences minimales?

Exigences minimales?

Centre national pour la cybersécurité

Il est grand temps de combler les failles de sécurité de Microsoft Exchange Server

16.02.2022 - Le NCSC appelle instamment les entreprises et les communes à appliquer les correctifs aux failles de sécurité de Microsoft Exchange Server. Ces dernières, qui sont connues depuis longtemps, sont activement exploitées par les cybercriminels, notamment pour introduire des chevaux de Troie qui verrouillent les données.

Au début du mois de mars 2022, le NCSC a informé une entreprise par lettre recommandée qu'un serveur Microsoft Exchange accessible sur Internet présentait diverses vulnérabilités, qui étaient utilisées notamment pour introduire un cheval de Troie verrouillant les données (rançongiciel).

À la mi-avril, le NCSC a appris d'une organisation partenaire que l'entreprise en question avait été compromise entre-temps. Le NCSC a de nouveau écrit à l'entreprise, par courrier électronique cette fois.

Les deux tentatives de contact du NCSC sont restées sans réponse. Selon des informations accessibles au public sur le darknet, l'infrastructure informatique de l'entreprise concernée a été cryptée par un rançongiciel, et les responsables de l'attaque exigent une somme d'argent d'un montant inconnu pour le décryptage des données. De plus, les pirates auraient vraisemblablement volé des données et menacent l'entreprise de les publier (double extorsion).

Conclusion

- Chaque étude d'avocats doit mettre en place des mesures techniques et organisationnelles appropriées selon le risque (principe de sécurité des données).

- Même avec de telles mesures, le risque d'une cyberattaque réussie (et donc d'un *data breach*) reste élevé.
  - En amont, l'étude d'avocats devrait clarifier les diverses responsabilités contractuelles, voire conclure un contrat de cyberassurance.
  - Après la cyberattaque, l'étude d'avocats doit en particulier vérifier rapidement s'il existe un devoir d'information (vu les brefs délais d'annonce) et, dans un second temps, clarifier les responsabilités respectives.

Merci de votre attention