Formation continue : nLPD
Synthèse des éléments vus

Aurélie Rosemberg - CEO & Founder - Syrma SA
Expert IT & health - cybersecurity
5 mars 2024

www.syrma.ch

Réglementation – RGPD et LPD

- Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (**RGPD**).

Nouvelle LPD (entrée en vigueur septembre 2023)

- La **nLPD, la nouvelle Loi sur la Protection des Données,** est la révision totale de la loi fédérale sur la protection des données LPD qui règle le traitement de données personnelles.
- Celle-ci est entrée en vigueur le 1er septembre 2023 (sans délai transitoire).

La loi sur la protection des données, de quoi s'agit-il ?

- La loi sur la protection des données nLPD (suisse) est la nouvelle réglementation sur la protection des données qui s'ajoute à la nouvelle ordonnance sur les certifications concernant la protection des données (OCPD) qui sont entrées en vigueur le 1er septembre 2023.

Quels changements apporte cette nouvelle loi sur la protection des données suisse ?

- Tout d'abord, cette nouvelle loi sur la protection des données suisse permet une **meilleure transparence de toute collecte des données par les entreprises.** A présent, il ne s'agit plus uniquement des données sensibles mais bien de toutes les données.
- La loi sur la protection des données possède un nouveau champ d'application qui se limite à la protection des données des personnes physiques et non morales, comme c'est encore le cas aujourd'hui.
- Sont considérées comme des données personnelles sensibles les données génétiques et biométriques (nouveau).

Quels changements va apporter cette nouvelle loi sur la protection des données suisse ?

- Pour ce qui concerne le registre des activités de traitement, cela induit que **chaque entreprise doit tenir à jour un registre des activités de traitement des données contenant les informations prescrites.** Actuellement, le conseil fédéral étudie d'attribuer une exception pour les entreprises comptant jusqu'à 250 collaborateurs.

- Enfin, la nLPD (suisse) exige que les entreprises tiennent compte des principes de **protection des données** dans la conception des traitements et des applications. Ce qu'on appelle le Privacy-by-Design et le Privacy-by-Default.

Quelle différence avec le RGPD ?

- La révision de la nLPD a pour but de se rapprocher de la législation européenne en termes de protection des données, plus connue sous le sigle RGPD.

- De manière générale, la nLPD se veut moins contraignante que la RGPD. Cependant les changements sont présents :
  - La cybersécurité est à considérer
  - Le devoir d'information des usagers
  - Le renforcement de la responsabilité individuelle
  - La notion d'amende
  - Pas de délai transitoire

Ce qu'il vous reste à faire pour être conforme à la nouvelle loi fédérale sur la protection des données suisse

Pour que votre entreprise soit conforme à la nLPD (suisse), voici une liste (non exhaustive) de ce qu'il vous reste à faire :

- **Recenser les données personnelles et évaluer les risques afin de déterminer les exigences de mise en conformité ;**
- Ajouter, mettre à jour les différentes **déclarations sur la protection des données** sur votre site web, vos contenus publicitaires et marketing, vos contrats, etc. ;
- **Mettre en place des procédures internes** pour être en mesure de répondre rapidement aux demandes des patients, des tiers, des fournisseurs en lien avec leurs données ;
- Etablir un **registre de traitement des données** ;
- Mettre en place un **processus pour les analyses d'impact** ;
- Examiner **les contrats actuels (sous-traitants) pour veiller à ce que la sécurité** des données soit assurée ;
- **Nommer un conseiller à la protection des données personnelles (DPO) en interne** ou bien faire appelle à une entreprise externe spécialisée.

En cas de non-respect de la loi fédérale sur la protection des données LPD, que se passe-t-il ?

- Entrée en vigueur 1er septembre 2023.
- Enfin, dans les cas les plus déraisonnables, **une amende pourra être infligée.**
- **En résumé, mettre en place des mesures dès maintenant pour concevoir une stratégie de mise en conformité cohérente à la nLPD est nécessaire afin d'être en règle avec sa mise en vigueur qui est effective.**

Principes de protection des données

- **Principe de légalité/licéité :** tout traitement de données doit être licite;
- **Principe de bonne foi :** le traitement et la collecte de données doivent être effectués en toute bonne foi, loyalement et de façon transparente;
- **Principe de finalité :** le but du traitement et de la collecte de données doit être clairement et préalablement défini. Dans le cas de données sensibles, le consentement de la personne concernée doit être explicite;
- **Principe de proportionnalité :** les données collectées ne doivent être traitées que dans le but indiqué lors de leur collecte;
- **Principe de sécurité :** toutes les mesures nécessaires, tant techniques qu'opérationnelles, doivent être mises en place pour protéger les données personnelles (sensibles ou non) et éviter tout traitement non autorisé de celles-ci.

Protections à mettre en oeuvre avec vos fournisseurs

- **Sauvegarde régulière des données :** indispensable pour la gestion du cabinet et lors d'attaque au ransomware.
- **Logiciels et logiciels de sécurité à jour :** les cabinets peuvent installer et maintenir à jour des logiciels de sécurité tels que des antivirus et des pare-feux pour détecter et bloquer les rançongiciels.
- **Mise à jour de stratégies de sécurité réseau :** les cabinets peuvent implémenter des stratégies de sécurité de réseau, telles que la segmentation du réseau et la mise en place de pare-feu pour limiter la propagation.
- **Sensibilisation du personnel :** les cabinets peuvent former leur personnel à la sécurité informatique et les sensibiliser aux techniques utilisées par les attaquants pour diffuser les rançongiciels, telles que les e-mails de phishing.
- **Mise en place d'une politique de sécurité stricte :** les cabinets peuvent mettre en place des politiques de sécurité strictes pour gérer les accès aux données sensibles et limiter les privilèges d'administration.
- **Mise en oeuvre de stratégies de sécurité par les e-mails :** les cabinets peuvent implémenter des strategies de sécurité pour les e-mails telles que la vérification de l'authenticité des emails et la détection des e-mails malveillants.
- **Surveillance en temps réel du système :** les cabinets peuvent surveiller en temps réel leur système pour détecter rapidement tout comportement anormal et réagir rapidement.

Comment sont introduits les virus ?

Vulnérabilités :

- Nos logiciels et systèmes contiennent de nombreuses lignes de codes. Les pirates recherchent les vulnérabilités du code. Ces vulnérabilités permettent souvent de prendre le contrôle de la machine pour y introduire un code malveillant.

Sites infectés :

- Ces sites recherchent les vulnérabilités notamment des navigateurs pour introduire un code malveillant. Les utilisateurs sont attirés sur les sites en proposant des contenus attractifs (jeux, etc.) ou en recevant un email de phishing.

Pièces jointes infectées :

- Les pirates envoient un email de phishing avec une pièce jointe (Word, Excel, PDF, etc.) qui est infectée, son ouverture provoquera l'installation d'un cheval de Trois ou autre sur votre machine.

Clés USB ou support amovible :

- Une autre technique est de deposer des clés USB aux endroits où les employés sont susceptibles de passer. Les clés contiennent un code malveillant qui s'active dès qu'on les branches.

PLATEAU DE JEU – SERIOUS GAME nLPD et CYBERSECURITE AU CABINET MEDICAL

1. **Cabinet médical**
2. **1 Hacker**
3. **Des participants représentant les professionnels d'un cabinet médical**
4. **Des cartes représentant les attaques**
5. **Des cartes représentant les mécanismes de défenses à trouver pour faire face aux attaques**
6. **Des indices**

1 Accueil

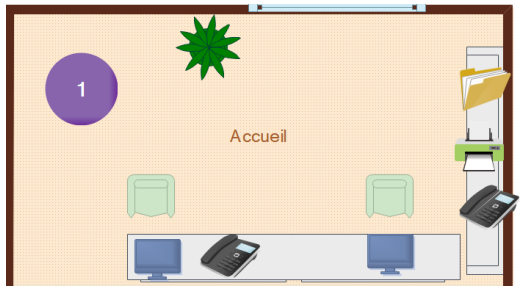
Protection des données, quelles questions se poser ?

- **Quelle information au patient concernant la collecte, les traitements et les transmissions des données et vers qui pour quels buts ?**
- **Signature d'un consentement explicite**
- **En 1ère étape, recenser les flux de données physiques et électroniques**

- **Quid de la cybersécurité….**

1

Accueil



L’accueil est la tour de contrôle du cabinet médical, en intéraction avec les patients, les fournisseurs externes comme les laboratoires, les hôpitaux, etc. De nombreuses données médicales y sont traitées. C’est aussi un lieu souvent facilement accessible de tous.

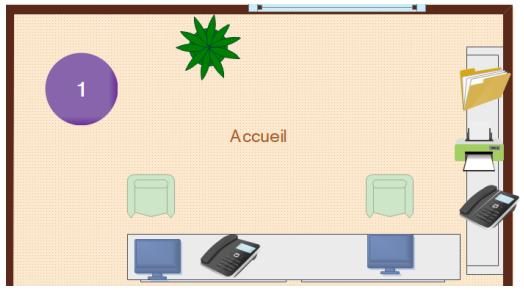
Attaque à l’ingénieurerie sociale

Quels sont les mécanismes de prévention ?

- ✓ Rester discrêt
- ✓ Challenger votre interlocuteur
- ✓ Se méfier des demandes inhabituelles
- ✓ Dans le doute, alerter

1

Accueil



L’accueil est la tour de contrôle du cabinet médical, en intéraction avec les patients, les fournisseurs externes comme les laboratoires, les hôpitaux, etc. De nombreuses données médicales y sont traitées. C’est aussi un lieu souvent facilement accessible de tous.

Phishing de masse

Quels sont les mécanismes de prévention ?

- ✓Réfléchir avant de cliquer
- ✓ Passer la souris avant de cliquer
- ✓ Recopier plutôt que cliquer
- ✓ Se méfier des pièces jointes
- ✓ Examiner l’adresse de l’émetteur du message (certificat)
- ✓Un oeil sur l’orthographe
- ✓ Usage professionnel de votre adresse e-mail professionnelle

2 Télétravail

Le télétravail est en pleine expansion aussi pour le monde médical. Parfois des données de l'environnement professionnel se retrouve dans l'environnement personnel pour faciliter le travail à la maison avec comme conséquence des lacunes de sécurité possibles.

Protection des données, quelles questions se poser ?

- **Quelle sécurité du matériel que j'utilise, des locaux, d'Internet ?**
- **Est-ce que mon employeur m'a fait signer une charte de télétravail ? Quels droits ?**

2

Télétravail

Le télétravail est en pleine expansion aussi pour le monde médical. Parfois des données de l'environnement professionnel se retrouve dans l'environnement personnel pour faciliter le travail à la maison avec comme conséquence des lacunes de sécurité possibles.

Attaque ciblée

- ✓ Sécurité des communications
- ✓Stockage des données
- ✓Eteindre les appareils à commande vocale
- ✓Attention à l'impression des documents
- ✓Identifier les participants des réunions en ligne
- ✓Sécurité physique à mettre en place
- ✓ Masquer la Webcam

3

Prise de mesure – bureau infirmier

Le développement des objets connectés (stéthoscopes, bracelets, balances, montre, etc.) expose principalement les professionnels de santé à deux types de risques : **l'utilisation commerciale des données personnelles et les atteintes à la vie privée.**

Protection des données, quelles questions se poser ?

- **Quid des contrats fournisseurs ?**
- **Où partent les données ?**

3

Prise de mesure – bureau infirmier

Le développement des objets connectés (stéthoscopes, bracelets, balances, montre, etc.) expose principalement les professionnels de santé à deux types de risques : **l'utilisation commerciale des données personnelles et les atteintes à la vie privée.**

Attaque ciblée – Objets connectés

- ✓ Modifier le mot de passe par défaut ou le code PIN de l'objet
- ✓ Effectuer les mises à jour régulières
- ✓ Garder le contrôle de vos données
- ✓ Evitez d'associer objets connectés et réseaux sociaux
- ✓ Eteindre l'objet connecté en cas de non utilisation
- ✓ En cas de création de compte en ligne sur le site fournisseur, ne communiquez que le strict minimum
- ✓ Attention au "sans fil" (Bluetooth, WiFi…)

4

Imprimante(s)

Comme les objets connectés, les imprimantes sont un haut lieu de vulnérabilité. Saviez-vous qu'il faut moins de 5 minutes pour entrer sur le réseau interne d'une entreprise depuis une imprimante avec un Wifi non sécurisé ?

Protection des données, quelles questions se poser ?

- **Qui a accès à l'imprimante ?**
- **Historique des impressions ?**
- **Pourquoi imprimer ? Quand je pars le soir, qu'est-ce que je laisse sur mon bureau ? Qu'est-ce qui est jeté dans la corbeille à papier ? Qu'est-ce qui est broyé ? Qu'est-ce qui est sous clé ?**

4

Imprimante(s)

Comme les objets connectés, les imprimantes sont un haut lieu de vulnérabilité. Saviez-vous qu'il faut moins de 5 minutes pour entrer sur le réseau interne d'une entreprise depuis une imprimante avec un Wifi non sécurisé ?

Entrée "facile" sur le réseau informatique du cabinet / Espionnage / vol de documents "papier"

- ✓Limiter l'accès physique aux multicopieurs
- ✓Séparer au niveau du réseau les multicopieurs du reste du réseau
- ✓Faire les mises à jour et suivre les bonnes pratiques
- ✓Eviter les connexions Wifi et Bluetooth aux imprimantes
- ✓Mettre des mots de passe personnels sur les multicopieurs

5 Bureau médical

Le bureau du médecin est sans doute celui qui contient le plus d'informations personnelles sensibles. Quelques règles s'imposent à ne pas manquer !

Protection des données, quelles questions se poser ?

- **Qui a accès au bureau ?**
- **Quand je pars le soir, qu'est-ce que je laisse sur mon bureau ? Qu'est-ce qui est jeté dans la corbeille à papier ? Qu'est-ce qui est broyé ? Qu'est-ce qui est sous clé ?**
- **Ménage ?**

5 Bureau médical

Le bureau du médecin est sans doute celui qui contient le plus d'informations personnelles sensibles. Quelques règles s'imposent à ne pas manquer !

Infection par virus via la clé USB / Vol de données depuis le PC portable par virus ou physique

- ✓Sécuriser vos accès et mot de passe
- ✓Encrypter vos données
- ✓N'utiliser pas de clé USB ou disques durs externes s'ils ne sont pas scannés
- ✓Mettre à jour votre sécurité
- ✓Faire vos back-ups de données
- ✓Si infecté débrancher du réseau
- ✓Avoir un bureau propre

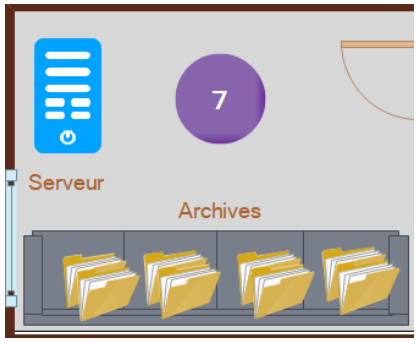
6 Salle d’attente

La salle d’attente comporte de plus en plus d’accès WiFi pour les patients. Le WiFi peut être un point de vulnérabilité. Surtout s’il est en plus accessible depuis l’extérieur de votre cabinet.

Accès à votre réseau Internet

- ✓ Sécuriser vos accès Internet

7 Archives



Ici cette pièce regroupe deux fonctions, celle de stocker votre serveur de données et celle de stocker vos archives de dossiers “papier”. Les archives “papier” doivent être conservées de manière légale pendant une longue période. Penser à un local dédié n’est pas une mauvaise chose (en dehors de la cave non sécurisée…). Pour l’accès au serveur, un local doit aussi être réservé et la température contrôlée (c’est toujours mieux que de trouver le serveur dans le placard de l’entrée…).

Accès physique à vos données

✓ Sécurisé vos accès physiques

8 Mobilité

A découvert…Dans le cadre de vos activités vous vous déplacez, chez les patients, en congrès, etc. Dans une moindre mesure le télétravail peut s'apparenter à cette situation. Dans ces situations vous emporter des données et des documents stockés sur votre ordinateur dont la perte ou le vol peut vous porter prejudice.

Attaque aux codes malveillants => vol de données physique ou virtuel

Quels sont les mécanismes de prévention ?

- ✓Protéger vos écrans
- ✓Pas de back-up dans le sac
- ✓ Pas de reseau public sans VPN & navigation sûre & Attention aux pj et liens dans emails
- ✓Surveiller vos appareils & connecter des équipements sûrs
- ✓Déclarer vos pertes et vols à votre employeur

9 Salle prises de sang

Nous avons pris l'habitude de tout faire avec notre téléphone portable, c'est devenu notre compagnon numérique qui nous suit à la trace. Nous passons environ 1h42 par jours sur notre smartphone. Les pirates ont compris depuis bien longtemps tout le parti qu'il pouvait tirer de nos smartphones. Dans cette salle, un soignant a déposé le sien.

Attaque sur votre smartphone

- ✓ Vérrouiller votre téléphone
- ✓ Chiffrer les données sensibles
- ✓ Faire les mises à jour et sauvegardes
- ✓ Attention au smishing
- ✓ Utiliser les stores officiels
- ✓ Aucune donnée confidentielle stockée sans protection
- ✓ Se méfier des réseaux publics
- ✓ Garder un œil sur votre appareil

En conclusions

- Sauvegarder régulièrement vos données : assurez-vous de la sauvegarde régulière de vos données sur un disque dur externe ou dans un cloud pour les restaurer en cas d'attaque
- Mettre à jour les logiciels régulièrement : pour prévenir des attaques
- Attention aux e-mails suspects : la vigilance est de mise
- Installer un logiciel anti-virus : à utiliser et mettre à jour sur les PC
- Eviter les réseaux publics non sécurisés
- Configurer les pares-feux : pour bloquer les connexions entrantes
- Former les employés à la sécurité informatque : c'est 80% des attaques évitées
- En cas d'attaque, ne pas payer de rançon : vous n'avez aucune certitude de récupérer vos données et cela alimente le crime

En conclusions…

- **Avant l'incident :**
  - Sensibiliser les collègues
  - Parler de la mise en oeuvre des risques
  - Animer des séances permettant d'ancrer la culture du risque cyber dans le cabinet
  - Se faire accompagner pour mettre en oeuvre un BCP des activités cyber menacées
  - En cas de situation de crise, dérouler les processus du plan préalablement établi si possible à l'aide d'experts
  - Pour le filtrage des mails, étudier les outils de sandbox
  - Organiser la collecte des historiques de toutes les machines : serveurs, clients, routeurs, switchs, FW, et les stocker pendant plusieurs mois
  - Se renseigner auprès des assureurs : cela permettant de voir s'il est possible d'assurer le risque
  - Se preparer avec des experts cybersécurité

En cas de crise

- **Pendant l'incident :**
  - Arrêter toutes les activités sur l'ordinateur infecté : pour éviter la propagation du rançongiciel ou autre à d'autres ordinateurs ou parties du réseau
  - Déconnectez-vous du réseau : pour limiter la propagation du rançongiciel
  - Contacter des experts : pour obtenir une assistance professionnelle et déterminer les mesures à prendre pour éliminer le rançongiciel

Comment pouvons-nous vous accompagner ?

Audit cybersécurité (*)

- **Quelles activités ?**
  - Analyse de vulnérabilités
  - Mise en conformité CIS 18
  - Recommandations techniques IT (sauvegarde, isolation des réseaux, Wifi, etc.)
- **Prix indicatif : 2’960 CHF**

SECUREMIND

Serious game «sensibilisation cybersécurité et nLPD»

- **Quelles activités ?**
  - 2 heures de jeu sérieux sur le thème pour retenir les concepts et quizz
  - Jusqu’à 16 pers.
  - 70% de risques en moins
- **Prix indicatif : 1’200 CHF**

Syrma Organisation Innovation Numérique Conseils stratégiques

Audit conformité nLPD (*)

- **Quelles activités ?**
  - 4 heures et recommandations
- **Prix indicatif : 1’200 CHF**

Syrma Organisation Innovation Numérique Conseils stratégiques

Etude des contrats IT

- **Quelles activités ?**
  - Etude des contrats
  - La cybersécurité passe par l’étude des contrats IT
  - Analyse des risques juridiques et techniques dans les 48H
- **Prix indicatif : 900 CHF**

Syrma Organisation Innovation Numérique Conseils stratégiques

Quinze Cours des Bastions

(*) : jusqu’à 3 médecins

Autres offres existantes…

- **Surveillance du parc informatique en «live»**

Contacts

Mme Aurélie Rosemberg
CEO & Fondatrice

info@syrma.ch
Tél. +41 21 560 93 30

www.syrma.ch

Retrouvez-nous depuis LinkedIn avec notre communauté :
https://www.linkedin.com/company/syrma-conseils

Syrma Conseils stratégiques
Organisation
Innovation
Numérique