Aide-mémoire Protection des données

Les questions à vous poser

- ☐ Connaissez-vous les données personnelles que vous traitez ? Avez-**vous recensé les traitements ?**
- ☐ Est-ce que vos traitements de données personnelles sont **licites** ?
- ☐ Les personnes dont vous traitez les données sont-elles **informées et consentantes** ?
- ☐ Collectez-vous et conservez-vous seulement les **données utiles** ?
- ☐ Avez-vous une personne responsable de la protection des données ?
- ☐ Les employés ont-ils reçu une **formation ou sensibilisation** sur la thématique ?
- ☐ Assurez-vous la **confidentialité, l'intégrité et la disponibilité** des traitements des données personnelles ?
- ☐ Avez-vous **analysé les risques** liés à l'utilisation de données personnelles ?
- ☐ Êtes-vous certain que vos **partenaires sont également conformes** ?
- ☐ Est-ce que vous êtes prêt à **gérer un incident ou une fuite de données** ?

Si vous avez 2 cases ou plus non cochées, c'est que vous n'êtes pas prêt pour le RGPD ou pour la future LPD révisée

REDstone consulting

Redstone Consulting SA
Rue Emile-Yung 10, 1205, GENEVE
Tél.: +41(0) 78 762 77 81
info@redstoneconsulting.ch
Web : www.redstoneconsulting.ch

Les malwares/maliciels

Spywares

Les « Espiogiciels » (logiciel espion) permettent de connaître ce qui se passe sur l'ordinateur infecté. Il y a deux grandes familles : Les Keyloggeurs et les Adwares.

Keyloggeurs

Les "Enregistreurs de touches" enregistrent toutes les touches que vous frappez sur le clavier dans un fichier. Le fichier en question, souvent crypté, est ensuite envoyé à, ou rapatrié par la personne malveillante qui a installé le dispositif pour vous nuire plus encore.

Adware

Les logiciels publicitaires, ou Publiciels ne sont pas très agressifs. Ils vont modifier la page de démarrage de votre navigateur Internet, ou installer un plug-in de recherche sur Internet, avec pour but de vous faire venir sur un site web, vous montrer de la publicité (ce qui rémunère l'auteur de l'Adware), et éventuellement vous voler des informations concernant votre vie privée.

Virus

Un virus informatique est un automate autoréplicatif souvent additionné de code malveillant conçu pour se propager en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté.

Vers

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il a la capacité de se dupliquer une fois qu'il a été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables.

Les chevaux de Troie (Trojan) et portes dérobées (Backdoor)

Ces programmes n'ont qu'un seul but : faire profiter à un tiers les ressources de votre ordinateur.

Macros

Les malwares sous forme de macros s'insèrent dans des documents de type "suites bureautiques". Ce qui fait d'eux de redoutables agents infectieux, notamment dans le cadre des entreprises.

Les Flooders

Ceux-ci n'ont qu'un seul but : inonder une cible (un site web par exemple) afin de l'empêcher de fonctionner. Partie intégrante des Denis de Service Distribués (DDOS), ces programmes passent souvent par une phase de contamination (installation sur le plus de machines possible) avant la phase d'attaque proprement dite.

Les Crypteurs et rançongiciels (ransomware en anglais)

Les rançongiciel. Ces chevaux de Troie infectent votre ordinateur, et chiffre vos fichiers avec un algorithme de cryptage considéré comme fort. Cela signifie que sans la clé de décryptage, il vous sera impossible de retrouver vos fichiers originaux. Une fois le cryptage de vos fichiers effectués, le malware vous affiche un message vous demandant de payer pour obtenir la clé de décryptage. La solution la plus efficace si vous êtes dans ce cas-là est de restaurer une sauvegarde de vos fichiers pour peu qu'elle ne soit pas chiffrée aussi. Les ransomwares les plus connus sont Cryptolocker, Crytowall, TeslaCrypt et Wannacry. Mais une multitude de variantes existe.