Delémont, le 15 février 2021

Communiqué de presse

Chiffres mensuels de la criminalité

Annexe au tableau daté du 05.02.2021

Protection efficace des données personnelles sur Internet et la suite à donner

Toute activité doit être accompagnée d'un certain niveau de vigilance. Les activités numériques n'y échappent pas. Sur Internet, des attaques peuvent être faites à l'encontre d'une personne morale ou physique. Elles portent sur une atteinte à la disponibilité ou à la confidentialité de données. Ces données, que les malfaiteurs obtiennent par différents moyens, ont de la valeur et méritent d'être protégées.

Avec des données personnelles, un malfrat peut par exemple les revendre, les utiliser pour effectuer des achats au nom du lésé, commettre des actes illégaux au nom du lésé, faire le maître chanteur par la menace de divulgation de secrets intimes, jeter le discrédit sur la victime. Pour obtenir des données, le malfaiteur agit comme dans la vie réelle. Soit il y accède en force (piratage, « prise d'otage des données »), par la ruse (se faire passer pour une banque, un service public ou un service d'assistance), par opportunité (en glanant les données laissées sans protection).

Les outils de ce cyber cambrioleur, usurpateur ou voleur opportuniste :

- un virus et des compétences en attaque informatique ;
- un téléphone, un email, un SMS et une poignée de poudre aux yeux ;
- un clavier, une souris et du temps pour aller chercher les données laissées de-ci de-là.

Finalement, c'est assez proche des traditionnels cambrioleurs, des faux plombiers ou des voleurs de vestiaires. Pour ces phénomènes, les mesures de protection sont connues et largement appliquées. Au niveau informatique, quelques actions à mener et le tour est joué :

- Sauvegarder ces données pour ne pas les regrettées si elles ont été détériorées ou bloquées ;
- Protéger ses terminaux informatiques avec un antivirus ;
- Utiliser et activer le pare-feu qui sécurise le trafic internet de votre appareil ;
- Mettre à jour les logiciels régulièrement ;
- Etre vigilant en vérifiant les adresses des sites et des emails, la teneur et la bonne facture des sites internet, ainsi que la vraisemblance d'une offre trop belle pour être vraie.

Les actions cyber constatées pour détrousser les utilisateurs d'Internet sont à annoncer au Centre national pour la cyber sécurité (NCSC) via sa plateforme d'annonce (https://www.report.ncsc.admin.ch/fr/). Ceci permet à cet organe national de détecter les tendances et d'agir de manière ciblée. Attention, cette démarche ne remplace pas une plainte dans un but de poursuite pénale et pour obtenir des

dédommagements. Les plaintes peuvent être déposées à la police dans les réceptions qui ont été adaptées aux mesures actuelles de protection contre la COVID-19. La police est et reste accessible par d'autres canaux. En composant le 117 en cas d'urgence, via le 032 / 420 65 65 pour une requête non urgente, par courrier électronique et postal selon les adresses présentes sur le site internet de la police.

Des informations sur le cyber risques actuels pour les utilisateurs privés, les entreprises et les spécialistes en informatique et télécommunication peuvent être obtenues sur le site internet du NCSC par ce lien : https://www.ncsc.admin.ch/ncsc/fr/home.html

Personne de contact pour la police cantonale jurassienne :
Daniel Affolter, cellule Prévention et Communication à la police cantonale jurassienne, 032 / 420 65 65