



3. Exemples concrets de cyberattaques survenues au Luxembourg

Mickael Sabatini

Responsable informatique du Syndicat des eaux du Sud (SES)



Syndicat des Eaux du Sud
Koerich



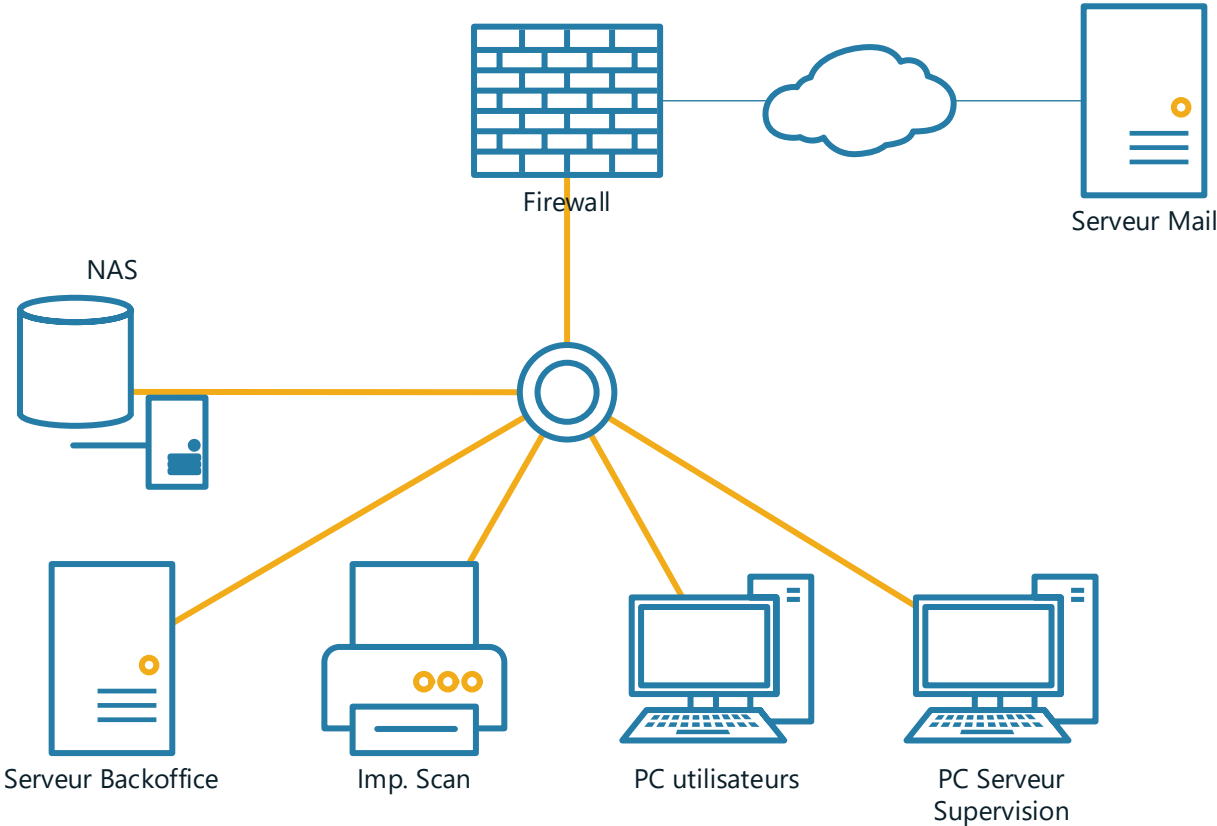
Fournir de l'eau potable, depuis 1908
22 communes Syndiquées



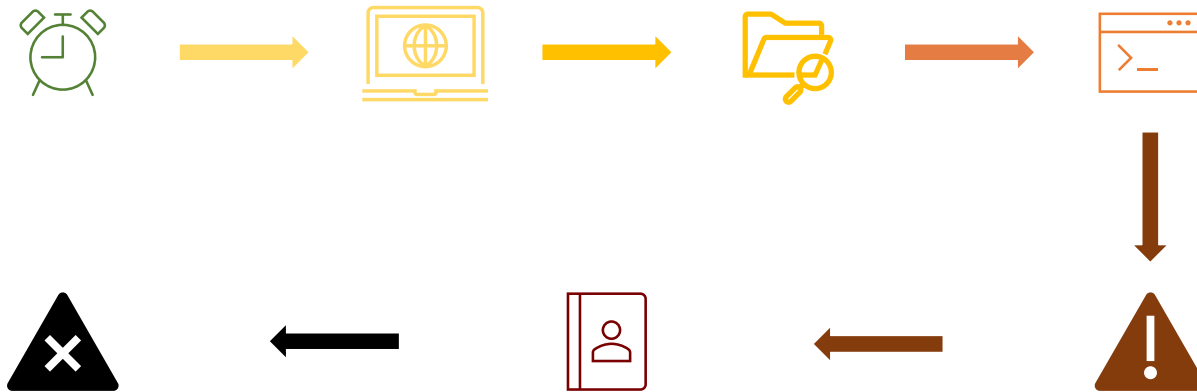
Développement des sources : forage, captage
Entretien du réseau d'eau (213 km)



Février 2013 Cyberattaque



L'histoire de Pol



Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/03/13 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h 59m 00s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 2860 files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

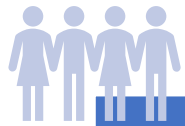
1. You should register Bitcon wallet ([click here for more information with pictures](#))

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of

PLAN D'ACTION



Organisationnel

Constitution d'une
équipe de gestion
de crise

Roadmap

Communication



Technique

Isoler les systèmes

Traçage de l'attaque

Désinfection

Restauration des
données

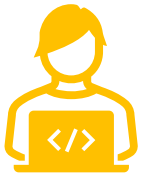
Décryptage des
données



Renforcer la sécurité



Renforcer la résilience



Mieux comprendre les menaces



Accroître la collaboration



Améliorer la détection
et la réponse



Gouvernance

Mise en place de stratégies

- Plan Directeur Informatique
- Formation et sensibilisation
- Politique de sauvegarde 3-2-1
- Contractualisation de la gestion informatique
- Conformité réglementaire



Technique

Hardware :

- Segmentation des réseaux
- Infrastructure serveur redondante
- Système de sauvegarde
- Pare-feu haute disponibilité (HA)

Software :

- Environnement professionnel Windows
- Logiciel antivirus/anti-ransomware
- Solution de messagerie Office 365



Sécurité



Vigilance



Mesures



Positif



Engagement

Questions

