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

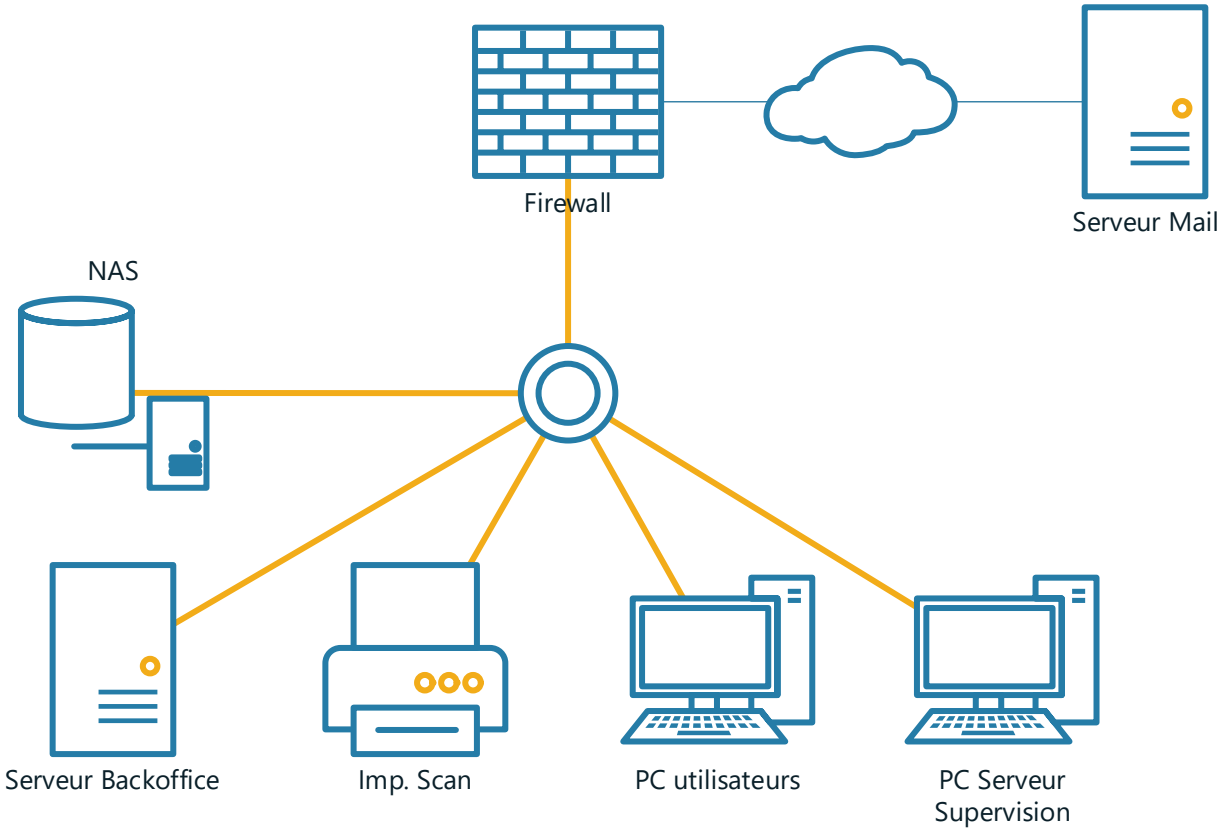
Fournir de l'eau potable, depuis 1908

22 communes Syndiquées

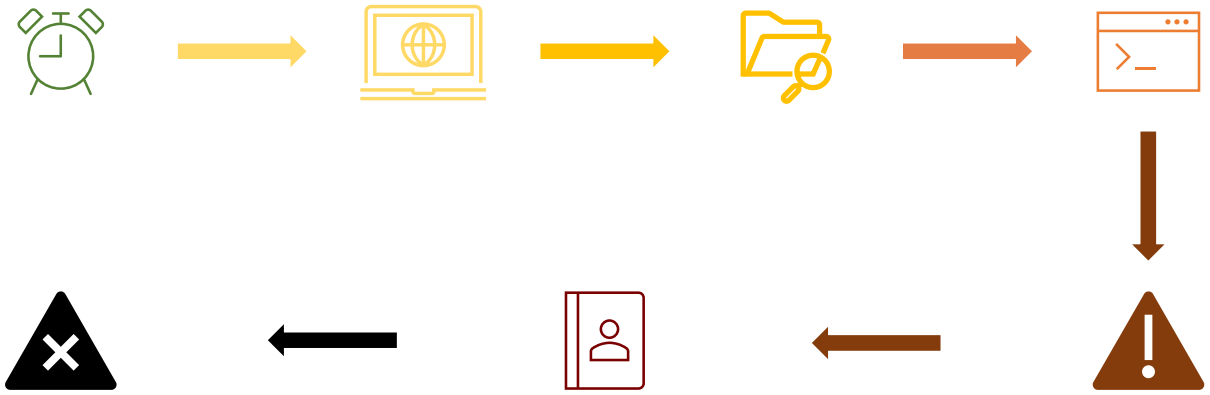
Développement des sources : forage, captage

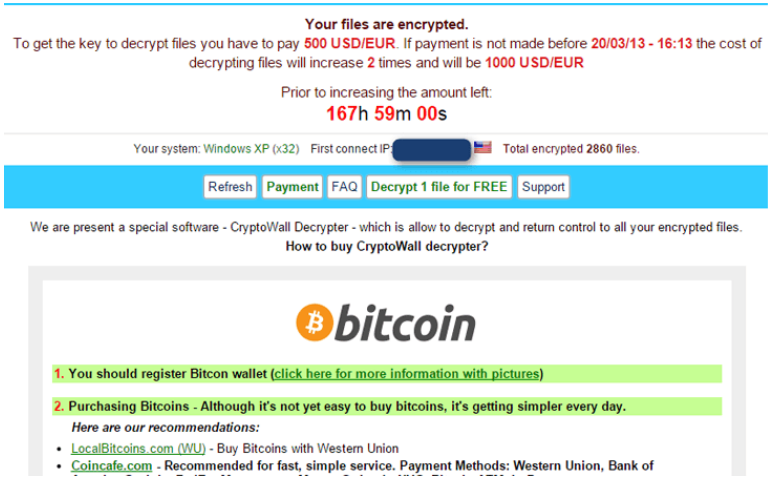
Entretien du réseau d'eau (213 km)

Février 2013 Cyberattaque

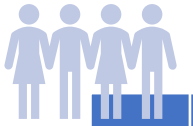

Firewall
Serveur Mail
NAS
Serveur Backoffice
Imp. Scan
PC utilisateurs
PC Serveur
Supervision

L'histoire de Pol





PLAN D'ACTION



Organisationnel

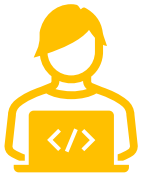
- Constitution d'une équipe de gestion de crise
- Roadmap
- Communication

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

Accroitre 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

Vigilence

Mesures

Positif

Engagement

Questions