# Après WannaCry et Petya : que faire en cas d'attaque de ransomware ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Après WannaCry et Petya : que faire en cas d'attaque de ransomware ?

**Bruxelles, le 17 juillet 2017 – C'est le plus grand cauchemar des équipes de sécurité : une attaque de ransomware comme WannaCry ou Petya. Balabit, fournisseur leader de solutions de gestion des accès privilégiés (PAM) et des logs, a reçu pendant ces attaques des informations en temps réel de ses clients et d'autres professionnels de la sécurité. L'organisation a aidé d'autres entreprises à minimiser leurs risques, tandis que sa propre équipe de sécurité a analysé les risques encourus en interne. Grâce à cette expérience, Balabit a reconstitué le déroulement des attaques afin d'en tirer des leçons. Que doivent donc faire les organisations pour contrer les programmes malveillants ? Elles doivent prendre les cinq mesures suivantes.**

Publié dans informaticien.be par zion

**1. Isolez**

Débranchez aussi vite que possible les appareils tels que les téléphones et les ordinateurs portables. Si vous êtes contaminé par un programme malveillant, retirez aussitôt le câble d'alimentation.

**2. Collectez des informations**

Qu'est-ce que c'est ? Quel est son mode opératoire ? Comment s'en prémunir ? Des équipes de désastre informatique nationales sont-elles disponibles ? Utilisez les plates-formes les plus pratiques pour diffuser ces informations : Twitter et les blogs de sécurité. Et bien sûr aussi la communication informelle entre entreprises.

**3. Segmentez le réseau**

Isolez le protocole infecté dans le trafic réseau. C'est une décision difficile : allez-vous contrer la diffusion du programme malveillant ou bien maintenir vos processus métier ?

**4. Déployez des contre-mesures**

Utilisez des Indicateur de compromission (IOC) et mettez à jour votre Système de détection des intrusions (IDS) et les paramètres du firewall, des systèmes AV et d'autant de serveurs et clients Windows que possible. Dans l'intervalle, les fournisseurs d'anti-virus travaillent évidemment sur une réponse adaptée à l'attaque.

**5. Croisez les doigts et espérez**

Anticipez l'avenir. Qu'est-ce qui se prépare ? Peut-être une nouvelle variante ? Tous les systèmes ont-ils eu leur patch ? L'organisation doit-elle craindre de figurer dans les journaux demain ? Une chose a-t-elle été perdue de vue dans l'urgence ? Étudiez tous les scénarios et essayez ainsi d'éviter un nouveau problème.

---

## Réagissez à cet article

**Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

**Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

**Quel sont nos principales activités ?**

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES

- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84

Datadock Organisme validé et référencé

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche*

*quotidienne qui permet une amélioration sur le long terme. Denis JACOPINI »*

**Besoin d'un Expert ? contactez-nous**

---



Source : *Après WannaCry et Petya : que faire en cas d'attaque de ransomware ? – Press Releases – Informaticien.be*