L'huissier, l'expert et la preuve des actes de cyber malveillance

Jérôme Legrain : legrain@blb-huissier.org

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Un bref rappel :

C’est fréquent, les entreprises ne sont pas préparées et ne donnent aucune suite

Comment se comportent les entreprises en cas de cyberattaque

91 entreprises interrogées, soit 27 % du panel, déclarent avoir été victime d'actes de cyber malveillance. Les TPE seraient les plus vulnérables (49 %) ainsi que les PME des services et de l'industrie (respectivement 29 % et 27 %). Cette attaque se matérialise la plupart de temps par le piratage du système d'information de l'entreprise (serveurs, site web, réseau de téléphonie, messagerie, etc.). 65 % des répondants indiquent avoir pu déterminer le point d'entrée dans leurs systèmes de la cyberattaque.

En cas d'incidents constatés, si certaines entreprises ont cherché à évaluer elles-mêmes la situation et régler le problème (47 %), d'autres ont fait le choix de demander une assistance extérieure pour mettre fin à cette situation (49 %).

Seulement 1 entreprise sur 5, parmi les entreprises interrogées ayant subies une cyberattaque, a déposé plainte.

70 % des répondants déclarent qu'ils étaient conscients des risques auxquels ils étaient exposés avant d'être victime de cyber malveillance.

Les pertes de données et les pertes financières induites par ces cyberattaques ont poussé les entreprises victimes à augmenter le niveau de sécurité de leurs systèmes d'information. Seules 14 entreprises ont précisé les contacts qu'elles ont cherchés à alerter.

« extrait d’un rapport de la CGPME - 2015 »

Benichou ● Legrain ● Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Quels sont les obligations et les enjeux pour l'entreprise?

Juridiques

- La plainte pénale
- L'obligation de notification des failles de sécurité
- Les responsabilités des divers intervenants

Opérationnels

- La remise en route des systèmes

Face à ces enjeux:
L'équipe de choc

- L'huissier de Justice : maitrise la preuve
- L'expert : maitrise la technologie

Leurs compétences au service des choix de l'entreprise ou de leurs conseils

- **les moyens de défense, les obligations et les enjeux étant déterminés**
- **Ils vont établir La meilleure preuve au regard de ces choix**

BLB
Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Le choix de la plainte pénale

La preuve de la cybermalveillance doit permettre de déposer une plainte pénale exploitable
La preuve est déterminante elle déterminera les textes applicables

Ce que nous devons montrer ou permettre de montrer :

- **finalité de la fraude**
  - vol de données
    - Données personnelles
    - Données bancaires
    - Secret des affaires
  - Détournement de fonds
- **mode opératoire de la fraude**
  - Atteinte au système de traitement automatisé de données
  - Usurpation d'identité
  - Escroquerie

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

L’obligation de notification

Il est nécessaire d’établir et de pouvoir décrire de façon certaine le périmètre de la cybermalveillance.

L’obligation de notification des failles de sécurité :

C’est une obligation à la charge d’acteurs spécifiques et bientôt une obligation généralisée : **La Directive NIS « Network Security and Information »**

Qui implique la notification des violations de données à caractère personnel ou failles de sécurité à l’autorité compétente et/ou à la personne intéressée

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Les responsabilités des différents acteurs

La responsabilité de l'entreprise en cas de faille de sécurité

- En tant que responsable de traitement ;
- En tant que sous-traitant
- En tant que prestataire de services informatiques.

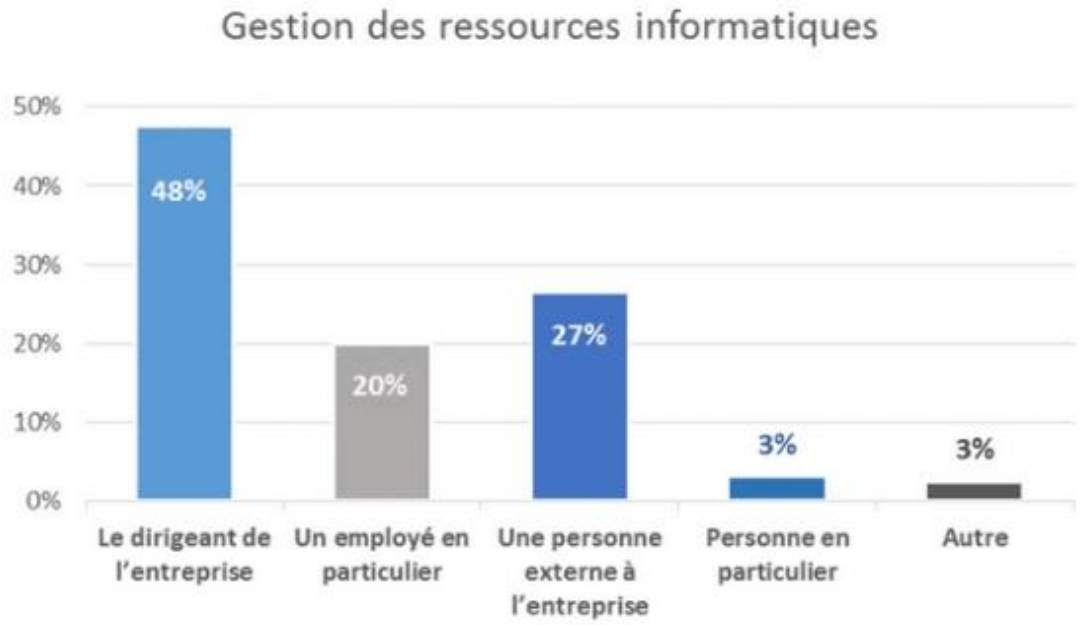
La cascade de responsabilités

- Les sociétés d'infogérance (mises à jour antivirus, patchs de sécurité)
- Les fournisseurs de matériel

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

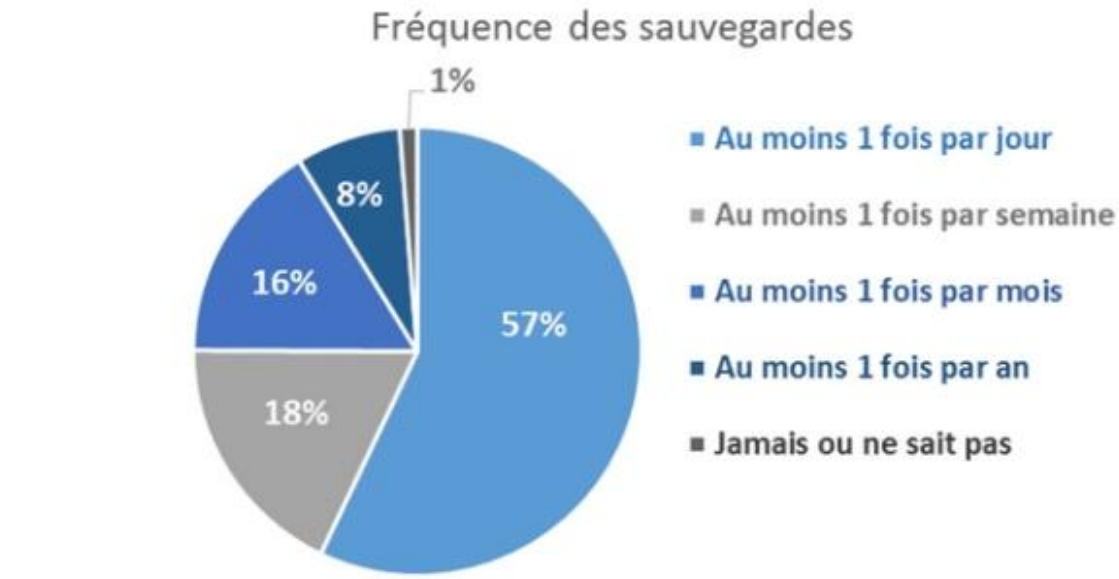
EST CE SIMPLE POUR NOTRE EQUIPE DE CHOC ?

L'entreprise, notre client, est notre meilleur ennemi



Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

EST CE SIMPLE ?
L'entreprise, notre client, est notre meilleur ennemi



Les causes principales de l'usage de ces sauvegardes sont :

- Un crash disque (42%)
- Une erreur humaine (40%)
- Une malveillance (10%)

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

ETABLISSONS ENSEMBLE LA MEILLEURE PREUVE

L'huissier et l'expert assurent :

- Une traçabilité qui indique les conditions de l'établissement de la preuve
- L'authenticité qui garantit l'origine de l'information
- L'intégrité qui garantit le contenu de l'information
- Le critère de pérennité qui garantit la bonne conservation de la preuve
- Le critère d'exploitabilité

BLB
Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Une traçabilité qui indique les conditions de l'établissement de la preuve

L'authenticité qui garantit l'origine de l'information

« Ce qui se conçoit bien s'énonce clairement, et les mots pour le dire arrivent aisément »

Une description lisible et claire du contexte :

la cybermalveillance pour les juges

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

L’intégrité qui garantit le contenu de l’information

- L’expert donne le moyen technologique de garantir le contenu de l’information

- L’huissier donne sa garantie de tiers de confiance

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

Le critère de pérennité qui garantit la bonne conservation de la preuve

Le critère d'exploitabilité

- L'expert fournit le moyen technologique : le support
- Le contenu du support doit être exploitable pour une post expertise

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS

SI LA MISSION EST BIEN REMPLIE

- L'entreprise peut s'attacher à ses impératifs opérationnels : Redémarrage des systèmes après corrections
- L'huissier et l'expert peuvent inclure la preuve de la correction des anomalies
- La preuve en amont de la conformité de l'installation

Benichou • Legrain • Berruer
HUISSIERS DE JUSTICE ASSOCIÉS