Tous unis contre la fraude et la cybermenace

Bernard GALL
Eurazeo
AFTE

Gérôme BILLOIS
Wavestone

Lari LEHTONEN
Marsh

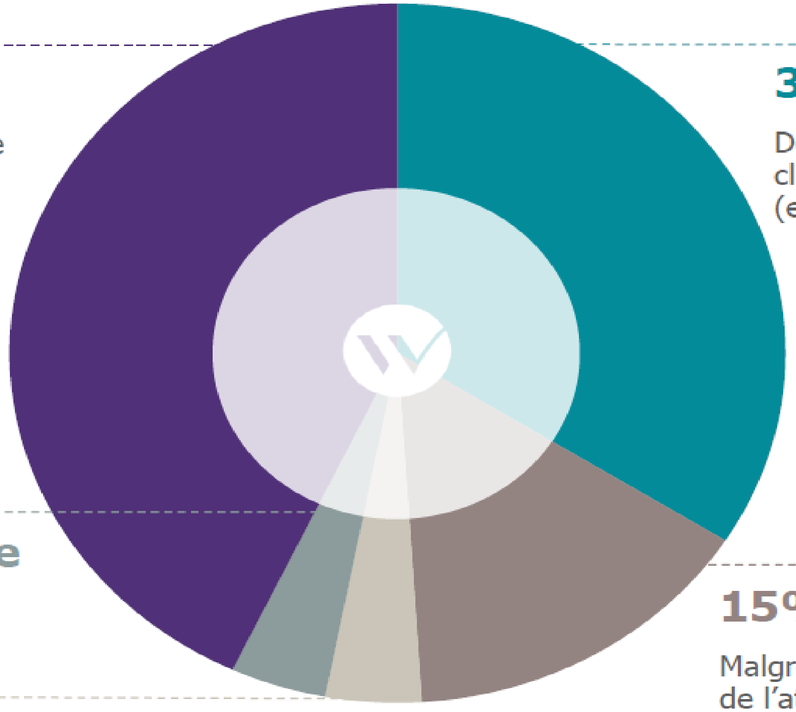
Monika RAZNY
EDF Renouvelables

Vincent LORIOT
ANSSI

Betty SFEZ
Cabinet
Sfez Avocats

L’appât du gain financier, le moteur principal des cybercriminels

Répartition des incidents de sécurité par motivation des attaquants



43% Gains financiers

Dont 36% d’attaques par ransomware et 7% de fraudes

34% Vol de données

Données métiers (e.g. coordonnées de clients, données bancaires…) et techniques (e.g. liste de comptes utilisateurs)

4% Nuisance à l’image

Défiguration de site web, vol de comptes sur des réseaux sociaux

4% Gains de capacité d’attaque

Détournement d’informations ou de ressources pour mener une attaque sur une autre cible

15% Indéterminée

Malgré la compromission, les motivations de l’attaquant n’ont pas pu être identifiées (attaque abandonnée, interrompue, compromission de systèmes sans actions ultérieures…)

Des capacités de détection très hétérogènes parmi les grandes entreprises accompagnées

167 jours

Temps moyen écoulé entre une intrusion et sa détection

Mais encore…

50%

des entreprises détectent l'intrusion **dans les deux jours**

35%

des entreprises ne détectent l'intrusion que **dans les 6 à 9 mois**

6 ans

le **délai maximum** observé entre le début d'une attaque et sa détection par l'une des entreprises du panel…

Combien de temps pour un retour à une **situation technique normale ?**

1 semaine

Pour un ransomware « simple » (i.e. sans propagation)

3,5 semaines

Pour une attaque ou un ransomworm ayant détruit une partie importante du système d'information

Et au moins 6 semaines pour une reconstruction saine, avec deux actions clés :

Reconstruction du cœur de confiance du SI pour bascule vers un nouvel environnement sain sur un week-end
Nettoyage et réimportation des données métiers créées pendant la crise

Comment éviter de devenir une cible ?

65%
des attaques sont opportunistes

Être au-dessus de la moyenne en cybersécurité permet de limiter fortement son attractivité auprès des cybercriminels

TOP 5 des actions pour se préparer à faire face à une attaque

- **Protéger les actifs les plus critiques en adoptant les bonnes pratiques de sécurité** (correctifs de sécurité, gestion des droits, gestion des administrateurs…)
- **Améliorer l'efficacité de la détection des attaques avec un service spécialisé** (surveillance 24/7, périmètre de détection adapté à la menace…)
- **Savoir gérer une crise majeure** (équipe 24/7, moyens de communication spécifiques…) **et reconstruire en urgence** (procédures, matériel spécifique…)
- **S'entrainer grâce à des exercices de crise** (répéter les efforts en différentes situations pour favoriser le développement de réflexes)
- **Souscrire une cyber-assurance et un contrat auprès d'une équipe spécialisée** (s'entourer des experts pouvant accélérer la résolution de l'incident)

Tous unis contre la fraude et la cybermenace

Bernard GALL
Eurazeo
AFTE

Gérôme BILLOIS
Wavestone

Lari LEHTONEN
Marsh

Monika RAZNY
EDF Renouvelables

Vincent LORIOT
ANSSI

Betty SFEZ
Cabinet
Sfez Avocats