WEBINAIRE

La FRENCH TECH PARIS SACLAY

Co-animateur

oxibox
Solutions de cyber-résilience

Les enjeux de la cyber-résilience dans un contexte de crise : comment affronter la recrudescence des cyberattaques ?

François Feugeas, fondateur d'Oxibox

oxibox
Solutions de cyber-résilience

Oxibox

Garantir la cyber-résilience de toutes les entreprises

Oxibox permet de garantir la pérennité des données de toutes les entreprises.

Nos solutions résolvent les enjeux suivants, ignorés par les solutions de sauvegarde traditionnelles :

1. **Résistance des silos de sauvegarde aux cyber-attaques** - Oxibox est sécurisé par défaut, par l'inclusion dû chiffrement à la source et par l'isolation des silos de sauvegardes du réseau de production.
2. **Restauration rapide** - notre technologie R2V permet un redémarrage instantané de machines virtuelles cross-hyperviseur.
3. **Unification** - nos solutions sont totalement cross-platform, permettant ainsi une protection des données quel que soit leur lieu de stockage - des postes de travail aux systèmes hyperconvergés.

oxibox

Exemples d'attaques

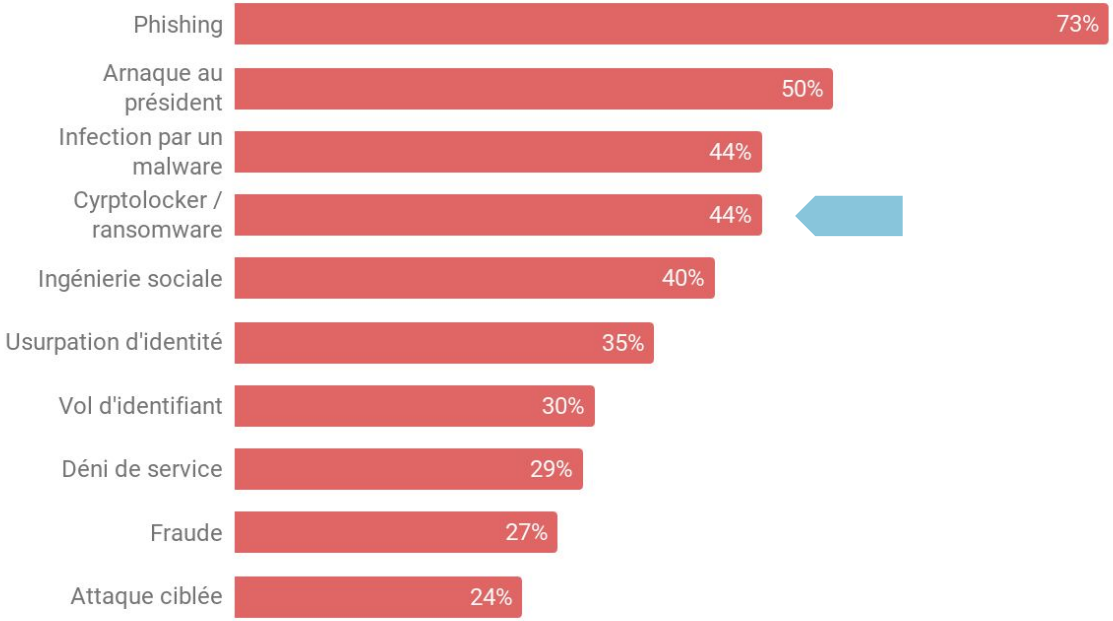
Maze Janvier 2020
700 To de données bloquées, Big game hunting,
10M$ réclamés

DDos Mars 2020
Serveurs visés par de fausses requêtes.
Interruption des emails et outils de télétravail

Ransomware Novembre 2019
150 collaborateurs bloqués, placé en redressement judiciaire par mesure de protection

Ransomware Mars 2020
SI et transmission des procurations visés sur la période électorale. Interruption des applications et services

Les cyber-attaques les plus courantes dans les entreprises



Source : Baromètre de la cybersécurité CESIN 2019

Industrialisation des menaces

Émergence du Ransomware-as-a-Service
Gandcrab : 2 Md$ de bénéfice revendiqués pour 392 affiliés “distributeurs”.

Spécialisation des attaquants
Maze : “big game hunting” et exfiltration de données.

DDoS as-a-Service
Mirai : plus de 600.000 devices IoT infectées, plus de 1.3 Tbps.

Plus d'attaques

80%

des entreprises françaises subissent au moins une attaque cyber dans l'année

+500%

croissance de la menace ransomware dans le monde en 2019

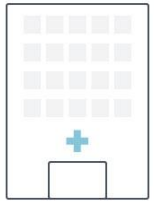
+200%

d'attaques cyber en France au mois d'avril 2020

Les entreprises sont menacées en permanence par les attaques **mais sont encore plus vulnérables en période de crise.**

Sources : CESIN, Panocrim, Orange Cyberdefense

Plus ciblées



Victimes choisies

Diffusion de masse (ex: Wannacry)
> Attaques planifiées : acteurs publics, établissements de santé, organisations détenant des données sensibles.

Attaques plus ciblées

Fichiers de sauvegarde visés en priorité
Objectif : conséquences plus lourdes pour bloquer / ralentir la reprise d'activité.

Avec plus de moyens

Les auteurs d'attaques sont des organisations ordonnées : services techniques de pointe, ressources financières importantes, communication bien orchestrée.

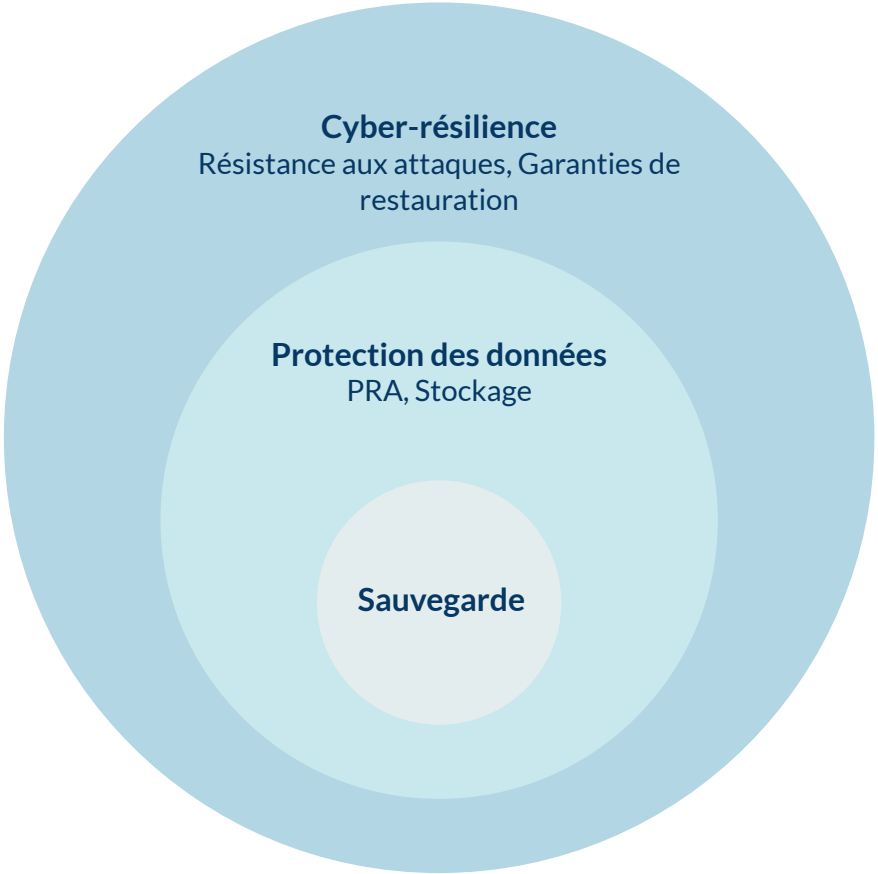
Pourquoi les entreprises sont plus vulnérables en période de crise ?

- Multiplication des vecteurs d'attaque.
- Connexions hors site mal sécurisées.
- Utilisation d'ordinateurs personnels peu ou mal protégés (Shadow IT, mises à jour non régulières…).
- Augmentation tentative phishing (+667% d'emails de phishing en mars*), salariés moins encadrés.
- Désorganisation des entreprises.
- Surface de données à protéger plus large / plus disparate.

** Source : Barracuda Networks*

Comment se protéger

- Sensibilisation des utilisateurs.
- Sécurisation réseau.
- Application des mises à jour.
- Solutions de cyber-résilience.
  - Protéger les données où qu'elles soient produites, exploitées ou stockées
  - Isoler les fichiers de sauvegarde
  - Restauration rapide pour une reprise d'activité immédiate



Enjeux de la cyber-résilience

- Garantir la résistance de la solution proprement dite aux cyberattaques.
- Faciliter l'implémentation d'un PRA/PCA et optimiser le RTO
  - Couverture de 100% du SI de manière uniforme : pas de différenciation.
  - Redémarrage immédiat (<5 minutes) d'un système sinistré sous forme de machine virtuelle.
  - Automatisation d'un montage VPN pour les restaurations remote
- Contrôle fin du RPO grâce aux performances de la solution

La FRENCH TECH
PARIS SACLAY

www.oxibox.fr
www.frenchtech-paris-saclay.fr

contact@oxibox.fr
+33 (0)1 85 40 03 49