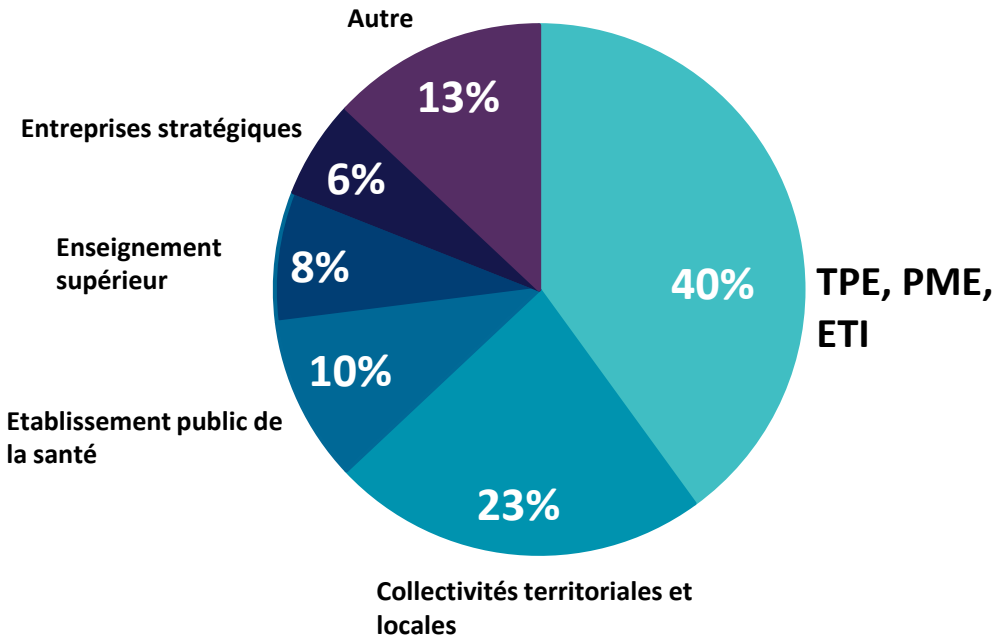
01

TOUS LES ETABLISSEMENTS SONT CONCERNÉS

LE RISQUE CYBER

Victimes de ransomware en 2022

ANSSI – Panorama de la cybermenace



EN QUOI SUIS-JE CONCERNÉ PAR UNE ATTAQUE CYBER ?

Enjeu de disponibilité

Quels outils informatiques utilisez-vous au quotidien ? Boite mail, gestion RH, outil de comptabilité...?

Quelles seraient les conséquences d'une indisponibilité de ces outils sur la bonne marche de votre activité ?

Enjeu d'intégrité

Que se passerait-il si les données étaient détruites, bloquées ou chiffrées ?

Quelles sont vos sauvegardes ?

Pourriez-vous poursuivre votre activité si un cyberattaquant rendait vos outils inutilisables ou chiffrait vos données ?

Enjeu de confidentialité

Quelles données possédez-vous ? Sur vos collaborateurs, vos élèves, vos partenaires...?

Quelles seraient les conséquences d'une publication de ces données sur internet?

.

Pour beaucoup d'organisations, il est plus probable d'être victime d'une cyberattaque que d'un incendie

LES CAUSES D'UN SINISTRE

1 La cybercriminalité

- Phishing
- Ransomware
- Vol de données
- Déni de service, défacement

- Déstabilisation, prépositionnement
- Espionnage industriel et/ ou stratégique
- Malveillance interne
- Activisme

2 Erreurs humaines

- Écrasements ou effacements des données
- Mauvaise utilisation du Système d'information (SI)
- Mises à jour non réalisées

3 Vulnérabilités techniques

- Mauvaise configuration d'un serveur
- Panne du SI

LES CONSÉQUENCES D'UN SINISTRE CYBER

Arrêt de l'activité
Suite à l'introduction d'un logiciel bloquant le système informatique

Conséquences humaines
Surmobilisation des collaborateurs liée à la gestion de crise

Conséquences juridiques
suite à une fuite de données ou à une transmission de virus

Pertes d'exploitation
Liées à l'arrêt de l'activité

Fuite de données
divulgation de données de l'entreprise, des clients, prestataires ou fournisseurs

Transmission de virus vers un tiers
clients, prestataires ou fournisseurs peuvent être impactés

Pertes indirectes
coûts de désorganisation, perte de marchés, atteinte à la réputation, perte d'avantages concurrentiels

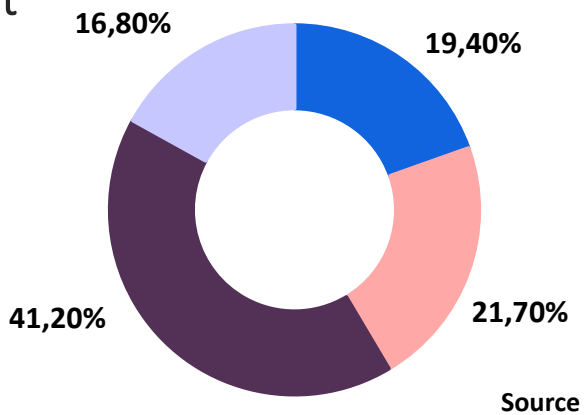
FOVI ou fraude au président
Détournement d'un paiement vers un compte frauduleux

LES CHIFFRES DU RISQUE CYBER

- *20% des intrusions consistent en l'exploitation d'une faille technique* sur ce qu'une entreprise expose sur internet, c'est-à-dire principalement son site internet. L'absence de site internet/de site vitrine peut éventuellement réduire ce risque, et encore...
- *80% des intrusions débutent par du phishing:* si vous avez des boîtes mails pros/des téléphones pros, alors vous êtes soumis à ce risque comme une autre entreprise.

Répartition des sinistres déclarés par type d'évènement

- Ransomware
- Fraude
- Compromission d'une messagerie
- Autres



Source : Stoïk

SCHÉMA TYPE D'UNE ATTAQUE CYBER

1 Intrusion sur le SI

Phishing
Vol de compte
Exploitation de vulnérabilité

2 Maintien des accès

Création de portes dérobées pour s'assurer une durabilité des accès au SI en cours d'attaque

3 Mouvement latéral, propagation sur le SI

Scan, exploration du SI pour découvrir sa structuration
Identification des ressources exploitables
Mise en œuvre de la stratégie de rentabilité de l'attaque (vol de données, rançon)
Identifier les sauvegardes

4 Elévation de privilèges

Compromission d'un compte administrateur,
Devenir Administrateur du Domaine
Prendre la main sur le SI et les sauvegardes

5 Exfiltration de données

Assurer ses moyens de pression
Rentabiliser l'attaque

6 Chiffrement du SI

Déploiement du Ransomware

INTRUSION | **ELEVATION DES PRIVILEGES** | **EXPLOITATION**

LES ÉTAPES DE LA DÉFENSE

INTRUSION

Sensibiliser l'ensemble des collaborateurs

Réaliser régulièrement des **tests**

Scanner, tester régulièrement pour identifier des points d'entrées

Définir des **politiques** de gestions des **droits d'accès** au SI (MFA)

Séparer les **comptes à privilèges** (administrateurs)

Intégrer les règles de **sécurité** aux **prestataires**

Maintenir ses systèmes sous support et **à jour**

ELEVATION DES PRIVILEGES

Surveiller le SI avec intervention (EDR, SIEM, SOC …)

Surveillance particulière des **comptes** en **mobilité**

Segmenter le réseau (IT / OT)

Sécuriser l'annuaire

EXPLOITATION

Stratégie de sauvegarde Offline / immuable / hors AD

Plan de reprise sur la base de scenarios prédéfinis

4 MOTS CLÉS :

PREVENIR l'exposition de l'entreprise vis à vis du risque Cyber

ANTICIPER la survenance d'une cyber-attaque

ATTENUER les conséquences d'une cyber-attaque

RESTAURER les capacités de reprise d'activités

02

CYBER-RISQUES : POURQUOI SOUSCRIRE ?

LES CONSÉQUENCES D'UN SINISTRE

Saint-Christophe
MUTUELLE D'ASSURANCES

Une police multirisques qui indemnisera :

LES FRAIS LIES A LA GESTION DE CRISE :

- ✓ Mesures d'urgence, d'experts informatiques, de monitoring et de surveillance
- ✓ Frais de notification
- ✓ Restauration des données
- ✓ Frais pour éviter ou limiter une atteinte à la réputation

VOLET RESPONSABILITE CIVILE :

- ✓ Une atteinte aux données personnelles et/ou confidentielles
- ✓ Atteinte à la sécurité du système d'information
- ✓ Manquement à une obligation de notification
- ✓ Atteinte à l'image suite à la publication ou la transmission de tout contenu média numérique sur des sites internet ou sur les médias sociaux

VOLET PERTE D'EXPLOITATION :

- ✓ La marge brute perdue
- ✓ Et/ou les frais supplémentaires que vous devez engager pour éviter une perte d'activité

LES CONSEQUENCES D'UNE EXTORSION INFORMATIQUE :
(demande de rançon via un RansomWare)

- ✓ Remboursement de la rançon
- ✓ Pertes d'exploitation
- ✓ Frais de consultants et de traducteurs interprètes

APPLICATION DES GARANTIES

Comment fonctionne l'assurance en cas d'incident ?

Assistance : équipe dédiée ou prestataire 24h /24h 7 j 7 Scenario type d'un sinistre

Son rôle :
-répondre aux incidents
- défendre le système d'information
- Échanges avec les autorités compétentes (force de l'ordre, CNIL…)
- Avocat et expert en communication de crise

Remédiation

Remise en état de l'infrastructure par les prestataires pour une reprise rapide de l'activité souvent pas accès à distance

Indemnisation

Suite à l'envoi des justificatifs permettant d'évaluer le sinistre : indemnisation selon les conditions du contrat.

Saint-Christophe
MUTUELLE D'ASSURANCES

Merci de votre attention

Vos questions

Praeventia
RISK MANAGEMENT