Sécurité
Chiffres clés

Au niveau mondial

- En 2021 le coût estimé de la cybercriminalité est de 760 milliards de dollars
- Cela représente plus de 1% du PIB mondial

(Source : CSIS, Centre for Stratégie and International Studies)

- Le secteur bancaire est le plus exposé :
  - Cyberattaques : + 255 %
  - Tentatives d'extorsion de données personnelles : + 800%

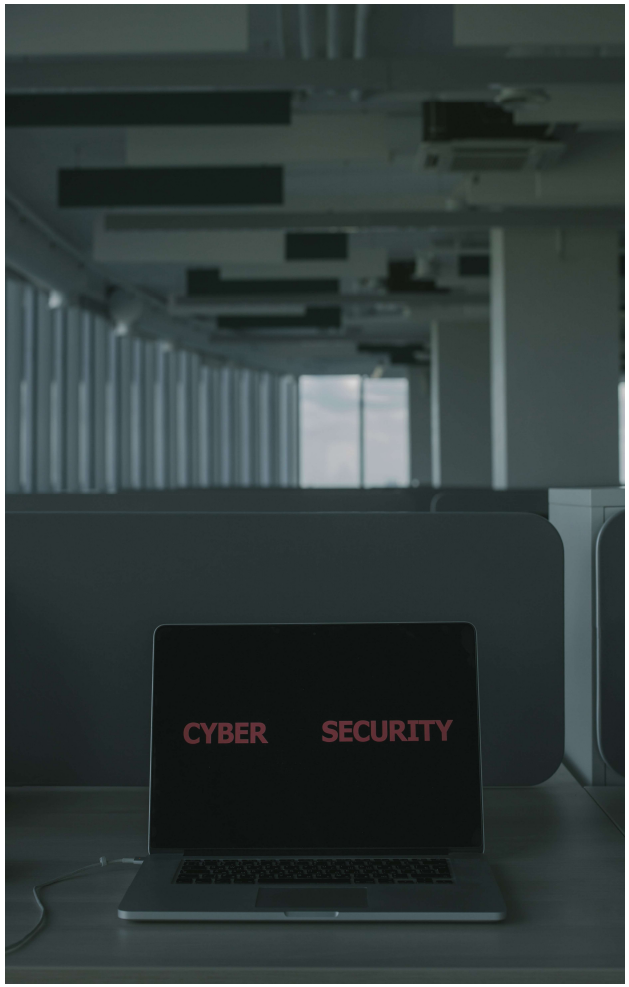
(Source : bureau d'études spécialisé VMware Carbon Black)

Les premiers constats pour les entreprises

- 54% des entreprises françaises ont été attaquées en 2021
- Le phishing est le mode d'attaque le plus fréquent avec 73% d'entreprises touchées
- 47 % des télétravailleurs se font piéger par le phishing
- 59% des entreprises affirment que les cyberattaques ont eu un impact sur leur activité
- 98% des entreprises interrogées estiment que la transformation numérique (usage du cloud et l'Internet des objets) a un impact sur la sécurité de leur SI
- 87% des entreprises stockent une partie de leurs données dans le cloud, dont 52% dans des clouds publics

Que font les collaborateurs d'une entreprise ?

- 70% utilisent des appareils professionnels à des fins personnelles
- 37 % utilisent leur ordinateur ou smartphone personnels pour accéder aux applications professionnelles
- 57 % des violations de données auraient pu être évitées en installant une mise à jour
  - systèmes d'exploitation
  - logiciels professionnels
  - logiciels de sécurité



Les petites entreprises comme les autres

- 43% des cyberattaques visent les petites entreprises
- 4 PME sur 10 ont la certitude d'avoir déjà subi des attaques
- Les principaux types d'attaques :
  - Hameçonnage (*phishing*) : 24 %
  - Malware : 20 %
  - Rançongiciel (*ransomware*) : 16 %
  - Fraude au président : 6 %
- Il faut entre 15 minutes et 10 jours pour s'introduire dans un réseau d'entreprise
- Le taux de réussite est supérieur à 90%

(source : rapport de Positive Technologies, spécialisée dans les pentests)

Les conséquences pour les entreprises

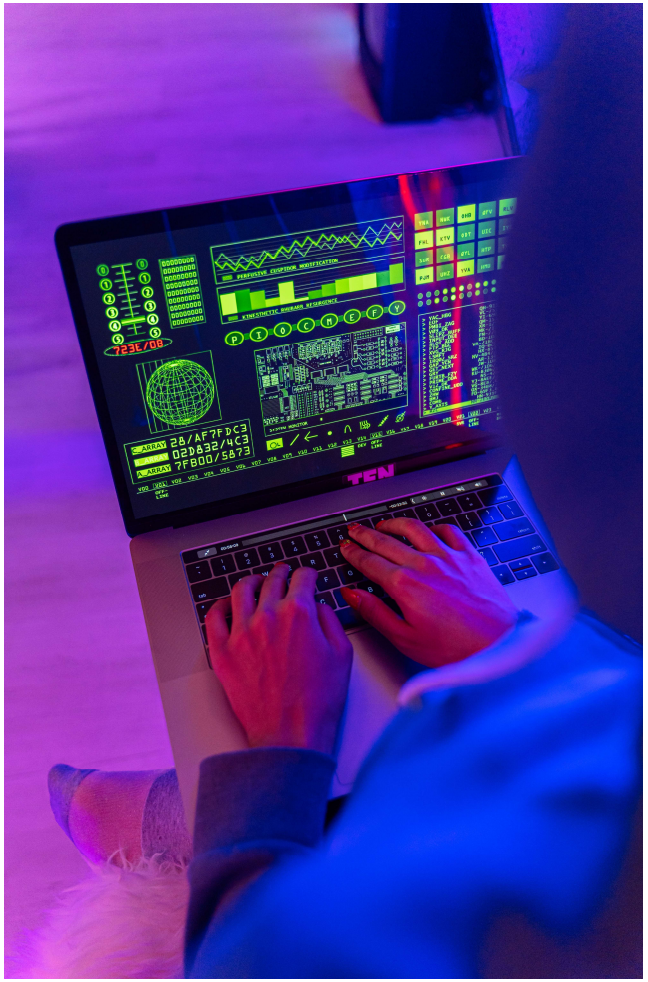
- 26% ont connu un ralentissement de la production pendant une période significative
- 9% ont subi un arrêt de la production pendant une période significative
- 23% ont constaté une indisponibilité de leur site Internet
- 12% ont subi des retards de livraison auprès des clients
- 11% ont eu des pertes de chiffre d'affaires

Les effets négatifs les plus significatifs

- augmentation de la charge de travail
- baisse de productivité des collaborateurs
- mauvaise réputation de l'entreprise

A noter que :

- les dépenses en cybersécurité ne devraient augmenter que de 12% par an et par entreprise d'ici à 2025 alors que …
- … une entreprise est victime d'une attaque par ransomware toutes les 20 secondes



Les outils et actions des entreprises

- 36 % des entreprises changent les mots de passe de leurs ordinateurs de bureau au moins une fois tous les six mois
- 39 % des entreprises disposent d'une triple protection (antivirus, firewall, anti-spam) pour leurs ordinateurs de bureau
- 30% disposent d'une triple protection (antivirus, firewall, anti-spam) pour leur réseau
- 98 % des entreprises disposent d'au moins un outil de sauvegarde
- Les outils de sauvegarde utilisés sont :
  - un support externe (clé USB, disque dur externe, etc.) : 68 %
  - une solution cloud : 49 %
  - un serveur de stockage interne : 45 %

Un bilan inquiétant pour les entreprises

- Seulement 17 % des PME sont assurées contre les attaques informatiques
- 76% des entreprises sensibilisent leurs salariés aux risques informatiques, dont 44% au moins tous les ans
- Il faut en moyenne 6 mois à une entreprise pour détecter une violation de ses données
- 21% de tous les dossiers d'une entreprise sont ouverts à tous
- 65% des entreprises ont des salariés qui n'ont jamais changé leur mot de passe
- 80 à 90% des violations de données sont dues à une erreur humaine

Et demain ?

- L'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information (*https://www.ssi.gouv.fr*) dispose d'un budget annuel un peu supérieur à 100 millions d'euros et d'un effectif d'environ 700 personnes
- En France, on recense environ 5 000 cyber enquêteurs qui évoluent dans des structures privées

Et demain ?

- Le budget 2023 de l'Etat français prévoit de créer 1 500 postes d'enquêteurs aussi appelés cyber-patrouilleurs
- L'État veut également créer une école de formation cyber et lancer le « 17 Cyber », un équivalent numérique du 17 téléphonique
- Ce « 17 Cyber » permettra de signaler en direct une cyberattaque ou une escroquerie en ligne, afin que « *chacun puisse être mis en relation avec un opérateur spécialisé* »
- Les policiers pourront, sur autorisation de la justice, saisir des actifs numériques