infoblox

ÉTUDE 2023 SUR LE BILAN MONDIAL DE LA CYBERSÉCURITÉ

FRANCE

CRA | Business Intelligence
A CyberRisk Alliance Resource

MÉTHODOLOGIE

Les données et les idées contenues dans ce rapport publié par CyberRisk Alliance sont basées sur une enquête mondiale menée à distance en juillet/août 2022 auprès de responsables et d'influenceurs du secteur de l'informatique et de la cybersécurité de 13 pays, dont 100 entreprises de toutes tailles basées en France. Les personnes interrogées en France étaient aussi bien des chefs d'entreprise et des directeurs que des analystes et des consultants. Les personnes interrogées occupaient des emplois dans divers secteurs, notamment la production (25 %), les services aux entreprises ou professionnels (24 %), les technologies (12 %) et l'énergie ou le commerce de détail (7 % chacun). Un petit nombre d'entre eux travaillaient dans les secteurs de l'éducation, des médias, de la santé, des transports, des services financiers, des administrations publiques, des organismes sans but lucratif ou des services publics.

RÉSUMÉ EXÉCUTIF

Les citoyens français ne se préparent pas seulement à un hiver interminable et glacial caractérisé par des restrictions énergétiques liées à la guerre entre la Russie et l'Ukraine. Les entreprises françaises craignent également une recrudescence des cyberattaques, en particulier celles liées à l'exploitation des terminaux distants, des accès Wi-Fi et des services cloud propres aux employeurs et aux employés. Tous ont vu leur utilisation augmenter fortement depuis mars 2020, date à laquelle les confinements COVID-19 ont débuté, selon l'étude de le CRA.

Il y a de bonnes raisons de redouter qu'un incident de sécurité ne se transforme en une violation de données : l'étude révèle que plus de 7 entreprises françaises sur 10 ont subi une telle brèche de sécurité au cours des 12 derniers mois. Il y a de fortes chances qu'il s'agisse d'une attaque par phishing, qui reste la plus commune en France. Les responsables et influenceurs du pays chargés de la cybersécurité ont reconnu que les menaces internes devenaient de plus en plus difficiles à gérer. « Il est impossible de savoir d'où le problème viendra, la menace interne est donc la plus difficile à anticiper », note une personne interrogée française.

Les entreprises françaises s'inquiètent de ne pas disposer de suffisamment de fonds et de personnel qualifié pour faire face à ce qu'elles considèrent comme les principales menaces pour l'année à venir : les fuites de données, les menaces internes, les attaques commanditées par des États et les attaques sur le cloud. La formation reste la priorité absolue, tout comme le recours à des outils de sécurité tels que le DNS et les flux réseau pour bloquer tout trafic suspect. Des formations plus poussées et des outils de sécurité plus performants pourraient s'avérer difficiles à instaurer, étant donné que le principal problème cité par les personnes interrogées en France est le manque de budget pour investir dans des dispositifs de cybersécurité plus performants au sein de leur entreprise.

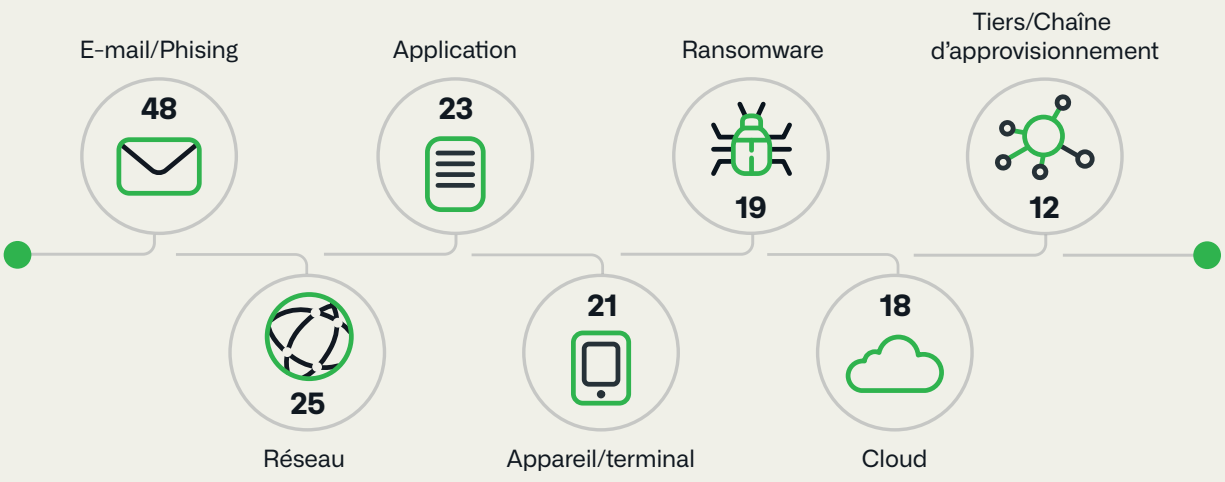
Les conclusions de l'étude 2022 auprès des personnes interrogées en France révèlent les tendances suivantes dans ce pays :

45 %

des entreprises françaises ont renforcé leur transformation numérique afin de soutenir les travailleurs à distance.

1. **Depuis le début de la pandémie de COVID-19, de nombreuses entreprises françaises ont renforcé leurs ressources réseau, accéléré leur transformation numérique pour soutenir les travailleurs à distance et embauché davantage de personnel informatique pour soutenir leur personnel et leurs clients.** Plus de la moitié (52 %) de toutes les personnes interrogées ont enrichi leurs réseaux et leurs bases de données, et 45 % ont accéléré leurs transformations numériques afin de soutenir les travailleurs à distance. 39 % d'entre eux ont embauché plus de personnel informatique, tandis que 32 % ont développé le support des portails clients pour favoriser l'engagement des clients à distance. En outre, 31 % ont réduit leur dépendance à l'égard des fournisseurs cloud tiers, tandis que 27 % ont transféré davantage d'applications vers des fournisseurs cloud tiers. Plus d'un quart (26 %) ont fermé des bureaux physiques et/ou concentré les contrôles de réseau et de sécurité sur la périphérie (comme le SASE, Secure Access Service Edge). Les mesures les moins courantes sont la réaffectation du personnel informatique à d'autres fonctions (22 %) et la réduction du personnel informatique (17 %).

France : nombre moyen de problèmes selon les différents vecteurs d'attaque



71 %

des personnes interrogées ont déclaré que leur entreprise avait ajouté des VPN ou des pare-feux

2x

plus d'entreprises françaises ont détecté au moins deux fois plus de problèmes résultant d'attaques par e-mail et/ou phishing que tout autre type d'attaque

2. **L'année dernière, une grande partie des entreprises françaises ont adopté des VPN, des pare-feux et des appareils mobiles distants appartenant à l'entreprise pour protéger leurs réseaux.** Près des trois quarts (71 %) des personnes interrogées ont déclaré que leur entreprise avait adopté des VPN ou des pare-feux, tandis que 43 % ont ajouté des appareils mobiles distants appartenant au réseau de l'entreprise, contre 36 % pour les appareils distants appartenant aux employés. Les kiosques intelligents ou les dispositifs similaires destinés à assister les clients à distance représentent 37 % des nouvelles fonctionnalités du réseau. Près d'un tiers (31 %) ont choisi d'ajouter à leurs réseaux des serveurs DNS-DHCP-IPAM gérés dans le cloud, appelés collectivement serveurs DDI, et presque autant (30 %) ont opté pour des serveurs DDI gérés en interne.

3. **Au cours des 12 prochains mois, les personnes interrogées en France ont déclaré que les risques de fuite de données, d'attaques par le biais des services cloud et de menaces internes seraient les plus préoccupants pour leur entreprise.** Les fuites de données (54 %) et les attaques directes par le biais des services cloud (37 %) restent les cybermenaces les plus problématiques, suivies des menaces internes (34 %) et des attaques exploitant les connexions des travailleurs à distance (32 %). Les ransomwares (27 %) et les attaques via l'IdO en réseau (21 %) ont été jugés plus préoccupants que les menaces avancées (18 %), la chaîne d'approvisionnement/les tiers (15 %) et les attaques commanditées par un État (9 %).

4. **Les personnes interrogées en France estiment que leur entreprise est moins bien armée contre les fuites de données, les menaces internes et les attaques commanditées par un État, ainsi que les attaques directes via les services cloud.** Les personnes interrogées ont déclaré qu'elles se sentaient moins disposées à défendre les réseaux de leur entreprise contre les fuites de données (25 %), les menaces internes (18 %) et les attaques commanditées par un État (16 %). Les possibilités d'une attaque directe par le biais d'un prestataire de services cloud et/ou d'une attaque via les connexions d'un travailleur à distance constituent également un problème pour 12 % des personnes interrogées. Le manque de ressources technologiques et humaines ainsi que la prévalence croissante des fuites de données, des menaces internes et des attaques commanditées par des États préoccupent les participants. « Mon entreprise sera moins bien armée pour se défendre parce que nous n'avons pas prévu de budget suffisant pour nous protéger », a noté un participant préoccupé par le risque de fuite de données.

5. **En moyenne, les entreprises françaises ont constaté au moins deux fois plus de problèmes résultant d'attaques par e-mail/phishing que tout autre type d'attaque, y compris les attaques visant des réseaux, des applications et des équipements/endpoints.** Les personnes interrogées ont estimé que leur entreprise avait détecté des problèmes résultant d'environ 48 attaques par e-mail/phishing au cours des 12 derniers mois, ainsi que 25 attaques visant les réseaux, 23 attaques visant les applications et 21 attaques visant les équipements/endpoints au cours de la même période.

7 participants français sur 10

Les personnes interrogées en France ont fait état d'une ou plusieurs violations de données de leur entreprise dues à des cyberattaques

6. **Près des trois quarts (72 %) des personnes interrogées en France ont fait état d'une ou plusieurs atteintes à leur entreprise dues à des cyberattaques, la plupart ayant pour origine le Wi-Fi, le cloud, des employés ou des terminaux distants appartenant à des employés.** Les points d'accès Wi-Fi ont été à l'origine de 40 % des brèches dans les entreprises des personnes interrogées au cours des 12 derniers mois, suivis par l'infrastructure ou les applications cloud (31 %), les employés et les ex employés (28 %) et les terminaux distants appartenant aux employés (26 %). Les terminaux distants appartenant à l'employeur ont été à l'origine de 24 % des brèches de sécurité, ainsi que les serveurs DNS, DHCP, IPAM ou autres serveurs de réseau non protégés.

7. **Le phishing était la méthode d'attaque la plus répandue contre les entreprises ayant fait l'objet d'une violation de données.** Le phishing a représenté 54 % des méthodes d'attaque au cours de l'année écoulée, suivi par les ransomwares (44 %) et les menaces persistantes avancées (APT) (40 %). La plupart des victimes de ces attaques ont déclaré que leurs agresseurs avaient le plus souvent recours à l'exfiltration de données (53 %), au détournement d'identifiants (46 %) et aux communications de commande et de contrôle (31 %).

8. **Au total, la valeur moyenne estimée des pertes subies par les entreprises françaises, à savoir les pertes financières directes et indirectes, le préjudice moral et les frais de restauration, résultant des attaques survenues au cours de l'année écoulée, s'élevait à environ 1,9 million d'euros au moment de l'étude.** Outre ces chiffres financiers, 21 % des entreprises françaises ont déclaré qu'une attaque avait entraîné des dommages corporels ou psychologiques, ce qui constitue le pourcentage le plus élevé parmi tous les pays étudiés. Dix-sept pour cent ont déclaré qu'une attaque avait entraîné la perte de vies humaines. Les entreprises victimes d'attaques ont surtout été victimes de manipulation de données (40 %), de pannes ou d'interruptions de système (35 %), d'exposition ou d'exfiltration de données sensibles ou de déni de service (DoS ou DDoS) (32 % chacun). Près d'un tiers (31 %) ont également fait part de confiscations de données imputables à des ransomwares.

9. **Les entreprises françaises ont recours à une multitude de contrôles pour protéger leurs actifs réseau dans des environnements sur site, cloud et hybrides (sur site et cloud).** Parmi les différents contrôles utilisés, les plus répandus sont les EDR pour les actifs sur site (39 %), le provisionnement et le déprovisionnement sécurisés (39 %) pour les environnements basés sur le cloud et le cryptage des données (44 %) pour les environnements hybrides.

« Je pense que de grandes menaces vont surgir et entraîner de très grandes pertes. »

Manager, fournisseur de technologie français

62 %

des entreprises mettront jusqu'à 24 heures pour enquêter sur une menace

10. **En moyenne, la plupart des entreprises (62 %) mettent jusqu'à 24 heures pour enquêter sur une menace, et beaucoup s'appuient sur les données de flux réseau.** Pour faciliter leurs enquêtes ou leurs recherches relatives aux menaces, les équipes de sécurité s'appuient sur les données de flux réseau (48 %), les requêtes et réponses DNS (38 %), les alertes de l'équipe d'intervention d'urgence informatique (CERT) (30 %) et les informations sur les vulnérabilités spécifiques à leurs systèmes (30 %).
11. **Le système de noms de domaine (DNS) fournit diverses mesures de sécurité pour protéger les organisations et est un élément clé dans presque toutes les stratégies de sécurité des organisations.** Les répondants ont indiqué que leur organisation utilise principalement le DNS dans sa stratégie pour aider à : se protéger contre les menaces telles que le tunneling DNS, l'exfiltration de données et les algorithmes de génération de domaine que d'autres outils de sécurité pourraient manquer (54 %) ; aider à détecter les activités des logiciels malveillants plus tôt dans la chaîne d'élimination (45 %) ; et les informer des appareils qui demandent à se connecter à des destinations malveillantes (43 %).
12. **Les principaux défis attendus en matière de protection contre les attaques concernent les budgets restreints et la capacité à surveiller les utilisateurs et les appareils sur leurs réseaux.** Les répondants français ont indiqué que leur entreprise était confrontée à un manque de fonds (33 %) et à un manque de visibilité de l'activité des utilisateurs et des appareils sur le réseau (30 %). Le contrôle de l'accès des travailleurs à distance et de pare-feux inadéquats ou obsolètes ont été cités par environ un quart des personnes interrogées. Un trop grand nombre d'alertes et des outils de sécurité disparates ont été évoqués par 23 % des personnes interrogées.

45 %

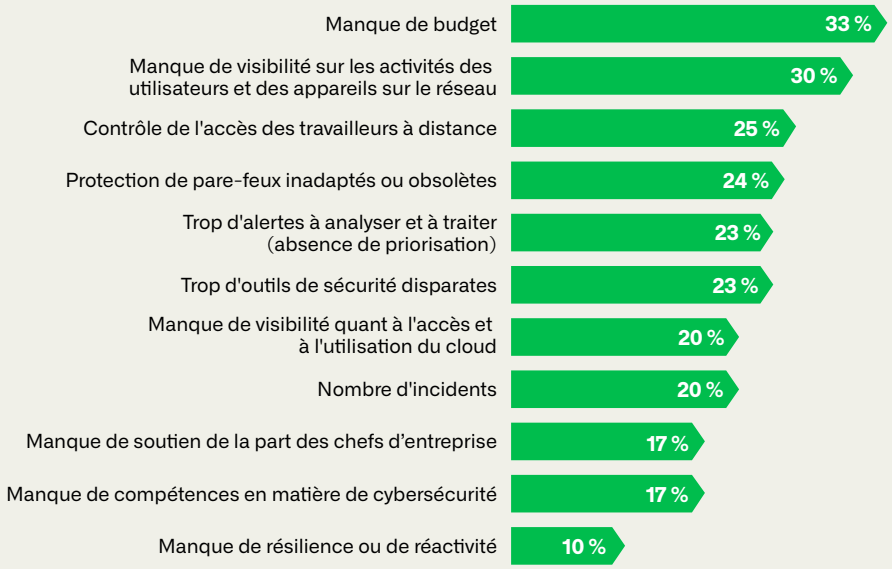
des entreprises françaises ont indiqué que leurs budgets consacrés à la sécurité informatique avaient augmenté en 2022

13. **Quarante-cinq pour cent des entreprises françaises ont indiqué que leurs budgets consacrés à la sécurité informatique avaient augmenté en 2022, et 55 % ont déclaré s'attendre à des budgets encore plus conséquents en 2023 afin de lutter contre les menaces connues et émergentes.** Par ailleurs, 13 % ne prévoient aucune modification de leurs budgets, tandis que 30 % tablent sur une diminution de leurs budgets l'année prochaine. Les personnes interrogées ont décrit divers types de menaces pressenties en 2023, parmi lesquelles les ransomwares et les « vols de données » occasionnés en interne, ainsi que les pressions économiques et environnementales. « Notre budget sera très largement tributaire de l'inflation future », a déclaré un ingénieur informatique pour un fabricant d'électronique.

14. **Les achats technologiques prévus les plus populaires sont le cryptage des données (36 %), la détection et la réponse aux terminaux (EDR) (34 %) et la sécurité du réseau (pare-feu, outils de prévention des intrusions, etc.) pour la protection sur site ; le Cloud Access Security Broker (CASB) (38 %), les passerelles web sécurisées (36 %) et l'EDR (32 %) pour les systèmes basés sur le cloud ; et les VPN/ contrôles d'accès (38 %), la sécurité du réseau (pare-feu, IPS, etc.) et l'approvisionnement et le déprovisionnement sécurisés (37 % chacun) pour les environnements hybrides.** Les principales mesures à prendre pour renforcer la protection des réseaux sont généralement le recrutement, la formation du personnel et la sécurité des données et du cloud.

15. **Les entreprises françaises ont délaissé leur stratégie de transformation numérique en 2021 pour privilégier les ressources allouées aux réseaux et aux bases de données en 2022 afin de soutenir leur personnel à distance pendant la pandémie.** En 2021, les préoccupations des personnes interrogées étaient principalement axées sur les fuites de données (55 %) et les attaques via les connexions des travailleurs à distance (52 %). Cependant, en 2022, en raison de la popularité croissante du cloud et de l'accélération de la migration vers celui-ci, les répondants étaient préoccupés par les risques de sécurité qui pesaient sur leurs environnements cloud, 37 % d'entre eux indiquant qu'il s'agissait de leur principale préoccupation après les fuites de données.

Quels sont les principaux défis que votre entreprise devra relever pour protéger son réseau contre les menaces ou les attaques au cours des 12 prochains mois ?



Sélectionnez jusqu'à trois réponses.

GAGNER EN COMPRÉHENSION

Ce rapport est basé sur des données nationales issues d'une enquête mondiale menée en ligne en juillet/août 2022. Un rapport mondial plus détaillé et un rapport régional pour l'Europe et les Émirats Arabes Unis sont disponibles sur le site d'Infoblox. Ils fournissent des informations supplémentaires sur les conclusions de l'enquête et offrent une perspective globale inestimable concernant les risques auxquels nous sommes tous confrontés, ainsi que les opinions d'autres experts en matière de technologie et de sécurité dans le monde entier.

infoblox.

Infoblox est l'entreprise qui associe réseau et sécurité pour offrir de meilleures performances et protection. Nous offrons une visibilité et un contrôle sur qui et ce qui se connecte à votre réseau et identifions les menaces via un DNS intelligent. Pour en savoir plus, rendez-vous sur https://www.infoblox.com.

Siège social
2390 Mission College Boulevard,
Ste. 501, Santa Clara, CA 95054

+1.408.986.4000
info@infoblox.com
www.infoblox.com

© 2023 Infoblox, Inc. Tous droits réservés. Le logo Infoblox et les autres marques apparaissant dans le présent document appartiennent à Infoblox, Inc.Toutes les autres marques sont la propriété de leur(s) propriétaire(s) respectif(s).