RAPPORT

Liberté, Égalité, Cybersécurité

La cybersécurité des 100 plus grandes entreprises françaises

SecurityScorecard

Introduction

Ce rapport présente une analyse de la cybersécurité des 100 plus grandes entreprises françaises par capitalisation boursière. Les entreprises ont été classées en fonction de divers facteurs, notamment la sécurité de leur réseau, les risques d'infections par des logiciels malveillants, la sécurité aux points d'entrée, la fréquence des correctifs, la sécurité des applications et l'intégrité du DNS.

Pour mesurer le risque cyber, SecurityScorecard attribue des notes standardisées de A à F, qui mesurent et valident en temps réel le niveau de sécurité des entreprises et de leur chaîne d'approvisionnement. La validation des scores de SecurityScorecard par analyse statistique montre que les entreprises ayant obtenu un F ont 13,8 fois plus de risques de subir une violation de données que les entreprises notées A.

PROBABILITÉ DE VIOLATION DE DONNÉES

Les entreprises ayant obtenu la note F ont

13,8 FOIS PLUS

de risques de subir une violation de données que les entreprises notées A.

Principales conclusions :

Si 60 % des entreprises de ce panel présentent une cybersécurité relativement forte, toutes sont en relation avec une entité ayant subi une violation de données. Un examen plus approfondi des données révèle que :

1. **91 %** des entreprises notées A n'ont pas été victimes d'une violation au cours des douze derniers mois.
2. **40 %** ont obtenu un C ou une note inférieure.
3. **7 %** ont été victimes d'une violation de données au cours des douze derniers mois.
4. **98 %** sont en relation avec un tiers ayant subi une violation de données.
5. **100 %** sont en relation avec une quatrième partie ayant subi une violation de données.
6. Les entreprises du **secteur des services sont les moins bien notées**, 79 % ayant obtenu une note globale C ou inférieure.
7. **L'énergie est le secteur le plus robuste en France** avec seulement 29 % des entreprises ayant obtenu un C ou une note inférieure. Néanmoins, 14 % d'entre elles ont été victimes d'une violation de données directe.

Note	Risque de violation
A	x1
B	x2,9
C	x5,4
D	x9,2
F	x13,8

Le coût moyen d'une violation de données s'élève à 4,2 millions d'euros.

IBM Security,
Rapport 2023 sur le coût d'une violation de données

Paysage des menaces de cybersécurité des 100 plus grandes entreprises françaises

Les menaces qui pèsent sur la chaîne d'approvisionnement, les attaques étatiques, le télétravail et l'élargissement de la surface d'attaque contribuent à rendre le paysage numérique de plus en plus vulnérable, une faiblesse que des acteurs malveillants cherchent constamment à exploiter. Ces attaquants connaissent bien les vulnérabilités des entreprises, d'où l'importance pour ces dernières d'évaluer et d'appréhender régulièrement leur sécurité du point de vue d'un hacker.

Le récent rapport de SecurityScorecard Global Third-Party Cyber Breach Report a révélé qu'au niveau mondial, le groupe de cybercriminalité C10p était responsable d'une part importante des violations imputables à des tiers. En effet, en exploitant massivement une vulnérabilité zero-day dans le logiciel de transfert de fichiers MOVEit, le groupe C10p a largement contribué à l'augmentation en 2023 du nombre de violations de données liées à des tiers.

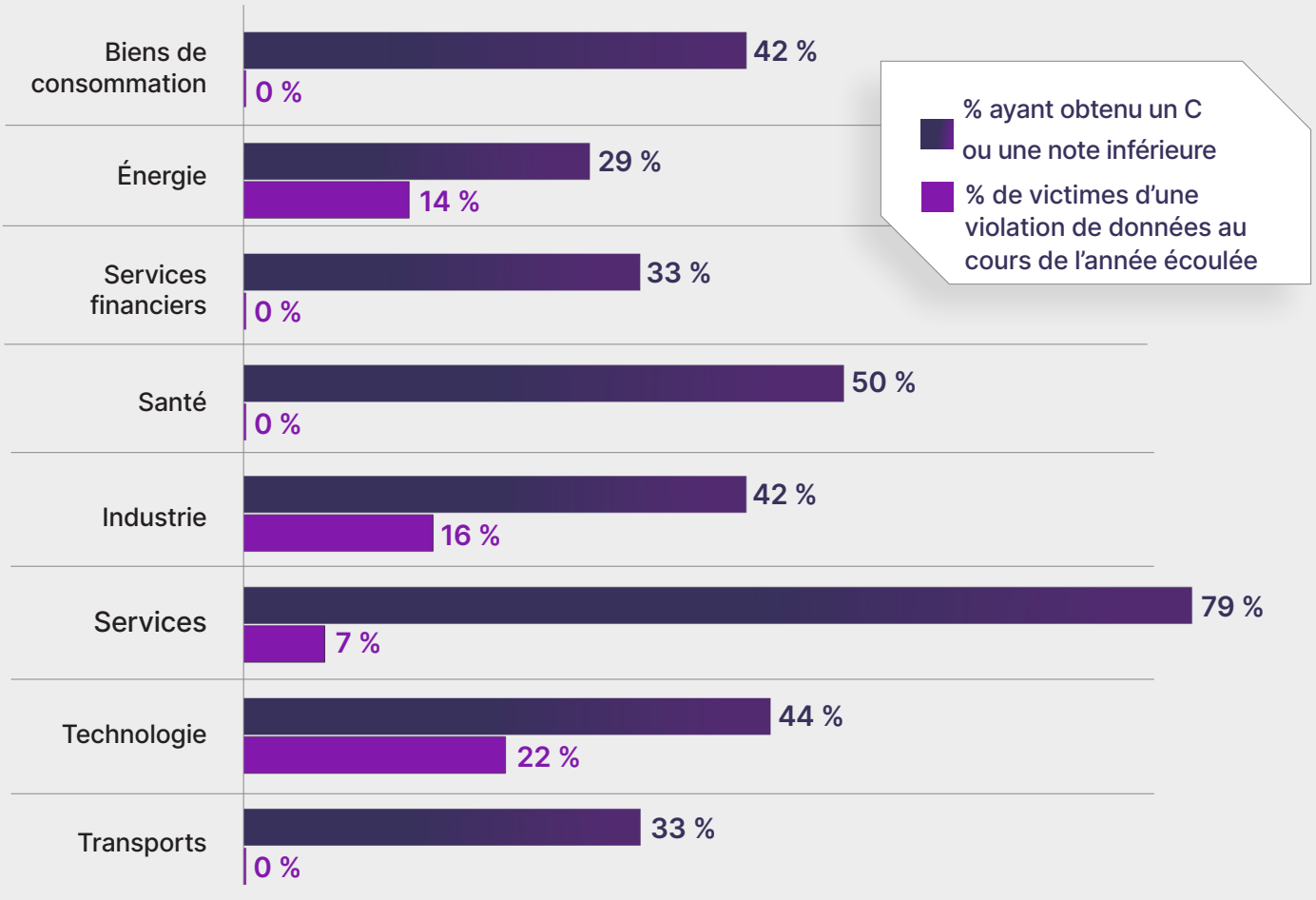
Résultats

Score global

1. **24 %** des entreprises ont obtenu un A, la note la plus élevée en matière de cybersécurité
2. **36 %** ont obtenu un B
3. **27 %** ont obtenu un C
4. **13 %** ont reçu une note défavorable (D ou F)

Cette analyse des 100 plus grandes entreprises françaises par capitalisation boursière met en évidence des axes concrets d'amélioration. Ce rapport a examiné les entreprises des secteurs suivants : finance, technologie, services, services publics, luxe, transports et communication.

Scores par secteur



Comparaison des scores par pays

Avec l'interconnexion de notre monde numérique, la cybersécurité dépasse désormais les frontières nationales pour devenir un enjeu global. Il est donc indispensable que les gouvernements, les secteurs d'activité et les entreprises collaborent pour garantir une cyber résilience collective.

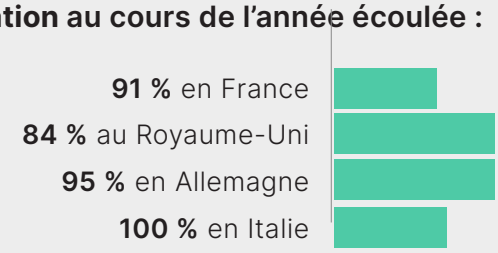
Bien que cette analyse soit principalement axée sur les entreprises françaises, elle englobe également des données similaires issues de grandes entreprises italiennes, allemandes et britanniques. Ces données montrent notamment que les entreprises britanniques ont la cybersécurité globale la plus solide (seulement 24 % ont un C ou une note inférieure) par rapport à leurs homologues françaises, italiennes et allemandes, avec respectivement 40 %, 41 % et 34 % ayant obtenu un C ou une note inférieure.

Par ailleurs, la France a le taux le plus élevé de violations de données subies par des tierces et quatrièmes parties (98 % et 100 %, respectivement) par rapport au Royaume-Uni, à l'Allemagne et à l'Italie.

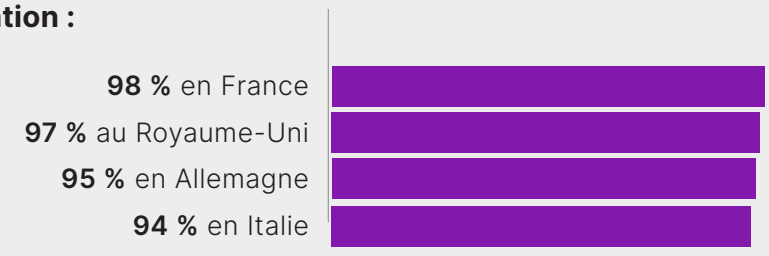
Autres informations par pays

Entreprises qui ont été victimes d'une violation de données au cours des douze derniers mois :

Entreprises notées A qui n'ont pas été victimes d'une violation au cours de l'année écoulée :



Entreprises en relation avec une tierce partie ayant subi une violation :



« Il est clair que les entreprises étudiées dans ce rapport ont tout intérêt à intégrer la gestion des risques liés aux tiers non seulement à leur stratégie de sécurité, mais aussi à leur processus de sélection des fournisseurs.

La France est déjà à l'avant-garde de la cybersécurité en Europe, mais ces entreprises et organisations doivent dès maintenant intensifier leureffort si elles veulent être prêtes pour l'entrée en vigueur du règlement sur la résilience opérationnelle numérique (DORA) en janvier 2025.

La solution proposée par SecurityScorecard simplifie et améliore cette démarche en offrant un système de notation pour évaluer les fournisseurs potentiels tout en permettant le suivi et l'incitation à la responsabilité des fournisseurs. »

Nadji Raib, directeur principal Europe du Sud

Les risques liés à la chaîne d'approvisionnement dépassent les tierces parties

Bien que l'attention se concentre habituellement sur les tierces parties dans l'examen de la chaîne d'approvisionnement, les fournisseurs de quatrième niveau constituent aussi un risque considérable.

Ce rapport montre que 98 % des entreprises du panel ont un lien avec une entité tierce ayant subi une violation. Ce chiffre rejoint les résultats de notre étude menée conjointement avec l'Institut Cyentia, qui a révélé que 98 % des entreprises sont en relation avec au moins une tierce partie qui a été victime d'une violation de données au cours des deux dernières années. Ce rapport montre également que 100 % des plus grandes entreprises françaises sont en relation avec une quatrième partie ayant subi une violation de données. Cette statistique souligne l'importance d'identifier et d'évaluer le niveau de sécurité de toutes les Nièmes parties de l'écosystème numérique de l'entreprise.

Plusieurs des entreprises analysées dans ce rapport sont de grandes holdings détenant des filiales dans différents secteurs. Nombre de ces secteurs (tels que les télécommunications, la santé, les services financiers, l'énergie et la technologie) sont interconnectés. Cela engendre une matrice complexe de dépendances mutuelles en matière de risques, face à laquelle les responsables politiques et les cadres d'entreprises à travers le monde cherchent à intervenir, en élaborant des lois, des directives et des approches de gestion des risques.

Dans le secteur financier en particulier, le Fonds Monétaire International a noté que la dépendance à l'égard de fournisseurs de services tiers communs signifie que les attaques ont une probabilité plus élevée d'avoir des implications systémiques et pourraient rendre des secteurs entiers vulnérables. Les entités financières de l'Union européenne se préparent d'ailleurs pour le règlement sur la résilience opérationnelle numérique (DORA), qui renforcera la cyber résilience et les chaînes d'approvisionnement numériques des établissements de crédit, des entreprises d'investissement, des assureurs, etc.

Corrélation entre la cyber résilience et la capitalisation boursière et le PIB

Une analyse plus poussée des données montre que les entreprises à plus forte capitalisation boursière font généralement preuve d'un meilleur niveau de cybersécurité. Par exemple, seuls 14 % des entreprises dont la capitalisation boursière est supérieure à 100 milliards de dollars obtiennent un C ou une note inférieure. **Conclusion : plus la capitalisation boursière est élevée, plus la probabilité d'obtenir un C est faible.**

Autres informations liées au chiffre d'affaires :

De 100 à 50 milliards de dollars

C ou moins : 29 %

De 50 à 10 milliards de dollars

C ou moins : 62 %

Moins de 10 milliards de dollars

C ou moins : 33 %

Ces conclusions rejoignent celles des études récentes menées par SecurityScorecard, qui ont mis en évidence une forte corrélation entre l'exposition d'un pays aux risques cyber et son PIB. En janvier de cette année, lors de la réunion annuelle du Forum économique mondial à Davos, SecurityScorecard a présenté son tableau de bord de la cyber résilience, qui a révélé que la prospérité économique d'un pays est étroitement liée à sa capacité à naviguer dans le paysage complexe des menaces cyber.

Selon le rapport, le Moyen-Orient, l'Amérique du Nord, le Pacifique, ainsi que l'Europe du Nord, l'Europe occidentale et l'Europe centrale affichent les scores de sécurité les plus élevés au monde. En d'autres termes, les régions dont le PIB par habitant est plus élevé tendent à présenter une meilleure maîtrise de la cybersécurité et un risque cyber moindre. La France (et d'autres pays d'Europe) ayant l'un des PIB par habitant les plus élevés, est sans doute mieux équipée pour investir dans des infrastructures résilientes et sûres, mais aussi pour mettre en œuvre et gérer des programmes de sécurité actifs afin de lutter contre des menaces cyber en perpétuelle mutation. Les pays riches comme la France sont peut-être aussi plus enclins à utiliser des logiciels régulièrement mis à jour avec des correctifs de sécurité.

Sécuriser les infrastructures critiques est essentiel

40 % des entreprises étudiées dans ce rapport représentent des secteurs stratégiques : énergie, télécommunications, transports, industrie et santé. Pour que la société fonctionne sans heurts, le public doit avoir confiance dans la sûreté de ces services et institutions. Les recommandations ci-dessous pourraient profiter aux entreprises de ces secteurs. Pour plus de conseils et de bonnes pratiques, consultez le rapport 2023 de SecurityScorecard, « Addressing the Trust Deficit in Critical Infrastructure » (en anglais).

Recommandations

Pour de nombreuses entreprises françaises, améliorer l'hygiène en cybersécurité devrait être une priorité absolue. Bien que la majorité des entreprises aient reçu des notes de cybersécurité élevées, presque toutes ont subi une violation de données de la part d'une tierce partie, et toutes ont subi une violation de la part d'une quatrième partie. Pour atténuer les risques et améliorer la posture globale de cybersécurité, nous recommandons les actions suivantes :

Concentrez-vous sur la sécurité des applications et des réseaux : toutes les entreprises devraient prioriser l'amélioration de la sécurité des applications et des réseaux. Ces deux aspects sont fondamentaux pour se prémunir contre un large éventail de menaces cyber.

Entreprises à haut risque : 40 % des entreprises ont une note de cybersécurité égale ou inférieure à C et doivent réagir sans plus attendre. Outre l'amélioration de la sécurité de leurs applications et de leurs réseaux, ces entreprises à haut risque doivent mettre l'accent sur les points suivants :

- **INTÉGRITÉ DU DNS.** Assurez la santé et l'intégrité de vos configurations du Système de Noms de Domaine (DNS). Une mauvaise configuration de ce composant critique peut être une source de vulnérabilités.
- **SÉCURITÉ DES TERMINAUX.** Renforcez la sécurité de tous les terminaux, notamment des ordinateurs portables, ordinateurs de bureau, appareils mobiles et appareils informatiques personnels (BYOD). Il est essentiel d'identifier et de corriger les vulnérabilités liées.
- **FRÉQUENCE DES CORRECTIFS.** Mettez en place un programme de gestion des correctifs pour vos systèmes, vos logiciels et votre matériel. Des mises à jour fréquentes permettent d'atténuer les vulnérabilités connues.

Quel que soit le score obtenu, toutes les entreprises doivent connaître non seulement leur note, mais aussi les facteurs qui l'influencent. Les entreprises peuvent demander gratuitement à SecurityScorecard un rapport détaillé sur leur score.

Conclusion

Confiance et transparence sont les maîtres-mots en matière de cybersécurité. Pourtant, de nombreuses entreprises peinent à évaluer avec précision leur cybersécurité. Or, le présent rapport témoigne de l'importance de ces principes.

L'évaluation de la cybersécurité est un processus continu. Les notations de sécurité donnent aux responsables de la cybersécurité les informations dont ils ont besoin pour prendre des décisions éclairées, renforcer le niveau de sécurité de leur entreprise et favoriser la collaboration face à un risque croissant.

Face à l'évolution des menaces, les solutions de notation de la sécurité et de surveillance des tiers constituent un engagement en faveur de la cybersécurité. Nous sommes convaincus que toutes les entreprises de notre panel peuvent devenir cyber résilientes et contribuer à un monde plus sûr et plus collaboratif.

Méthodologie

Les menaces sont en perpétuelle évolution, il est donc indispensable de mettre en place une évaluation en temps réel. Les risques cyber doivent être évalués sur la base de données. SecurityScorecard recueille des quantités considérables de données de façon non intrusive sur l'hygiène cyber des entreprises du monde entier. Ces données nous permettent d'évaluer les défenses des entreprises contre les menaces cyber. Nous attribuons un score global (de A à F) sur la base de dix facteurs prédictifs d'une violation de la sécurité.

Période d'analyse :
Le rapport étudie le niveau de cybersécurité des 100 plus grandes entreprises françaises en termes de capitalisation boursière entre le 13 mars 2023 et 13 mars 2024.

Annexe

En quoi consistent les notations de sécurité ?

SecurityScorecard fournit aux entreprises une vue d'ensemble de leur niveau de sécurité, y compris les risques liés aux tierces et quatrièmes parties.

Les notations de sécurité reposent entièrement sur des faits ; tout est noté sur la base d'une observation sous-jacente et transparente, fondée sur des analyses de l'ensemble de l'IPv4 mondial. En corrélation avec les données d'incidence, les facteurs de SecurityScorecard fournissent des informations qui guident les entreprises sur la stratégie à adopter pour réduire leur exposition aux risques. Voici ces dix facteurs :

La sécurité du réseau vérifie les ports ouverts (tels que SMB et RDP), les certificats SSL non sécurisés ou mal configurés, les vulnérabilités des bases de données et les vulnérabilités IoT.

L'intégrité du DNS vérifie les mauvaises configurations, telles que les Resolvers ouverts, ainsi que les configurations recommandées pour DNSSEC, SPF, DKIM et DMARC.

La fréquence des correctifs mesure la fréquence des mises à jour des services, logiciels et matériels identifiés au sein d'une entreprise.

La sécurité des terminaux mesure les versions et l'exploitabilité des ordinateurs portables, ordinateurs de bureau, appareils mobiles et appareils BYOD qui accèdent aux réseaux de l'entreprise.

Les signaux liés à la réputation IP sont collectés par le système sinkhole de SecurityScorecard, qui ingère des millions de signaux de logiciels malveillants provenant d'infrastructures de commande et contrôle (C2) du monde entier. Les adresses IP infectées identifiées sont mises en correspondance avec les entreprises concernées.

Les échanges entre hackers sont recueillis sur des sites Web illégaux et le dark Web où ils discutent des entreprises et des adresses IP ciblées.

Les fuites d'informations sont des informations d'identification compromises qui ont été exposées dans le cadre d'une violation ou d'une fuite de données, de vidages de keylogger, de vidages de pastebin, de vidages de bases de données et d'autres référentiels d'informations.

L'ingénierie sociale consiste à mesurer l'utilisation de comptes d'entreprise sur les réseaux sociaux, les comptes financiers et les listes marketing.

Les scores Cubit sont calculés à l'aide de l'algorithme de menace exclusif de SecurityScorecard qui mesure un ensemble de problèmes critiques de sécurité et de configuration, tels que les panneaux de commande administratifs exposés.

Pour en savoir plus et créer votre compte gratuit, rendez-vous sur SecurityScorecard.com.

À PROPOS DE SECURITYSCORECARD

Financée par des investisseurs de premier rang tels qu'Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital et bien d'autres, SecurityScorecard est le leader mondial dans l'évaluation, la réponse et la résilience en matière de cybersécurité, avec plus de 12 millions d'entreprises évaluées en permanence.

Fondée en 2013 par Aleksandr Yampolskiy et Sam Kassoumeh, experts en sécurité et en gestion des risques, SecurityScorecard propose une technologie de notation brevetée qui est utilisée par plus de 25 000 organisations pour la gestion des risques d'entreprise, la gestion des risques liés aux tiers, le reporting destiné aux dirigeants, la diligence raisonnable, la souscription de cyber-assurances et la surveillance réglementaire.

SecurityScorecard contribue à rendre le monde plus sûr en transformant la manière dont les entreprises appréhendent les risques de cybersécurité, les traitent et communiquent à leur sujet auprès de leurs conseils d'administration, de leurs employés et de leurs fournisseurs. SecurityScorecard a obtenu la certification FedRAMP, programme fédéral américain de gestion des risques et des autorisations, ce qui témoigne des normes de sécurité robustes qu'elle déploie pour protéger les informations de ses clients. Par ailleurs, sa solution est répertoriée comme outil et service de cybersécurité gratuit par l'Agence de cybersécurité et de sécurité des infrastructures (CISA). Chaque entreprise dispose du droit universel à recevoir sa notation fiable et transparente SecurityScorecard. Pour plus d'informations, rendez-vous sur securityscorecard.com ou suivez-nous sur LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io