

cyber**vadis**

Rapport CyberVadis 2021

**Cybersécurité de la supply chain :
5 défis clés à relever**

Introduction

En raison du nombre croissant de cyberattaques, toujours plus complexes, dans un contexte de pandémie, les organisations doivent faire face à de nouveaux défis en matière de cybersécurité.

À cela s'ajoutent l'instauration du télétravail et le recours aux outils numériques. Une question nous vient alors à l'esprit :



Sommes-nous
prêts à faire face
aux défis existants
et à venir
en matière
de cybersécurité ?



Cette étude porte sur les cinq thématiques suivantes :

Protection des données et RGPD

Gestion des accès

Sécurité du cloud

Détection et réponse aux incidents

Continuité d'activité et gestion de crise

Dans le cadre de cette étude, nous avons analysé les résultats d'évaluation de 1 289 entreprises de différentes tailles, de différents secteurs d'activité et issues de 67 pays.

Nos analystes CyberVadis ont évalué les contrôles de sécurité que les entreprises évaluées déclarent opérer sur la base des preuves fournies.



Protection des données et RGPD

Contexte et auto-évaluation

Le nombre de cyberattaques ciblant les données personnelles augmente à une vitesse fulgurante. Il est donc désormais obligatoire d'établir un processus de protection des données sophistiqué.

80 % des violations impliquaient des données à caractère personnel)¹

En 2020, il y a eu une hausse de

40 % d'amendes infligées pour non-respect du RGPD²

Les entreprises doivent faire face à un autre défi majeur : mettre en place un solide processus de protection des données pour garantir la conformité avec la législation et la réglementation en vigueur.

¹ Rapport 2020 sur le coût d'une violation des données, Ponemon Institute & IBM

² Enquête 2020 sur la violation des données selon le RGPD, DLA Piper

Analyse de CyberVadis des entreprises évaluées



Gouvernance et conformité

29 % d'entre elles ont évalué les risques liés à une éventuelle non-conformité avec la réglementation relative à la protection des données personnelles



Droits des personnes concernées

57 % d'entre elles ont désigné une personne en charge de l'exercice des droits des individus



Sensibilisation

49 % d'entre elles forment leurs employés aux bonnes pratiques en matière de protection des données personnelles



Gestion de la sous-traitance

22 % d'entre elles se sont assurées que les processus d'achat prévoient un contrôle de conformité lié à la protection des données personnelles



Gestion des accès

Contexte et auto-évaluation

La crise du Covid-19 a contraint la plupart des organisations à opter pour le télétravail.

62 % des entreprises évaluées ont déclaré autoriser l'accès à distance à leurs systèmes³.

Parallèlement, la menace en interne est en croissance.

60 % des entreprises ont déclaré subir plus de 30 incidents par an dus à une menace interne⁴.

Ces faits démontrent l'importance d'établir des stratégies d'accès plus efficaces. Il devient primordial d'adopter des pratiques d'authentification avancées pour faire face à ce risque grandissant de menaces d'initié.

³ Données CyberVadis recueillies selon les déclarations des entreprises

⁴ Rapport mondial 2020 sur le coût des menaces d'initié, Ponemon Institute

Analyse de CyberVadis des entreprises évaluées



Contrôle des accès à distance

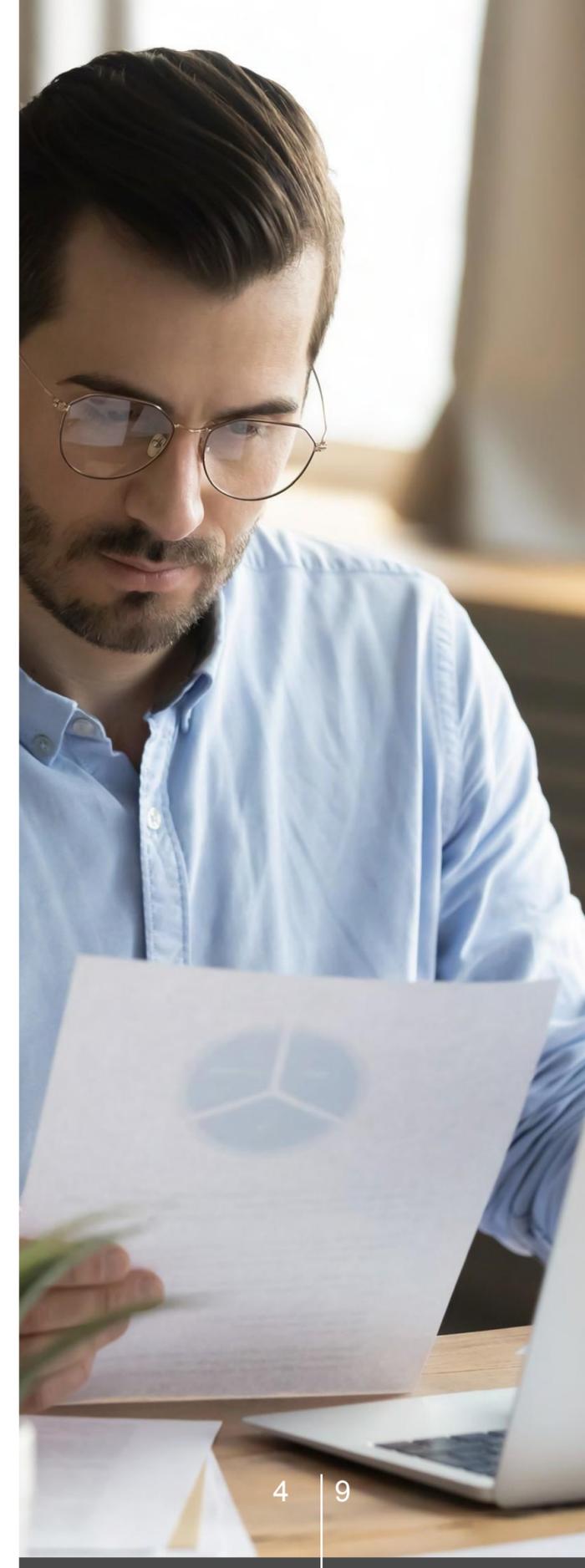
44 % d'entre elles ont déployé une solution d'accès à distance sécurisée.



Des méthodes d'authentification avancées

37 % d'entre elles ont mis en place des méthodes d'authentification avancées pour les comptes à privilèges.

25 % d'entre elles ont encadré la gestion des accès des tiers à leur système d'information.



Sécurité du cloud

Contexte et auto-évaluation

En raison de la pandémie, les entreprises se tournent de plus en plus vers les solutions cloud pour stocker leurs données.

Selon le rapport 2020 de CyberVadis,

81 % des entreprises ont déclaré utiliser un système cloud⁵.

Selon le NIST, en plus des approches sur site traditionnelles, le cloud offre un libre accès sur demande, un réseau à bande passante élevée, le partage des ressources, une élasticité de l'offre ou encore des services mesurés.

Néanmoins, il présente des risques spécifiques qui doivent être pris en compte, car

19 % des attaques malveillantes étaient dues à des clouds mal configurés⁶.

Analyse de CyberVadis des entreprises évaluées



Contrôles propres au cloud

26 % d'entre elles gèrent les risques relatifs à leur prestataire de service cloud.

34 % d'entre elles s'assurent que leur prestataire de services a mis en place un plan de continuité d'activité..

30 % d'entre elles s'assurent que leur prestataire de service cloud a mis en place un processus de réponse aux incidents.

⁵Données CyberVadis recueillies selon les déclarations des entreprises

⁶Rapport 2020 sur le coût d'une violation des données, Ponemon Institute & IBM



Détection et réponse aux incidents

Contexte et auto-évaluation

Aujourd'hui, les organisations doivent mettre en place un solide processus de détection et de réponse aux incidents pour identifier et maîtriser les cyberattaques le plus précocement possible.

Cela est primordial, car en 2020,

52 % des violations ont été provoquées par des attaques malveillantes, soit une augmentation de 10 % par rapport à 2014⁷.

Les entreprises doivent intégrer à leur processus de gestion des incidents un processus des enseignements tirés pour les aider à identifier la cause des incidents et empêcher ou limiter la probabilité qu'un problème similaire ne survienne à l'avenir.

⁷Rapport 2020 sur le coût d'une violation des données, Ponemon Institute & IBM

⁸Ce contrôle a uniquement été évalué chez les grandes entreprises (> 300 ETP) et les petites entreprises (> 50 ETP) œuvrant dans des secteurs particulièrement critiques

Analyse de CyberVadis des entreprises évaluées



75 % d'entre elles ont préparé un processus de gestion des incidents.

32 %⁸ d'entre elles ont déployé un processus de gestion de l'information et des événements de sécurité (SIEM).



32 % d'entre elles ont établi un processus relatif aux enseignements tirés pour identifier les causes des incidents et éviter qu'ils ne se reproduisent.

Continuité d'activité et gestion de crise

Contexte et auto-évaluation

La pandémie de COVID-19 a révélé l'importance d'anticiper les événements imprévus et de mettre en place des mesures pour maîtriser les situations de crise. Ainsi,

95 % des chefs d'entreprise ont indiqué que leur processus de gestion de crise méritait d'être amélioré⁹.

L'un des aspects clés d'un processus de gestion de crise réussi est de s'assurer que l'équipe dédiée est correctement formée et préparée à réagir rapidement si un événement majeur se produit.

L'équipe de gestion de crise doit orchestrer le déclenchement du plan de continuité d'activité (PCA) qui contribue à la résilience de l'entreprise.

⁹ Global crisis survey 2021, PwC

¹⁰ Ce contrôle a uniquement été évalué chez les grandes entreprises (> 300 ETP) et les petites entreprises (> 50 ETP) œuvrant dans des secteurs particulièrement critiques

Analyse de CyberVadis des entreprises évaluées



Processus de continuité d'activité

44 % d'entre elles ont mis en place un plan de continuité d'activité (PCA).

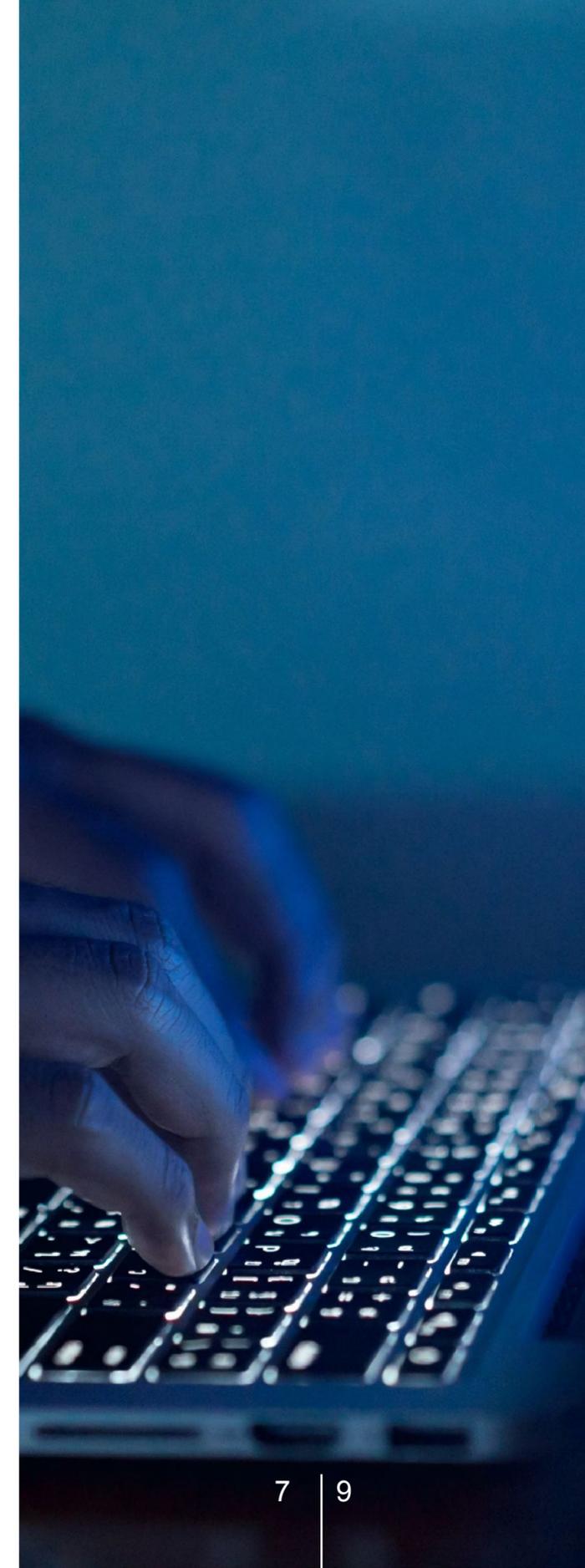
22 % d'entre elles testent leur plan de continuité d'activité (PCA) de façon périodique.



Gestion de crise

24 %¹⁰ d'entre elles ont établi un processus de gestion de crise.

4 % d'entre elles réalisent des exercices de simulation périodiques.



A propos de CyberVadis

CyberVadis propose aux entreprises une solution évolutive et économique pour évaluer les risques en matière de cybersécurité de leurs tiers. Notre méthodologie respecte toutes les principales normes de conformité internationales, et notamment le cadre de cybersécurité du NIST, la norme ISO 27001, le RGPD et plusieurs autres cadres spécifiques aux entreprises.

La solution de CyberVadis associe la vitesse d'automatisation à la précision et l'efficacité d'une équipe d'experts. Nous nous engageons directement avec les fournisseurs du monde entier. Une fois l'évaluation terminée, notre équipe interne d'analystes en sécurité vérifie les questionnaires et les preuves fournies et attribue une note de cybersécurité standardisée que les entreprises évaluées peuvent partager avec d'autres clients et partenaires via notre plateforme. Nous fournissons également un plan d'amélioration détaillé pour leur permettre d'augmenter leur note et de travailler en ligne avec leurs clients sur la mise en place de bonnes pratiques.

Cette étude a été réalisée par:



Marta Figueroa,

Responsable cybersécurité chez CyberVadis



Irene Grau,

Analyste principale en sécurité de l'information
chez CyberVadis

**Pour plus d'information veuillez nous
contacter: info@cybervadis.com**



www.cybervadis.com

Nous suivre:

