VARONIS

RAPPORT 2021 SUR LES RISQUES LIÉS AUX DONNÉES

INDUSTRIE

Plus de **six millions** de fichiers sont ouverts à tous les employés, un rayon d'exposition surprenant qui met en péril ces informations en raison des ransomwares et des menaces internes.

TABLE DES MATIÈRES

VARONIS

À PROPOS DU RAPPORT

Le *rapport 2021 sur les risques liés aux données dans le secteur industriel* est le troisième numéro de notre série de rapports annuels visant à analyser les menaces, les tendances et les solutions spécifiques à chaque secteur d'activité.

Ce rapport s'intéresse aux menaces croissantes auxquelles font face les industriels et les sociétés d'ingénierie en matière de cybersécurité. Ces résultats se basent sur l'analyse de quatre milliards de fichiers dans 50 entreprises.

Un grand nombre de nos résultats sont par ailleurs détaillés par taille d'entreprise :

1. **Petites entreprises :** 0 à 500 employés
2. **Moyennes entreprises :** 501 à 1 500 employés
3. **Grandes entreprises :** plus de 1 501 employés

L'objectif de ce rapport est d'aider les industriels à évaluer objectivement le domaine de la cybersécurité d'aujourd'hui et de leur fournir des conseils leur permettant de réduire leur surface d'attaque.

Rapport établi sur la base de l'analyse de **4 milliards de fichiers** dans **50 entreprises industrielles**

Fabricants industriels

Sociétés d'ingénierie

VARONIS

RÉSULTATS CLÉS

Des menaces continuent de peser sur le secteur industriel. Celles-ci peuvent provenir des grands groupes de ransomwares qui dérobent puis chiffrent les données de leur victime, sans parler des hackers issus de certains États-nations qui recherchent des secrets technologiques ou encore des employés internes qui cherchent à mettre la main sur des informations pour les vendre au plus offrant. Les récentes actualités nous révèlent les effets catastrophiques des attaques de ransomware, qui peuvent interrompre les chaînes d'assemblage et perturber les chaînes d'approvisionnement.

La surexposition des informations, en particulier des données sensibles, augmente les risques de manière exponentielle. Celles-ci forment ce que nous appelons votre « rayon d'exposition ». Imaginez les dégâts que pourraient faire les hackers s'ils parvenaient à pénétrer dans votre environnement. Il suffit qu'un employé clique sur un e-mail d'hameçonnage pour qu'un pirate puisse accéder à tous les fichiers auxquels cet utilisateur a accès. Lorsqu'une personne interne à l'entreprise a des intentions malveillantes, elle peut prendre son temps et s'emparer de précieuses informations pour en retirer un bénéfice personnel.

Nous avons cherché à comprendre dans quelle mesure le secteur industriel protège ses informations sensibles contre ces menaces toujours plus sophistiquées.

Nous avons constaté que **six millions de fichiers en moyenne sont ouverts à tous les employés, et ce dès leur premier jour de travail.**[1] Nous avons également observé que, en moyenne, plus de **27 000 fichiers sensibles** sont ouverts à l'ensemble des effectifs d'une entreprise.

[1] Dans ce rapport, l'expression « tout le monde » fait référence à tous les employés de l'organisation en question.

VARONIS

Secteur industriel
Données à risque : principales conclusions

En moyenne, chaque employé a accès à **six millions de fichiers**, et notamment à des informations appartenant à l'entreprise.

En moyenne, **plus de 27 000 fichiers sensibles** (données financières, secrets commerciaux, plans de développement) sont ouverts à tout le monde.

4 entreprises sur 10 ont plus de **1 000 fichiers sensibles** accessibles **à tous les employés.**

Plus de la moitié des entreprises ont **plus de 500 comptes avec des mots de passe qui n'expirent jamais.**

RÉSULTATS GÉNÉRAUX

Les grandes entreprises sont deux fois plus exposées

Exposition des entreprises en fonction de leur taille

Taille de l'organisation	Nombre moyen de fichiers	Nombre moyen de fichiers accessibles à tous	Pourcentage moyen de fichiers accessibles à tous
Grandes entreprises	63 571 806	12 303 704	19 %
Moyenne	21 920 382	3 776 187	17 %
Petites entreprises	12 347 728	2 212 460	18 %
Moyenne du secteur	**33 975 882**	**6 331 523**	**18 %**

Taille de l'organisation	Nombre moyen de dossiers	Nombre moyen de dossiers accessibles à tous	% moyen de dossiers accessibles à tous
Grandes entreprises	6 173 686	1 152 954	19 %
Moyenne	1 974 167	308 329	16 %
Petites entreprises	1 244 511	218 620	18 %
Moyenne du secteur	**3 241 479**	**575 766**	**18 %**

Taille de l'organisation	Nombre moyen de fichiers sensibles	Nombre moyen de fichiers sensibles accessibles à tous	% moyen de fichiers sensibles accessibles à tous
Grandes entreprises	310 014	39 122	13 %
Moyenne	232 305	19 958	9 %
Petites entreprises	166 051	23 684	14 %
Moyenne du secteur	**244 150**	**27 293**	**10 %**

En moyenne, chaque employé a accès à plus de six millions de fichiers, soit près d'un fichier sur cinq, dès son premier jour de travail. Dans les grandes entreprises, ce chiffre est multiplié par deux : dans les organisations qui emploient plus de 1 500 personnes, les employés peuvent accéder à plus de 12 millions de fichiers.

Le fait qu'un fichier sur dix soit ouvert à tous les membres de l'entreprise est très risqué. Ces fichiers peuvent inclure des documents relatifs à la propriété intellectuelle, les données des employés, des informations relatives à la fabrication, à la chaîne logistique et au développement de produits, aux plans marketing… Chez les industriels, le nombre de fichiers ouverts à tous est moins important que dans les entreprises de services financiers, dans lesquelles l'employé moyen peut accéder à 11 millions de fichiers.

RÉSULTATS GÉNÉRAUX

État des données par téraoctet : secteur industriel

Taille de l'organisation	Fichiers	Dossiers	Dossiers exposés	Fichiers sensibles	Dossiers disposant de droits uniques	Fichiers sensibles exposés	Fichiers sensibles obsolètes	Identifiants sécurisés non résolus	Dossiers dont les droits sont incohérents	Nombre de rapports	To analysés par entreprise
Grandes entreprises	1 654 486	112 973	11 772	11 58	9 460	1 739	8 506	561	375	17	86
Moyenne	1 073 643	103 425	26 529	21 781	8 112	2 102	12 551	1 079	250	22	19
Petites entreprises	1 291 091	134 830	18 143	5 236	15 322	721	4 217	482	689	11	13
Moyenne	**1 318 968**	**113 581**	**19 667**	**14 665**	**10 157**	**1 675**	**9 342**	**772**	**389**	**50**	**40**

L'évaluation du risque par téraoctet de données permet de faire apparaître une image plus nette de la surface d'attaque classique d'une entreprise en fonction de sa taille et met en lumière celles qui sont les plus vulnérables aux menaces internes et externes. En moyenne, un téraoctet représente 1,3 million de fichiers.

Nous avons constaté que, pour chaque téraoctet, les industriels comptent **en moyenne près de 20 000 dossiers exposés (ouverts à tous)**. Ce nombre est similaire à celui du secteur des services financiers (19 251) et nettement inférieur à celui du secteur de la santé (29 965). Il faut compter entre 6 et 8 heures pour permettre aux professionnels de l'informatique de localiser et de supprimer manuellement l'accès global, ce qui signifie que la protection et la maintenance de ces dossiers pourraient prendre des années.

Les industriels ont plus de 1 675 fichiers sensibles exposés pour chaque téraoctet. Ce chiffre est légèrement inférieur à celui du secteur de la santé (1 837) et à peu près identique à celui du secteur financier (1 646).

Notre analyse a révélé que les entreprises du secteur industriel **comptent en moyenne un nombre inférieur de fichiers ouverts à tous** par rapport à d'autres secteurs très ciblés tels que la finance et la santé. En revanche, les industriels ont en moyenne **un nombre supérieur de fichiers sensibles ouverts à tous par téraoctet**. Les PME sont particulièrement vulnérables, car elles ont un nombre record de fichiers sensibles ouverts à tous pour chaque téraoctet.

RÉSULTATS GÉNÉRAUX

Protection des données dans le secteur industriel

Entreprises dont des fichiers sensibles sont accessibles par tous les employés via l'accès global

Fichiers sensibles accessibles à tous	% des entreprises
< 1 000	56 %
1 000-10 000	22 %
>10 000	22 %

Données sensibles obsolètes par taille d'entreprise

Taille de l'entreprise	Nombre moyen de fichiers sensibles obsolètes	% moyen de fichiers sensibles obsolètes
Grandes entreprises	190 215	80 %
Moyenne	131 978	74 %
Petites entreprises	133 957	84 %
Moyenne du secteur	**152 214**	**78 %**

Les groupes d'accès globaux (p. ex. « Tout le monde », « Utilisateurs du domaine », « Utilisateurs authentifiés ») peuvent être utiles pour collaborer en interne, mais cela permet aux cybercriminels d'infiltrer beaucoup plus facilement votre environnement. Si un acteur malveillant parvient à compromettre un utilisateur final, il peut obtenir un chemin d'accès qui lui permet de copier, de partager, de supprimer et de modifier des informations sensibles non protégées.

Au total, 44 % des entreprises du secteur industriel ont en moyenne plus de 1 000 fichiers ouverts à tous les employés, et plus d'une entreprise sur cinq en compte 10 000. Pour ces entreprises dont les données sensibles sont surexposées, limiter l'accès ouvert en appliquant le principe du moindre privilège est un élément essentiel pour minimiser les risques.

La quantité de données sensibles et obsolètes stockées par les entreprises du secteur industriel sont supérieures à la moyenne, ce qui augmente la surface d'attaque et gonfle inutilement les coûts de stockage. En moyenne, **78 % des fichiers sensibles d'une entreprise sont obsolètes et pourraient être supprimés ou archivés.**

UN FANTÔME DANS LA MACHINE

Les vulnérabilités d'Active Directory

Entreprises disposant de mots de passe qui n'expirent pas

Mots de passe qui n'expirent pas	% des entreprises
< 500	44 %
500–1 500	32 %
> 1 500	24 %

Entreprises disposant d'utilisateurs fantômes

Taille du groupe de compte d'utilisateur obsolète	% des entreprises
< 1 000	56 %
1 000-10 000	36 %
> 10 000	8 %

Les comptes d'utilisateurs et de services inutilisés qui restent activés bien après le départ des employés (« utilisateurs fantômes ») offrent aux hackers beaucoup de temps pour s'adapter à votre environnement et, une fois à l'intérieur, accéder à vos dépôts de données. À partir de là, ils peuvent tranquillement dérober et chiffrer vos données sans être détectés.

Les comptes avec des privilèges d'administrateur inutilisés, mais activés, avec des mots de passe qui n'expirent jamais, sont l'un des plus beaux cadeaux que vous puissiez faire aux cybercriminels. Si vous ne bénéficiez pas d'une bonne visibilité sur votre environnement, ces vulnérabilités souvent négligées sont difficiles à détecter et à éliminer.

56 % des entreprises ont plus de 500 comptes avec des mots de passe qui n'expirent jamais et 44 % ont plus de 1 000 comptes « utilisateurs fantômes » inutilisés mais actifs.

ÉTAT DU SECTEUR

Le secteur industriel est le **cinquième secteur le plus ciblé en 2020,** avec **une fuite de données en moyenne équivalente à 4,99 millions de dollars. Il faut en moyenne à ces entreprises 220 jours pour contenir une fuite,** l'un des plus longs cycles de vie des menaces, tous secteurs confondus.

Si l'on tient compte de nos résultats, nous pouvons en tirer deux principales conclusions :

1. En matière de cybersécurité, le secteur industriel est en retard par rapport au secteur financier. Bien que certaines tactiques aient été mises en place, telles que la restriction de l'accès aux fichiers sensibles, près de la moitié des entreprises ne sont pas à l'abri d'une attaque perturbatrice.
2. L'état de préparation des industriels en matière de cybersécurité est plus susceptible de varier que celui d'autres secteurs réglementés tels que la santé ou les services financiers. Si certaines entreprises s'appuient sur des politiques bien établies en matière de sécurité des données et de procédures de réponse aux incidents, d'autres n'ont pris que très peu de mesures d'atténuation.

Pour avoir toutes les cartes en main, les entreprises du secteur industriel peuvent exploiter pleinement les solutions qu'elles ont déjà déployées. Pour cela, il leur faut éliminer les angles morts de la sécurité des données en augmentant la visibilité et en adoptant le modèle du moindre privilège pour réduire l'accès aux données grâce à l'automatisation. En réduisant votre rayon d'exposition, vous minimiserez les dommages que les attaquants peuvent causer lorsqu'ils pénètrent dans votre réseau, ce qui ne manquera pas d'arriver.

[2] Rapport IBM de 2020 sur le coût d'une fuite de données

Le coût moyen d'une fuite de données dans le secteur industriel s'élevait à **4,99 millions de dollars en 2020.[2]**

ÉTUDE DE CAS

Comment Varonis Edge aide un fabricant basé aux États-Unis à renforcer la sécurité de ses données sur site et dans le cloud

Lorsqu'un utilisateur non autorisé a ouvert un dossier des RH contenant des informations sur les salaires des employés, la solution Varonis a permis de l'identifier et de voir exactement ce à quoi il a accédé et ce qu'il a modifié.

Découvrez l'intégralité de l'étude de cas pour en savoir plus.

LIRE L'ÉTUDE DE CAS

À PROPOS DE VARONIS

Varonis est un pionnier en sécurité et analyse des données, spécialisé dans les logiciels de protection des données, de détection des menaces et de mise en conformité. Varonis protège les données des entreprises en analysant l'activité liée aux données, la télémétrie du périmètre et le comportement des utilisateurs, évite les sinistres en verrouillant les données et maintient un état sécurisé grâce à l'automatisation.

La solution Varonis est la meilleure de sa catégorie. Elle nous permet de tout faire, de la gestion des autorisations de partage à la localisation des données sensibles en passant par la sécurisation de nos environnements sur site et dans le cloud. En ayant la possibilité de faire tout cela à partir d'une seule et même interface, nous gagnons un temps précieux.

RESPONSABLE DES INFRASTRUCTURES
Fabricant américain

Vous souhaitez savoir où en est **votre entreprise** ?

Demandez une évaluation gratuite des risques par Varonis. Mettez en lumière rapidement les risques cachés auxquels sont exposées vos données les plus importantes rapidement, sans alourdir votre charge de travail.

CONTACTEZ-NOUS