# Six idées reçues dont doivent se méfier les conseils d'administration des entreprises

juin 23, 2022
by SentinelOne

Aujourd'hui, les cyber risques doivent être appréhendés au même niveau que tous les autres risques en entreprise. De plus en plus, les RSSI et/ou les DSI font partie désormais des conseils d'administration, mais il n'en reste pas moins que tous les administrateurs doivent comprendre l'impact des risques liés à la cybersécurité lorsqu'ils prennent des décisions stratégiques.

Ne pas saisir la nature de la cybersécurité dans l'environnement professionnel actuel peut avoir des conséquences désastreuses. Une préparation et une planification adéquates du conseil d'administration sont essentielles à la fois pour protéger l'entreprise mais également les dirigeants et les administrateurs en cas d'attaque, ils doivent être capables de démontrer qu'ils ont mis en place tout ce qui était nécessaire pour sécuriser l'entreprise.

Les informations sur la cybersécurité ne manquent pas, mais la plupart d'entre elles sont destinées à un public averti, rarement pertinent pour les décideurs de haut niveau. Afin d'aider les administrateurs dans leur gestion des cyber risques, voici six idées reçues dont ils doivent absolument se méfier.

## La cybersécurité ne concerne que certaines entreprises

Beaucoup pensent que la mise en place d'une politique de sécurité ne concerne que les grandes entreprises, les entreprises technologiques, les entreprises du secteur de la santé ou celles qui stockent des données clients sensibles (PII). Mais en réalité, elle est indispensable à toutes les entreprises pour se protéger des attaques potentielles.

La vague incessante de ransomwares a montré que les attaquants sont opportunistes et n'hésitent pas à cibler toutes les sociétés qui disposent de données ou de systèmes stratégiques exploitables. Même les entreprises qui ne stockent pas de données sensibles peuvent être piratées ou infectées par un ransomware si elles ne sont pas correctement sécurisées. En effet, au-delà des PII, les entreprises peuvent perdre de l'argent, voir leur réputation entachée ou subir d'autres conséquences désastreuses. La taille des entreprises n'est pas non plus un facteur déterminant pour les cybercriminels. Les petites entreprises sont d'ailleurs considérées comme des cibles plus faciles car elles consacrent en général moins de budget et de ressources à la cybersécurité.

> En résumé, le niveau de risque augmentera si les entreprises ne prennent pas les précautions nécessaires pour se protéger, et ce quels que soient leur taille, valeur et secteur d'activité.

## Les logiciels de sécurité suffisent pour protéger une entreprise

Des firewalls aux outils SIEM et SOAR, en passant par des anti-virus… il existe de nombreuses solutions en matière de cybersécurité. Mais les dernières années ont prouvé qu'elles n'étaient pas suffisantes pour protéger efficacement les entreprises.

L'environnement de travail hybride actuel offre plus de liberté que jamais aux collaborateurs. Ces derniers peuvent installer des logiciels et accéder aux actifs de l'entreprise, quel que soit l'endroit où ils se trouvent. Pour se prémunir contre les cyber risques et bénéficier d'une bonne visibilité, les entreprises peuvent dans un 1er temps opter pour l'une des solutions citées plus haut, mais cela ne suffira pas. Le paysage de la cybersécurité étant en constante évolution, les capacités de protection doivent également suivre le rythme.

> L'idée d'une protection totale contre les cybermenaces est illusoire. Cependant, les entreprises sont mieux accompagnées lorsque les conseils d'administration encouragent une culture de la cyber conscience et intègrent la cyber résilience à leur vision stratégique de l'entreprise.

**Les vulnérabilités logicielles ne sont pas un problème majeur**

Chaque logiciel utilisé par une entreprise peut également introduire des vulnérabilités qui facilitent la pénétration du réseau de l'entreprise. Parmi les exemples récents les plus médiatisés, citons Follina (CVE-2022-30190), qui permet aux attaquants de compromettre une machine Windows simplement en envoyant un document Word malveillant mais également la vulnérabilité Log4Shell détectée dans la bibliothèque Log4j d'Apache (CVE-2021-44228).

Malheureusement, la source la plus importante et la plus probable de vulnérabilités reste le système d'exploitation lui-même. Bien que la gestion des correctifs relève majoritairement de la responsabilité de l'équipe informatique, les conseils d'administration doivent comprendre qu'un nombre important de correctifs ne signifie pas que la sécurité est optimale.

> Ainsi toutes les entreprises devraient s'appuyer sur des experts capables de fournir une approche holistique de la sécurité. Il faut également éviter de se reposer sur le fournisseur du système d'exploitation pour tout corriger ou pour fournir des modules complémentaires de sécurité afin de pallier les problèmes.

## Nul besoin de s'inquiéter des attaques sur la chaine logistique

Même si une entreprise parvient à assurer la sécurité de ses propres logiciels, tout autre fournisseur de services peut, sans le savoir, faciliter l'accès au réseau. Récemment, nous avons assisté à l'attaque de la chaine logistique de SolarWinds et à l'incident Kaseya. Ces attaques sont très lucratives pour les attaquants, car la compromission d'un maillon faible permet d'accéder à un portefeuille complet de clients utilisant ce logiciel.

> Pour une protection optimale, les conseils d'administration doivent intégrer dans leur stratégie le déploiement d'une solution de sécurité adaptée, le développement d'un plan de réponse aux incidents (IR), la garantie que les politiques d'intégrité des applications ne permettent que l'exécution des applications autorisées et la promotion d'une culture de cybersécurité.

## On ne peut rien faire contre les menaces de cybersécurité

S'il est vrai que certaines menaces échappent au contrôle des entreprises, beaucoup d'alternatives existent pour les protéger contre les cyberattaques. La mise en œuvre de mesures de cybersécurité robustes peut contribuer à réduire le risque d'être ciblé par des cybercriminels.

Par ailleurs, même s'il est vrai qu'on ne peut pas protéger son entreprise contre toutes les attaques existantes, il est néanmoins possible de mettre en œuvre des mesures pour se protéger contre les plus prévisibles.

Dans la grande majorité des cas, les cybercriminels sont motivés par l'appât du gain. Les entreprises qui ne se protègent pas suffisamment seront sans aucun doute leurs prochaines cibles.

> La mise en œuvre d'un plan de cybersécurité global, comprenant plusieurs couches de sécurité, contribuera à protéger les entreprises contre la plupart des attaques.

**Il est impossible de former les employés à la cybersécurité**

Bien que les employés soient un élément clé de la stratégie de cybersécurité de toute entreprise, on ne peut pas attendre d'eux qu'ils soient des experts en cybersécurité. Chaque entreprise doit fournir à ses employés une formation et des ressources appropriées. Il s'agit notamment de les sensibiliser régulièrement aux menaces auxquelles l'entreprise a été ou peut être confrontée, de leur expliquer comment identifier les mails d'hameçonnage ou les demandes inhabituelles, mais aussi la marche à suivre pour signaler toute activité suspecte. L'ingénierie sociale reste l'une des méthodes les plus utilisées par les cybercriminels aujourd'hui. Les employés doivent être considérés comme une véritable aide à la cyberdéfense et se sentir suffisamment en sécurité et en confiance pour agir.

> Aucune entreprise au monde n'est à l'abri des cyberattaques, mais dans le paysage actuel des menaces, la cybersécurité doit être une priorité, un enjeu stratégique, planifié au plus haut niveau de l'organisation.

---

**Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.**

### Read more about Cyber Security

- Comprendre la différence entre EDR, SIEM, SOAR et XDR
- Dix conseils pour protéger votre annuaire Active Directory
- Comment défendre l'entreprise contre les risques liés à la chaîne logistique en 2022 ?
- Cloud : quelles sont les menaces les plus dangereuses et comment s'en protéger ?