Livre blanc 2024

Quatre façons de préparer votre entreprise à l'IA et aux technologies interconnectées

Des stratégies efficaces à l'intention des chefs d'entreprise

kaspersky bring on the future

EN SAVOIR PLUS : KASPERSKY.FR

Le prochain grand défi pour les entreprises : utiliser et sécuriser les technologies interconnectées

Les chefs d'entreprise doivent s'assurer qu'ils font les bons investissements technologiques au bon moment. Ils doivent mettre en place les personnes et les systèmes qui peuvent leur assurer la réussite.

De tous les investissements actuels, les technologies interconnectées, c'est-à-dire le réseau croissant d'appareils, de systèmes et d'applications connectés à Internet et les uns aux autres, sont les plus importants et les plus difficiles à mettre en œuvre. De l'intelligence artificielle (IA) aux espaces de données en passant par l'Internet des objets (IdO), les technologies interconnectées transforment les entreprises, leur permettant de recueillir davantage de données, d'automatiser les processus et de prendre de meilleures décisions.

Alors que cette « quatrième révolution industrielle » pousse au changement dans toutes les industries, les environnements hyperconnectés entraînent de nouveaux risques et défis en matière de sécurisation des entreprises et de protection des clients.

Notre recherche vise à aider les entreprises à garder une longueur d'avance sur les changements qu'apportent les technologies interconnectées, en posant des questions fondamentales sur la façon dont la cybersécurité doit s'adapter aux technologies interconnectées.

À propos de la recherche

Nous avons interrogé 560 responsables de la sécurité informatique dans six zones géographiques : Amérique du Nord (US), Amérique latine (LATAM : Brésil, Chili, Colombie et Mexique), Europe (Autriche, France, Allemagne et Suisse), Moyen-Orient et Afrique (META : Arabie saoudite, Afrique du Sud, Turquie et Émirats arabes unis), Russie et Asie-Pacifique (APAC : Chine, Inde, Indonésie) pour comprendre comment ils mettent en place et sécurisent les technologies interconnectées.

Les participants provenaient d'entreprises comptant au moins 1 000 employés dans de nombreux secteurs d'activité. Chacun d'entre eux était au courant des décisions prises dans le domaine de la cybersécurité pour les technologies interconnectées ou y participait.

Technologies interconnectées examinées

AI	Les systèmes imitent l'intelligence humaine dans des domaines tels que l'apprentissage, la résolution de problèmes et la prise de décision.
Web 3.0	Offre des applications décentralisées (DApps), des contrats intelligents (blockchain) et des données gérées par l'utilisateur, ce qui favorise l'efficacité et la confiance dans les écosystèmes numériques.
Espaces de données	Offrent un partage transparent des données dans un cadre collaboratif, favorisant ainsi la prise de décision en temps réel, l'innovation et l'interopérabilité.
Jumeaux numériques, réalité augmentée et réalité virtuelle	Les jumeaux numériques reproduisent numériquement des objets physiques. La réalité augmentée (RA) ajoute des superpositions numériques au monde réel. La réalité virtuelle (RV) crée des environnements immersifs.
6G	La prochaine génération de communication sans fil avec des vitesses ultra-rapides, une faible latence et de nouvelles capacités de connexion.
Internet des objets (IoT)	Les appareils « intelligents » interconnectés permettent le contrôle à distance et le partage de données.

« Ces nouvelles technologies sont le fruit d'une évolution qui a commencé avec l'intelligence économique et s'est poursuivie avec la science des données. Nous trouvons sans cesse de nouveaux moyens de tirer des renseignements à partir des données, et l'IA générative en est un exemple. »

Responsable de la cybersécurité d'une grande banque brésilienne

Les quatre stratégies pour se préparer à sécuriser les technologies interconnectées

Compte tenu de l'ampleur des changements que ces nouvelles technologies sont susceptibles d'entraîner, les organisations doivent élaborer une stratégie pour se préparer à adopter et à sécuriser les technologies interconnectées.

L'étude de Kaspersky a mis en évidence quatre stratégies efficaces pour être prêt à sécuriser les technologies interconnectées.

Les quatre stratégies

1. Adopter les principes de la sécurité dès la conception

2. Former les salariés et leur permettre de se perfectionner

3. Moderniser les solutions de cybersécurité

4. Respecter les réglementations et les normes

Stratégie 1

Adopter les principes de la sécurité dès la conception

L'intégration de la cybersécurité à chaque étape du cycle de développement des logiciels permet aux logiciels et aux matériels sécurisés dès leur conception de mieux résister aux cyberattaques, ce qui contribue à la sécurité globale des systèmes numériques.

Notre étude a révélé que les dirigeants qui se concentrent sur l'intégration de la cybersécurité dans les processus de développement, c'est-à-dire les promoteurs de la sécurité dès la conception, sont mieux préparés à sécuriser les technologies interconnectées.

Niveau de préparation général pour sécuriser les technologies interconnectées

50 %

des promoteurs de la sécurité dès la conception

26 %

des entreprises qui n'accordent pas la priorité à la sécurité dès la conception

Trois questions pour l'équipe de direction

1. À quel moment de nos processus de conception l'expertise en cybersécurité intervient-elle pour la première fois ?
2. Planifions-nous et budgétisons-nous les tests de sécurité pendant les phases de conception ?
3. Comment garantir la sécurité dès la conception tout en restant flexible et souple ?

« Les professionnels de la cybersécurité devraient participer au processus de conception initial et ne pas être relégués aux étapes finales. Cette approche proactive permet de s'assurer que les aspects liés à la sécurité sont pris en compte dès le départ, ce que l'on appelle souvent la sécurité par conception. »

Responsable de la cybersécurité d'une grande banque brésilienne

Stratégie 2

Former les salariés et leur permettre de se perfectionner

Le personnel qui comprend les cyberattaques et les moyens de les prévenir constitue une formidable ligne de défense. L'instauration d'une culture de la cyberconscience exige une stratégie globale qui permette aux employés d'acquérir des connaissances et de les mettre en pratique.

Notre étude révèle que les promoteurs de formation et de perfectionnement, c'est-à-dire les organisations qui accordent la priorité à la formation et au perfectionnement de leur personnel, sont mieux préparés à sécuriser les technologies interconnectées.

Niveau de préparation général pour sécuriser les technologies interconnectées

55 %

des promoteurs de formation et de perfectionnement

25 %

de ceux qui n'investissent pas encore dans la formation et l'amélioration des compétences

« Mon personnel n'est pas encore prêt pour les technologies interconnectées. Il y parviendra avec le temps – c'est un processus d'apprentissage continu. Il faut un plan de formation adéquat pour que les employés soient prêts. »

RSSI d'une entreprise médicale de premier plan en Arabie saoudite

Comment combler les lacunes en matière de compétences : ce que les dirigeants recommandent

Dans l'étude de Kaspersky, les dirigeants ont recommandé les moyens suivants pour améliorer les compétences des employés et les former.

Programmes d'éducation et de formation : des programmes réguliers couvrant des sujets tels que vos politiques de cybersécurité, les cybermenaces les plus courantes et les bonnes pratiques en matière de sécurité.

Simulation de phishing : aider les employés à reconnaître les emails de phishing et à y répondre. Les résultats donnent des informations sur les besoins en matière de formation continue.

Campagnes de communication et de sensibilisation : partagez les mises à jour, les actualités et les bonnes pratiques en matière de cybersécurité par le biais de plusieurs canaux. Utilisez des exemples concrets pour montrer l'impact des incidents de cybersécurité et l'importance de la contribution de chacun.

Politiques de sécurité conviviales : les employés sont plus enclins à suivre les politiques si elles sont claires, concises et faciles d'accès.

Collaboration avec les équipes informatiques et de sécurité : des liens plus étroits entre l'entreprise au sens large et les équipes chargées des technologies de l'information et de la sécurité encouragent le signalement des problèmes de sécurité.

Implication des dirigeants : montrez aux dirigeants qui participent à des initiatives de cybersécurité un message clair sur l'importance de cette dernière.

Trois questions pour l'équipe de direction

1. À quelle fréquence faut-il former les employés à la cybersécurité ?
2. Comment savoir si les employés comprennent la cybersécurité ?
3. Comment favoriser une culture de sensibilisation à la cybersécurité au sein de notre organisation ?

Stratégie 3

Moderniser les solutions de cybersécurité

Plus le nombre d'appareils connectés à Internet est élevé, plus les possibilités d'attaque sont nombreuses. Au fur et à mesure que vous adoptez ces technologies, vous pouvez être amené à utiliser des fonctions plus avancées dans les solutions de cybersécurité, telles que des contrôles d'accès renforcés, le chiffrement et la conformité aux réglementations.

Notre étude révèle que les utilisateurs avancés de la cybersécurité, c'est-à-dire les entreprises qui adoptent des solutions de cybersécurité avancées, sont mieux préparés à sécuriser les technologies interconnectées.

Niveau de préparation général pour sécuriser les technologies interconnectées

55 %

des utilisateurs avancés de la cybersécurité

22 %

des entreprises qui n'ont pas encore adopté des mesures de cybersécurité avancées

« Les failles de sécurité coûtent très cher, et la question n'est pas « si », mais « quand » elle arriveront. Au lieu de dépenser de l'argent pour nettoyer les dégâts, il faut le dépenser à se préparer. »

Directeur de la cybersécurité, Aselsan

Avantages de la mise à niveau des solutions de cybersécurité

S'adapter à un paysage changeant : la cybersécurité doit s'adapter à des menaces en constante évolution. La mise à jour des solutions de cybersécurité permet aux entreprises de garder une longueur d'avance sur les nouvelles menaces.

Respecter les normes réglementaires :la modernisation de la cybersécurité aide les entreprises à répondre aux exigences des nouvelles réglementations et normes, réduisant ainsi le risque de problèmes juridiques et d'atteinte à la réputation.

Mieux protéger les données stratégiques :le passage à des solutions de cybersécurité dotées de fonctionnalités telles que le chiffrement avancé, les contrôles d'accès et la détection améliorée des menaces permet de mieux protéger les informations de l'entreprise.

Trois questions pour l'équipe de direction

1. Que savons-nous des menaces et des vulnérabilités qui nous incitent à moderniser nos solutions de cybersécurité ?
2. Comment minimiser l'impact de la mise à niveau des solutions sur les flux de travail ?
3. Comment s'assurer que les employés peuvent utiliser efficacement nos outils de cybersécurité améliorés ?

Stratégie 4

Respecter les réglementations et les normes

Pour éviter les problèmes juridiques ou les atteintes à la réputation, veillez à ce que vos pratiques en matière de cybersécurité soient conformes à l'évolution des normes et des exigences légales.

Notre étude a révélé que les organisations qui accordent la priorité au respect des nouvelles réglementations et normes, c'est-à-dire les promoteurs de réglementations, sont mieux préparées à sécuriser les technologies interconnectées.

Niveau de préparation général pour sécuriser les technologies interconnectées

40 %

des promoteurs de réglementations

27 %

de ceux qui ne respectent pas encore les réglementations et les normes en matière de sécurité

Trois questions pour l'équipe de direction

1. Respectons-nous toutes les normes et réglementations en matière de sécurité ?
2. Devons-nous respecter toutes les normes et réglementations en matière de sécurité ? Comment les classer par ordre de priorité ?
3. Comment instaurer la confiance numérique par le biais de nos processus de conformité en matière de cybersécurité ?

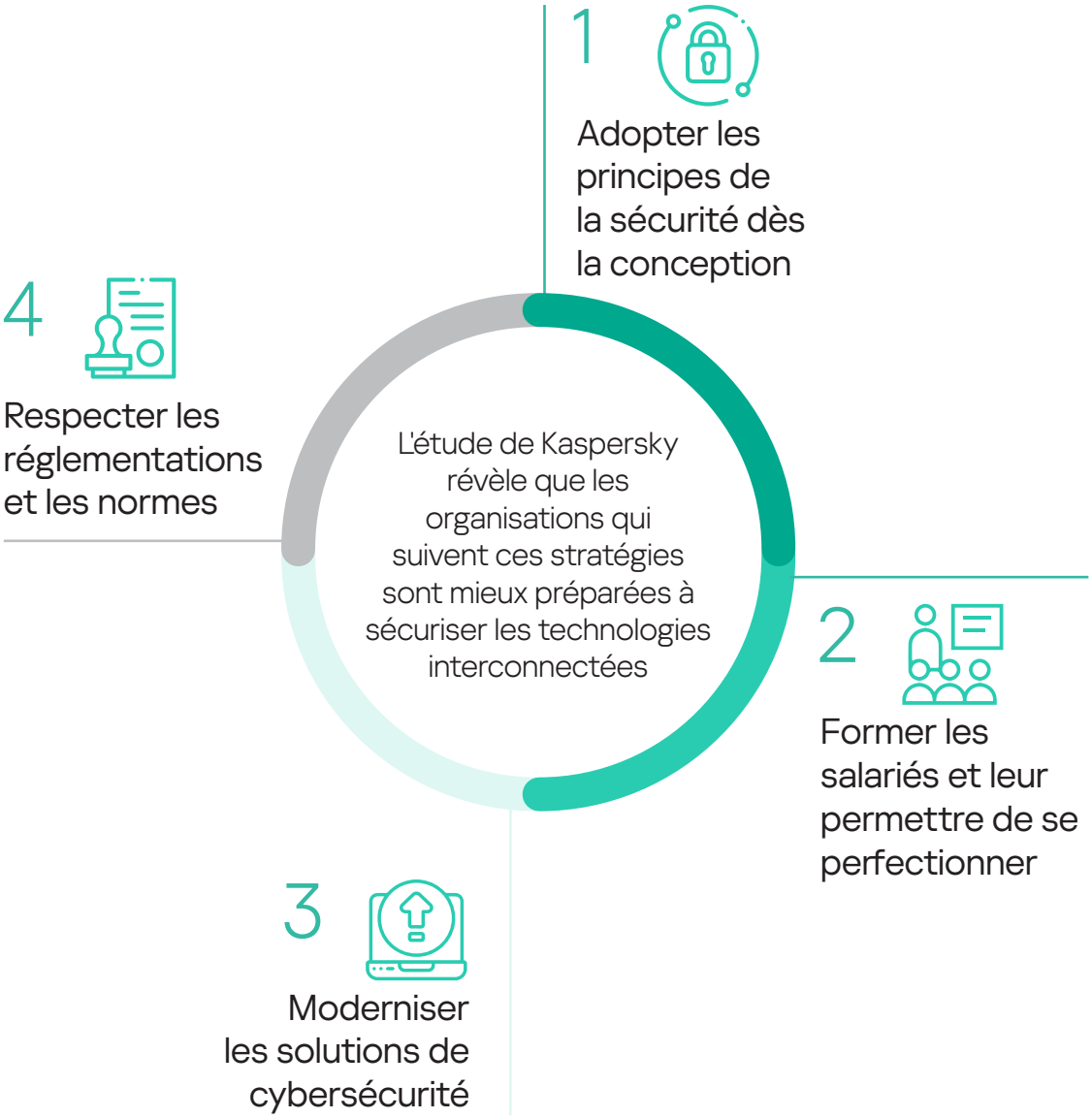
« Lorsque les entreprises adoptent ces technologies [IA], elles doivent également prendre en compte les lois et les perspectives d'audit qui peuvent permettre d'identifier les causes des cyberattaques et des failles de sécurité. »

Responsable de la cybersécurité d'une grande banque brésilienne

Un dernier mot sur la sécurisation des technologies interconnectées

Les technologies interconnectées offrent d'immenses possibilités commerciales, mais elles ouvrent également la voie à une nouvelle ère de vulnérabilité face à de graves cybermenaces. Avec la multiplication des données collectées et transmises, les mesures de cybersécurité doivent être renforcées.

Les entreprises devraient utiliser les quatre stratégies présentées dans ce rapport pour protéger leurs ressources critiques et renforcer la confiance de leurs clients dans un contexte où les appareils sont de plus en plus interconnectés :



Les dirigeants doivent veiller à ce que leurs ressources en matière de cybersécurité soient suffisantes pour leur permettre d'utiliser de nouvelles solutions de cybersécurité capables de relever les défis à venir de la technologie interconnectée.

Pour en savoir plus, téléchargez le rapport complet : Un avenir connecté pour les entreprises : comment les dirigeants doivent se préparer à utiliser et à sécuriser l'IA ainsi que les technologies interconnectées

kaspersky.fr

kaspersky

Actualitéssur les cybermenaces: securelist.com
Actualités sur la sécurité informatique : business.kaspersky.fr
Revue destinée aux chefs d'entreprise : kaspersky.com/blog/secure-futures-magazine
Solutions de cybersécurité pour les entreprises : kaspersky.fr/enterprise-security