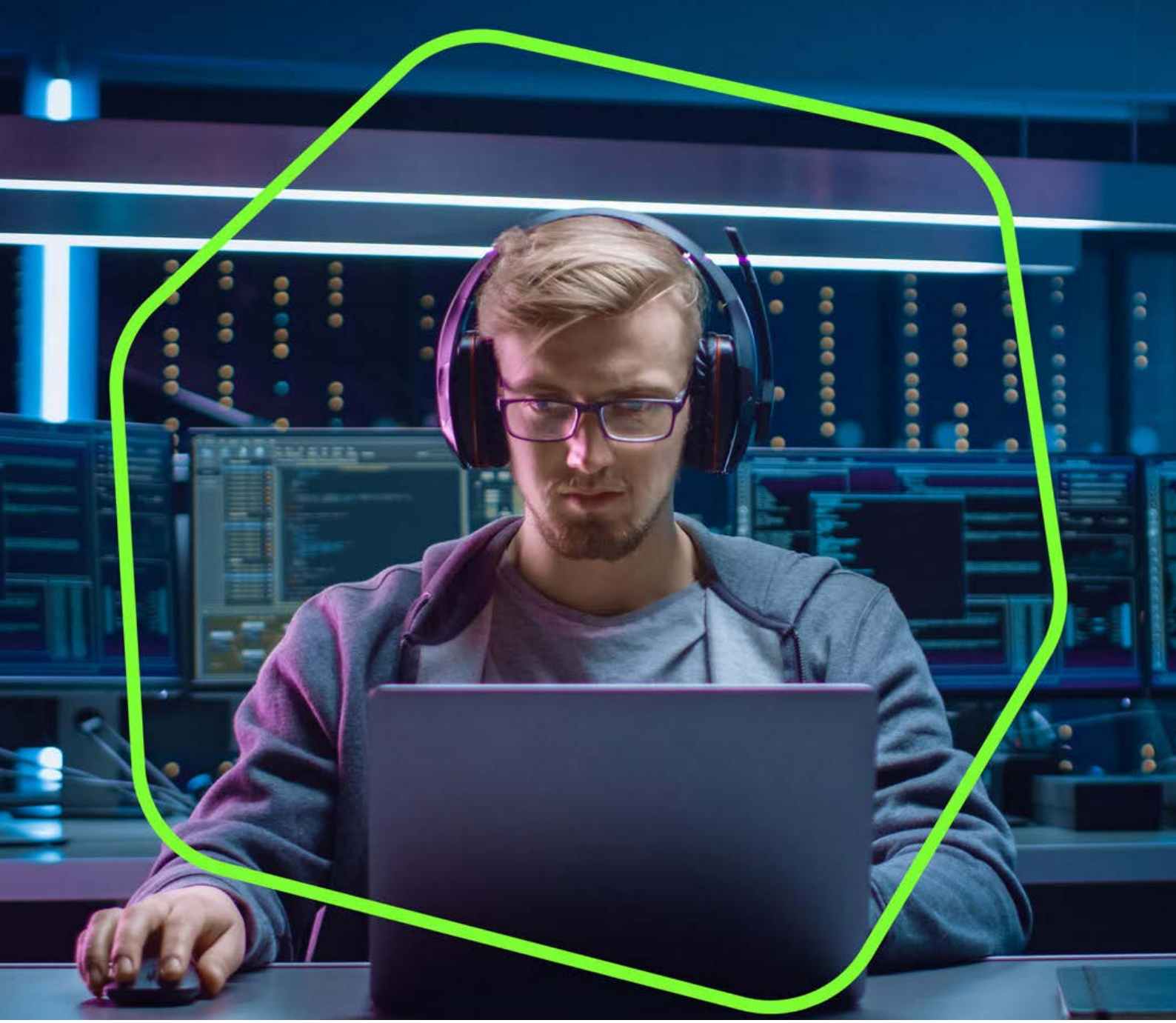


Faites preuve d'ingéniosité pour relever les défis modernes en matière de cybersécurité.

Sécurité simplifiée : un guide pas-à-pas pour atténuer les risques de cybersécurité en entreprise

kaspersky BRING ON THE FUTURE

Sommaire

Introduction

Le mode de fonctionnement des petites et moyennes entreprises (PME) a changé. La productivité a atteint des niveaux autrefois inespérés, grâce à l'informatique dématérialisée, aux outils de collaboration en ligne et aux stratégies de travail à distance, qui sont désormais devenues monnaie courante. Toutefois, le revers de la médaille est l'élargissement des surfaces d'attaque et l'augmentation des cyberattaques – des éléments qui peuvent s'avérer coûteux, voire mortels, pour les entreprises négligentes.

Une grande partie du risque que les PME ont assumé a été déclenchée par la pandémie, lorsque les opérations commerciales ont été bouleversées de fond en comble. Dans leur volonté de limiter les effets du confinement, de nombreuses organisations ont autorisé le travail à distance en l'absence de contrôles de sécurité. Si l'on considère que les employés qui découvrent tout juste le travail à distance **présentent un risque élevé en matière de sécurité**[1], cette tendance est préoccupante.

La moitié des entreprises britanniques identifiant des cyberattaques déclarent qu'elles se produisent mensuellement[3]

Gouvernement du Royaume-Uni

L'adoption du cloud a également grimpé en flèche et est désormais essentielle pour être compétitif sur les marchés modernes où la vitesse et l'échelle sont reines. Les PME sont en fait celles qui **adoptent le plus rapidement le cloud**[2], ce qui signifie que les données se déplacent rapidement dans leurs écosystèmes où elles peuvent être perdues ou volées.

La transformation numérique a donc rendu plus probables les cyberattaques et les violations des données. Cependant, avec les connaissances appropriées, il est possible d'appliquer des mesures de défense abordables qui éviteront à votre entreprise de faire partie du lot.

Par exemple, savez-vous...

- Quelles sont les réglementations gouvernementales auxquelles vous devez vous conformer ?
- Si vos mots de passe sont partagés avec des tiers « de confiance » ?
- Si des informations personnellement identifiables (PII) sont en circulation dans votre cloud public ?
- Si vos logiciels sont à jour et si tous les correctifs sont installés ?

Si ce n'est pas le cas, il y a matière à amélioration, mais pas de panique. Dans ce guide, vous apprendrez **comment** et **pourquoi** votre entreprise est vulnérable, et découvrirez des conseils, des astuces et des solutions pour la sécuriser.

Pourquoi les pirates informatiques ciblent-ils les PME ?

« Nous sommes trop petits pour être ciblés »

Les petites entreprises pensent à tort qu'elles n'ont pas de valeur aux yeux des attaquants. Ce n'était pas le cas il y a cinq ans et ce n'est certainement pas le cas aujourd'hui. Si les entreprises sont le plus souvent ciblées, elles sont également plus susceptibles de disposer d'une assurance complète et de mesures de sécurité solides pour dissuader les acteurs malveillants potentiels. Les attaques apocalyptiques, comme celle qui a frappé le gouvernement américain (SUNBURST[4]), poussent à l'action et à l'augmentation des budgets alloués à la cybersécurité.

61 % des petites entreprises américaines ne sont pas préoccupées par les cyberattaques[5]

CNBC

En revanche, il arrive que des PME opèrent sans un seul spécialiste de la cybersécurité. Cela signifie qu'un pirate informatique pourrait non seulement s'infiltrer dans ces organisations, mais aussi y rester sans être détecté, et collecter des données, préparant ainsi la voie à de futures actions malveillantes.

Un manque d'investissement dans la cybersécurité

Les pirates informatiques savent que les petites entreprises manquent d'investissements dans le domaine de la cybersécurité sur deux fronts : la technologie et le personnel. Les systèmes présentent plus de trous qu'un bloc de gruyère suisse, tandis que le personnel est vulnérable à des techniques comme le phishing (qui est à l'origine de la plupart des cyberattaques au Royaume-Uni[3]). L'erreur humaine est en fait la principale cause des violations de données dans les petites entreprises. Il est donc essentiel de promouvoir une culture de la sécurité au sein du personnel.

Cela rapporte

Les PME ne sont pas seulement des cibles faciles, elles sont aussi des cibles **intéressantes** en raison des données qu'elles traitent. Prenons l'exemple des startups des secteurs de la santé ou de la finance : lorsqu'elles commencent à accumuler des clients, elles deviennent garantes des données de paiement et des antécédents médicaux, protégés par des réglementations telles que le règlement général sur la protection des données (RGPD) et la loi sur la portabilité et la responsabilité des assurances-maladie (HIPAA). Les pirates informatiques qui dérobent ces données peuvent non seulement les vendre en ligne, mais aussi les chiffrer en vue de les exploiter dans le cadre d'une attaque par ransomware. Si une victime ne paie pas la rançon demandée (en moyenne 258 143 dollars[6] en 2022), le pirate informatique la publie par dépit.

Les PME sont plus susceptibles de payer une rançon que les entreprises parce qu'elles manquent souvent de systèmes de sauvegarde et qu'elles ne peuvent pas se permettre de perdre leurs données. Toutefois, une telle situation peut être préjudiciable à la fois sur le plan financier et sur celui de la réputation. Les investisseurs, les clients et les forces de l'ordre surveillent de près toute entreprise prête à négocier avec des criminels, dont le champ d'action peut s'étendre au terrorisme, à la traite d'êtres humains et à d'autres domaines.

LE SAVIEZ-VOUS ?

Les ransomwares sont apparus en 1989 lorsqu'un biologiste évolutionniste formé à Harvard, Joseph L. Popp, a créé le cheval de Troie AIDS. M. Popp a remis des disquettes infectées à des spécialistes mondiaux du sida et a déclaré qu'elles contenaient un programme permettant d'analyser le niveau de risque d'une personne. En réalité, les disques chiffraient les fichiers d'une machine et demandaient 189 $... par facture !

Comment les PME sont-elles vulnérables aux cybermenaces ?

Vous savez maintenant pourquoi les cybercriminels s'intéressent à votre entreprise, mais qu'est-ce qui la rend vulnérable ?

Un manque de compétences pertinentes

Historiquement, les investissements dans les technologies de sécurité ont largement surpassé les investissements dans les capacités humaines.

En 2022, **près de 700 000 entreprises britanniques**[7] ont connu une pénurie de compétences en cybersécurité, ce qui signifie que les responsables de la sécurité manquaient de maîtrise des tâches définies dans le programme gouvernemental Cyber Essentials[8]. Ce **manque d'expertise probant** met les entreprises en danger.

Mauvaise hygiène en matière de sécurité

Une mauvaise hygiène en matière de sécurité correspond à un manque général de connaissances ou d'actions appropriées dans ce domaine, comme l'utilisation de mots de passe faibles (prendre de mauvaises mesures), le fait de ne pas détruire des documents confidentiels (oublier de prendre des mesures) ou le fait d'ignorer les stratégies de l'entreprise (refuser de prendre des mesures). Ce type d'erreur humaine est à l'origine de **82 % des violations de données**[9] et peut être exploité par des acteurs malveillants peu qualifiés.

Mauvaise gestion des vulnérabilités

Même les petites entreprises se servent parfois de dizaines de logiciels, qui peuvent tous être vulnérables s'ils ne sont pas mis à jour ou si les correctifs ne sont pas appliqués. Sans un inventaire des ressources et un solide programme de gestion des correctifs, les entreprises se retrouvent très vulnérables.

Un phénomène connu sous le nom de Shadow IT, qui consiste pour les employés à utiliser des services et des programmes à l'insu de leur service informatique, complique davantage les choses, car certains services en ligne inconnus peuvent présenter des vulnérabilités, voire être malveillants. Les travailleurs à distance de votre entreprise peuvent présenter un risque plus élevé en ce sens.

Faible visibilité des données

À l'heure actuelle, seul un quart des entreprises est en mesure de classer leurs données, alors qu'une mauvaise manipulation de celles-ci peut entraîner des violations coûteuses. Demandez aux **45 %**[10] des entreprises qui ont subi une violation de données dans le cloud ou qui ont échoué à un audit portant sur celles-ci. Si vous ne voyez pas vos données et si vous ne pouvez pas savoir quand elles sont partagées, vous ne pouvez pas les protéger.

Protection faible (ou inexistante) en matière de cybersécurité

Les petites entreprises peuvent être tentées de faire l'impasse sur la cybersécurité, ce qui est le cas d'**environ la moitié**[11] d'entre elles. Si vous disposez d'une empreinte numérique mais que vous négligez la cybersécurité, vous jouez à la roulette russe.

Les cybermenaces les plus courantes pour les PME

Le paysage des menaces se développe au fur et à mesure de l'émergence de nouvelles technologies, et il existe actuellement de nombreuses façons pour les acteurs malveillants d'infiltrer votre organisation. En dresser la liste dépasse les objectifs de ce guide, mais ce que nous pouvons faire, c'est partager les méthodes les plus courantes utilisées par les attaquants pour s'infiltrer dans les PME. Que vous soyez une entreprise ou une équipe de dix personnes, les attaquants tenteront leur chance s'ils pensent qu'il y a de l'argent à gagner.

Le fait de comprendre les vecteurs d'attaque auxquels vous êtes confrontés, même au niveau le plus élevé, constitue le fondement sur lequel vous pouvez commencer à consolider votre sécurité. Nous reconnaissons que le suivi des cybermenaces peut être une tâche ardue, mais vous avez de grandes chances de rester en sécurité en vous concentrant simplement sur les techniques les plus courantes, celles que Kaspersky voit et repousse tous les jours.

Quelles sont donc les méthodes les plus utilisées par les criminels pour pénétrer dans des entreprises comme la vôtre ?

Phishing et escroqueries

Il existe deux grands types de fraudes en ligne visant à voler les données et l'argent des utilisateurs : le phishing et l'escroquerie. La première est la menace la plus néfaste et la plus répandue à laquelle sont confrontées les PME. Les auteurs de phishing cherchent avant tout à soutirer des informations confidentielles à leurs victimes, comme des identifiants ou des données de cartes bancaires, tandis que les escrocs déploient des techniques d'ingénierie sociale (une forme de coercition numérique) pour persuader leurs cibles de transférer de l'argent de leur plein gré.

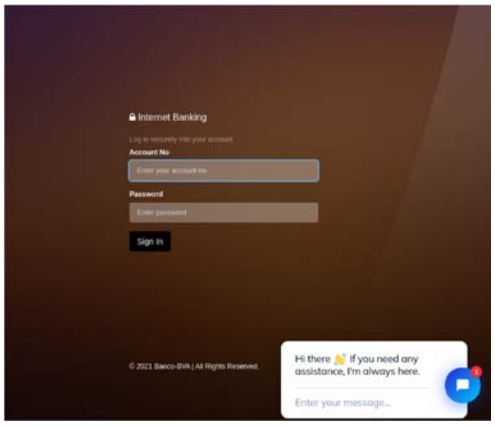
Bien que les attaques de phishing commencent généralement par des emails de masse contenant des liens vers de faux sites Internet, d'autres vecteurs d'attaque gagnent du terrain, comme le **vishing** (phishing vocal). Il existe aujourd'hui d'innombrables plateformes de communication et de partage de données que les pirates informatiques peuvent utiliser pour diffuser des liens de phishing, c'est pourquoi la vigilance est de mise.

Découvrez comment un hôtel-boutique a perdu 1 million de dollars à la suite d'une attaque de phishing[12]

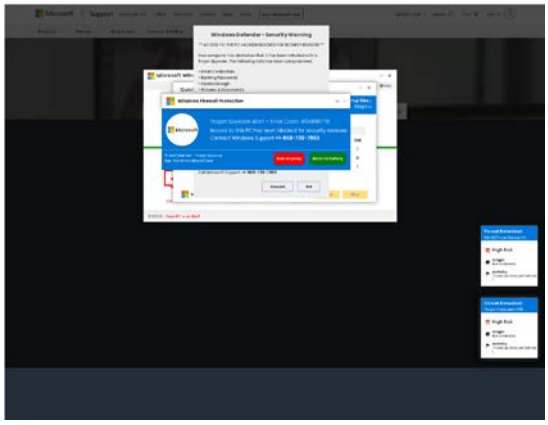
En fait, les auteurs de phishing peuvent cibler les identifiants de n'importe quel service en ligne : réseaux sociaux, boutiques en ligne, services de messagerie et bien d'autres. Ils tentent de persuader les victimes qu'elles se connectent à de vrais sites Internet ou qu'elles partagent leurs identifiants avec un employé de l'entreprise. Bien souvent, les faux sites ne se distinguent pas de l'original et même un utilisateur expérimenté peut se faire avoir. Et malheureusement, les pirates informatiques peuvent mettre en péril votre organisation en piégeant un seul employé.

LE SAVIEZ-VOUS ?

Le terme « phishing » a été inventé en 1996 lorsque des cybercriminels ont attaqué les utilisateurs d'AOL, le plus grand fournisseur d'accès Internet à l'époque. Les attaquants se sont fait passer pour des employés d'AOL et ont envoyé des messages malveillants demandant aux utilisateurs de vérifier leurs comptes ou de fournir des données de paiement.



Site de phishing avec assistance en ligne



Faux message concernant des problèmes liés à Windows

Pour en savoir plus et obtenir des conseils et des astuces pour rester en sécurité, consultez notre rapport complet sur le phishing et les escroqueries[13].

Programmes malveillants et ransomwares

Les programmes malveillants (ou malwares) sont des logiciels conçus pour nuire à vos appareils. Si votre ordinateur portable, votre ordinateur de bureau ou votre téléphone est infecté par un programme malveillant, son fonctionnement peut ralentir ou il peut ne plus fonctionner du tout. Les programmes malveillants peuvent également supprimer ou voler des données, mettant en danger la confidentialité des données de votre entreprise.

Il existe de nombreux types de programmes malveillants, mais les suivants sont parmi les plus courants :

- **Vers** – ils se reproduisent d'un ordinateur à l'autre sans infecter d'autres objets sur le même ordinateur
- **Logiciels publicitaires** – logiciels diffusant des annonces que vous pouvez télécharger par inadvertance
- **Virus** – ils se reproduisent d'eux-mêmes et se propagent dans le système de votre appareil
- **Bots** – ils effectuent automatiquement des opérations particulières et récoltent des données
- **Chevaux de Troie** – ils se camouflent en fichiers ordinaires mais exécutent des opérations nuisibles sur votre appareil

Les programmes malveillants peuvent compromettre vos appareils de différentes manières, comme lorsque quelqu'un clique sur un lien infecté ou ouvre une pièce jointe dans un spam. Sans intervention, les programmes malveillants peuvent faire des ravages sur vos appareils et vous exposer au vol de données.

Une forme de plus en plus répandue de programmes malveillants est le **ransomware**, qui bloque l'accès à un système informatique jusqu'au versement d'une somme d'argent. Les gangs organisés de ransomwares appliquent également des stratégies de double extorsion : ils volent les données avant de les chiffrer. Si une victime refuse de payer, ils menacent de publier les données dérobées en ligne.

Rien qu'au troisième trimestre 2022, Kaspersky a arrêté des attaques par ransomwares sur 72 941 ordinateurs[14]

L'attaque de Colonial Pipeline[15], qui a porté atteinte à des infrastructures américaines de première importance, en est un bon exemple. Un groupe appelé DarkSide a mis hors service le plus grand oléoduc du pays, provoquant des pénuries de carburant et des hausses de prix à l'échelle nationale. Colonial a finalement payé une rançon de 5 millions de dollars[16] aux pirates informatiques, ce qui montre à quel point cette activité est lucrative.

Votre entreprise dispose-t-elle d'un spécialiste de l'informatique ou de la sécurité ? Si c'est le cas, pensez à partager avec eux notre rapport sur les TTP des groupes de ransomware[17].

LE SAVIEZ-VOUS ?

L'attaque WannaCry qui a mis à mal le service national de santé britannique (NHS) en 2017 reposait sur une vulnérabilité de Microsoft Windows appelée EternalBlue. Les entreprises qui n'ont pas corrigé cette vulnérabilité ont encore été exploitées des années plus tard.

En moyenne, il faut 85 jours pour maîtriser un incident lié à une menace interne[18]

The Ponemon Institute

Vulnérabilités des terminaux

L'environnement de travail moderne est tellement distribué que les points d'entrée du réseau d'une entreprise pourraient se trouver simultanément sur chaque continent. C'est en grande partie le résultat de la main-d'œuvre délocalisée, où les politiques de BYOD et les outils de collaboration en ligne sont la norme. Pourtant, même les plus petites entreprises, ne pouvant ignorer les avantages d'une agilité accrue, fonctionnent aujourd'hui de manière distribuée.

Chaque appareil connecté à votre réseau est un terminal, un point d'entrée potentiel pour une infection. En plus des systèmes d'exploitation eux-mêmes, chaque application sur un terminal (pensez à Slack, Zoom et Outlook) peut être vulnérable, ce qui signifie qu'une entreprise avec seulement 50 machines peut héberger des centaines de vulnérabilités. Les pirates informatiques peuvent exploiter des vulnérabilités non corrigées pour pénétrer dans votre réseau. Cette méthode est l'une des plus courantes pour nuire à l'infrastructure informatique par le biais d'un seul terminal. Même les correctifs peuvent introduire des vulnérabilités !

Menaces internes

Une menace interne est un risque organisationnel qui provient de l'intérieur du cadre de sécurité. Il peut s'agir d'employés (actuels ou anciens), mais également de sous-traitants ou de partenaires, soit toute personne ayant accès à des informations confidentielles ou à des infrastructures importantes. Les menaces internes peuvent résulter **d'une intention malveillante ou d'une erreur humaine**. Par exemple, un employé qui perd une clé USB contenant des données confidentielles constitue une menace interne.

Le personnel interne a un accès légitime au réseau informatique de l'entreprise dans le cadre de ses responsabilités professionnelles, raison pour laquelle les outils de sécurité ne les considèrent pas comme une menace. Ils n'ont donc pas besoin de pirater les comptes des employés ni de contourner les défenses périmétriques pour accéder aux données.

Le personnel interne peut occasionner les dommages suivants :

- Voler des informations confidentielles et les transmettre à des concurrents
- Divulguer des données à caractère personnel soumises à des réglementations gouvernementales
- Détruire des informations essentielles
- Installer et exécuter des programmes malveillants
- Désactiver ou perturber les systèmes de sécurité de l'information en prévision d'attaques extérieures

Les menaces internes se multiplient dans les PME, car de plus en plus d'employés ont accès à de nombreux comptes qui contiennent toujours plus de données. Les possibilités d'activités malveillantes sont plus nombreuses, tout comme les risques de négligence, qu'il s'agisse du recyclage de mots de passe ou de l'utilisation de logiciels non homologués.

Vous voulez connaître les signes révélateurs des menaces internes ? Consultez notre **page encyclopédique**[19].

Comment votre entreprise peut-elle réduire les risques de cybersécurité ?

Le remède à ces attaques et à ces vulnérabilités n'est pas un antidote du tout, mais plutôt un ensemble d'éléments qui doivent fonctionner en tandem pour être efficaces. Les acteurs de la menace innovent presque constamment, et cette aptitude à concevoir et à exécuter rapidement des attaques implique qu'il n'existe pas de solution miracle. De nombreuses conditions doivent être remplies. Cette situation peut être préoccupante pour les entreprises dont le niveau de maturité informatique est faible, en particulier celles qui dépendent de plus en plus de l'informatique dans le cloud et des technologies connectées. Cependant, votre solde bancaire, votre réputation et la sécurité de vos clients sont en jeu.

Heureusement, vous n'avez pas besoin d'une équipe dédiée à la cybersécurité ni d'un budget important pour mettre en œuvre des mesures défensives efficaces. La première étape consiste à comprendre comment protéger votre entreprise contre les menaces les plus courantes, afin que vous puissiez prendre des mesures réfléchies et décisives, en choisissant une solution de sécurité qui vous convienne.

Examinons les conditions à remplir pour qu'une PME puisse faire face aux cybermenaces.

Protection des terminaux

La prolifération du travail à distance, des services cloud et des processus agiles signifie que votre stratégie de sécurité doit englober l'ensemble de vos terminaux. Sont concernés les serveurs, les ordinateurs portables, les appareils mobiles ainsi que tous les appareils personnels utilisés à des fins professionnelles. Voici ce que vous devriez rechercher :

- La **meilleure sécurité possible** pour chaque poste de travail, serveur et appareil mobile qui contient vos données – où qu'il se trouve et que vous en soyez le propriétaire ou non
- L'**assurance** de pouvoir couvrir tous les systèmes d'exploitation de votre environnement mixte – y compris Windows, Mac, Linux, iOS et Android – avec une solution unique, à partir d'une seule console

Une protection endpoint de qualité est au cœur de votre stratégie de cybersécurité. Lorsque vous avez trouvé une solution qui répond à vos besoins, vous devez examiner ce qu'elle peut faire plus particulièrement pour minimiser le risque de cyberattaque ou de violation de données. Voici ce que votre solution devrait vous permettre de faire :

- Protéger pleinement vos données, vos employés et votre infrastructure, sans nuire aux performances
- Réduire votre surface d'attaque en contrôlant les applications, les sites web et les appareils qui peuvent interagir avec vos terminaux
- Repérer et contrer les menaces émergentes qui vous guettent

Enfin, vous devez vous interroger sur la **facilité** d'utilisation de la solution. Si, en tant que PME, vous devez investir des dizaines d'heures par mois pour assurer un fonctionnement optimal, ce n'est pas la solution qu'il vous faut. En ce sens, voici ce que vous devriez rechercher :

- Des niveaux élevés d'automatisation, en particulier pour les tâches essentielles (mais routinières), comme l'application de correctifs et le déploiement de systèmes d'exploitation
- Des capacités de gestion à distance, qu'il s'agisse de configurer des postes de travail dans des bureaux à domicile ou de sécuriser les données grâce à des options de chiffrement
- Une gestion intégrée à écran unique à votre périmètre ou dans le cloud

L'expertise nécessaire pour protéger une infrastructure informatique en pleine croissance a un coût, c'est pourquoi il est nécessaire d'investir judicieusement dans la protection des terminaux afin de répondre à l'évolution des conditions de sécurité de votre entreprise, tant en matière de temps que de budget et de compétences.

Exemples de violations du RGPD

- L'organisation caritative britannique Mermaids a été condamnée à une **amende de 29 000 euros**[22] pour « mesures techniques et organisationnelles insuffisantes pour assurer la sécurité de l'information ».
- La société française de covoiturage Ubeeqo a été condamnée à une **amende de 175 000 euros**[23] pour « non-respect des principes généraux de traitement des données ».
- L'université italienne Bocconi a été condamnée à une **amende de 200 000 euros**[24] pour « non-respect des principes généraux de traitement des données »

Visibilité des données

Deux tiers des organisations[20] se servent d'un fournisseur de services cloud (CSP), et la plupart d'entre elles font appel à plusieurs fournisseurs de ce type, ce qui complique la sécurisation des données. Cela explique aussi en partie pourquoi **près de la moitié des violations de données**[21] se produisent désormais dans le cloud. Il est impératif que votre organisation dispose d'une visibilité totale des données. Ce n'est qu'à ce moment-là que vous pourrez classer vos ressources d'informations (par exemple les bases de données des clients) et gérer les risques qui y sont liés. Cela signifie que vous devez être en mesure de faire ce qui suit :

- Détecter le traitement et le stockage de données personnelles dans les services accessibles par des tiers, susceptibles d'entraîner une violation de données
- Mettre fin à l'utilisation inappropriée d'applications cloud
- Identifier les informations confidentielles liées aux informations personnellement identifiables (PII) et aux données de paiement
- Détecter des données stockées plus longtemps que nécessaire (ou que la durée spécifiée par votre politique de conservation des données)
- Empêcher les utilisateurs de connecter des appareils externes non autorisés à leur ordinateur pour transférer des données
- Chiffrer les appareils contenant les données les plus confidentielles, comme par exemple les ordinateurs portables des directeurs, afin que les données ne soient pas accessibles en cas de perte ou de vol

Si votre solution de sécurité ne permet pas ce niveau de visibilité et de contrôle, vous risquez de violer des réglementations comme le règlement général sur la protection des données (RGPD), ce qui peut entraîner d'énormes amendes. Même les petites organisations à but non lucratif doivent se conformer à ces réglementations.

Stratégies de cybersécurité

Une mesure de base consiste à documenter les stratégies de cybersécurité afin de s'assurer que les membres de votre organisation savent ce que l'on attend d'eux. Cependant, les stratégies ne suffisent pas à garantir la conformité, en particulier si votre personnel travaille à distance, loin des contraintes du bureau. **Deux tiers**[25] des employés à distance n'ont pas respecté les stratégies de cybersécurité au moins une fois, et **près de la moitié**[26] des PME ont subi une atteinte à la sécurité informatique.

Votre solution de sécurité doit donc **vous aider à appliquer vos stratégies**. Voici quelques exemples :

- **Règles relatives aux mots de passe** : imposer un mélange de chiffres, de caractères, de majuscules et de symboles, en invitant les utilisateurs à modifier périodiquement leurs mots de passe
- **Authentification multi-facteurs (MFA)** : assurez-vous que les utilisateurs doivent s'identifier en passant plusieurs contrôles, par exemple à l'aide d'un mot de passe et d'un message texte
- **Appareils externes** : empêchez les appareils externes de fonctionner lorsqu'ils sont branchés
- **Logiciels non approuvés** : autorisez une liste d'éditeurs de confiance et veillez à ce que seuls les administrateurs du système puissent télécharger des logiciels provenant de nouvelles sources

Formation des employés

On distingue deux niveaux de formation des employés : la sensibilisation à la sécurité et la formation dédiée à la cybersécurité. Pour bloquer les menaces internes, par exemple, les petites entreprises doivent s'assurer qu'elles appliquent une solide culture de **sensibilisation à la sécurité**. Cette approche permet de minimiser la cyber-ignorance et d'aider les employés à détecter lorsqu'un pirate informatique tente de compromettre les données de l'entreprise. Chaque employé devrait pouvoir bénéficier d'une formation de sensibilisation à la sécurité afin de promouvoir une culture de la sécurité. N'oubliez pas qu'une entreprise est aussi forte que son maillon le plus faible.

Il est également extrêmement important que le personnel technique de votre entreprise (qu'il s'agisse de professionnels de la cybersécurité, de spécialistes de l'informatique ou tout simplement de techniciens) **développe des compétences informatiques appropriées** qui ne se limitent pas à la sensibilisation à la sécurité. Il est essentiel de disposer d'une personne qui connaisse les mesures à prendre en cas d'activité inhabituelle sur le réseau, par exemple.

Cela dit, une étude menée par Forrester[27] a montré que de nombreux utilisateurs n'aiment pas les certifications traditionnelles en raison de leur **coût élevé** et de leur **faible applicabilité**, soit les mêmes raisons pour lesquelles les PME négligent les formations à la cybersécurité. Ces programmes sont largement axés sur les entreprises, mais la cybersécurité n'est pas uniforme. **Les programmes destinés aux PME doivent être adaptés à leur taille et à leur niveau de maturité informatique**, et les compétences les plus essentielles pour ces entreprises doivent être présentées sous une forme digeste et accessible.

La formation à la cybersécurité n'est peut-être pas une priorité pour votre entreprise si sa fonction informatique est limitée, mais le personnel de votre organisation est en première ligne. Choisissez une formation dispensée par des experts, adaptée à la taille de votre entreprise, et vous comprendrez vite l'intérêt qu'elle représente.

Besoins des entreprises, défis informatiques et solutions

Besoin commercial	Problème informatique	Solution Kaspersky Endpoint Security Cloud
Adoption renforcée du cloud	Shadow IT	 **Cloud Discovery** vous aide à détecter et à restreindre l'utilisation de ressources cloud inappropriées ou non autorisées
Réduction des dépenses informatiques	Identification et arrêt des cyberattaques	 **Protection de classe mondiale des terminaux** pour les ordinateurs de bureau et les serveurs de fichiers Windows, les appareils Mac OS, les appareils mobiles iOS et Android
Productivité maximale	La collaboration en ligne présente des risques	 Collaboration sécurisée avec Microsoft Office 365
Capacités de réponse à incidents	Manque de personnel formé/ petit budget consacré à la cybersécurité	 Formation continue et à la demande en matière de cybersécurité
Conformité réglementaire	Manque de visibilité et de contrôle des données	 **Data Discovery** vous permet d'identifier facilement les informations confidentielles dans votre cloud, par exemple des informations de paiement et des informations personnellement identifiables
Infrastructure informatique sécurisée	La gestion des ressources peut demander beaucoup de ressources	 Correction automatique des vulnérabilités
Capacité de travail à distance	Personnel dispersé qui peut ne pas être sensibilisé à la sécurité	 Soyez partout et protégez tout à l'aide d'une console basée dans le cloud Possibilité de chiffrement en cas de perte ou de vol des appareils contenant des données confidentielles

Une solution de sécurité unique et abordable – Kaspersky Endpoint Security Cloud

L'adoption croissante du cloud et le travail à distance ont été complétés par des exigences réglementaires strictes et la présence continue d'acteurs malveillants. Il peut être décourageant de réduire les cyber-risques dans ce contexte, en particulier pour les petites entreprises dont la fonction informatique est limitée. Nous avons conçu notre solution de sécurité phare pour les PME, **Kaspersky Endpoint Security Cloud**, en nous concentrant sur des entreprises comme la vôtre, en réunissant tout ce dont vous avez besoin pour vous développer et prospérer dans le monde numérique.

Voici comment, à un coût abordable, nous vous fournissons le calme et la tranquillité d'esprit dont vous avez besoin pour développer votre entreprise.

Protection des terminaux de niveau mondial

Dans la section précédente, nous avons décrit le caractère crucial de la protection des terminaux de votre entreprise, quel que soit le système d'exploitation utilisé. Notre solution dispose de **tout ce dont vous avez besoin pour protéger les ordinateurs de bureau et les serveurs de fichiers Windows, les appareils Mac OS, les appareils mobiles iOS et Android ainsi que Microsoft Office 365**. Elle propose une interface unique et conviviale et ne requiert aucune formation. Une grande partie de la protection offerte, comme la correction des vulnérabilités, est facilement automatisable, ce qui permet de renforcer votre périmètre tout en réduisant le temps que vous passez à gérer la sécurité. De plus, la solution est si discrète que vous pourriez même oublier qu'elle est là.

« La solution Kaspersky Endpoint Security Cloud répond parfaitement aux exigences de mon entreprise et à celles de nos clients. Elle offre toute l'expertise et la technologie Kaspersky, sans exiger du temps et des ressources que les petites entreprises n'ont tout simplement pas. »[28]

PDG, CURAit

Les menaces que nous avons présentées précédemment, comme le phishing, les programmes malveillants et les vulnérabilités des terminaux, sont toutes couvertes par notre protection mise à jour en permanence – et vous pouvez nous croire quand nous disons qu'elle est fiable. Nos produits ont obtenu **518 premières places** (plus que n'importe quel concurrent) lors de tests indépendants entre 2012 et 2021, et nous sommes aujourd'hui le seul fournisseur à **bloquer 100 % des attaques de ransomwares**[29].

Nous reconnaissons également qu'au fur et à mesure que vous évoluez, votre maturité informatique évolue également. Nous voulons faciliter cette évolution et vous accompagner dans votre réussite. C'est pourquoi nos **licences Plus/Pro incluent Endpoint Detection and Response (EDR)**, un outil de niveau professionnel qui offre une visibilité sur les menaces, des outils d'enquête simples ainsi qu'une réponse automatisée permettant de détecter les menaces et d'en atténuer les effets. (Cela ne vous fera peut-être pas battre la chamade, mais vos nouveaux professionnels de la sécurité vous en seront reconnaissants).

Visibilité et contrôle complets des données

Comme nous l'avons souligné précédemment, l'un des aspects les plus importants de la cybersécurité aujourd'hui est la protection des données, qui commence par leur visibilité. Si vous ne connaissez pas les données que vous contrôlez, l'endroit où elles se trouvent et les personnes qui peuvent y accéder, vous ne pouvez pas en assurer la sécurité, et les régulateurs ne tarderont pas à vous le rappeler.

C'est pourquoi notre fonctionnalité **Data Discovery** propose des modèles préréglés qui vous permettent d'**identifier facilement les informations confidentielles**. Vous serez informé des partages dans Teams, OneDrive, SharePoint (presque tous les services Microsoft Office 365), ce qui vous permettra d'appliquer des mesures correctives pour préserver l'intégrité des données et répondre aux critères de conformité.

Vous reprendrez également le contrôle du cloud grâce à **Cloud Discovery**, qui permet d'atténuer les risques liés au travail à distance **en détectant et en limitant l'utilisation de ressources cloud inappropriées ou non autorisées**. Les sources de violation potentielle de données sont rapidement suivies et éliminées, vous aidant ainsi à maintenir la conformité. Et si un appareil est perdu ou volé, vous pouvez **protéger vos données grâce au chiffrement à distance**.

Les rapports continus de Kaspersky Endpoint Security Cloud et la résolution manuelle occasionnelle d'un partage risqué sont tout ce dont vous avez besoin pour rester en conformité.

L'étude de Kaspersky montre que 90 % des employés surestiment leurs capacités en matière de cybersécurité[32]

Capacités de gestion à distance, assistance en matière de stratégies et formation des employés

Vous avez constaté précédemment que les politiques, bien qu'elles constituent un élément important de votre stratégie de cybersécurité, ne suffisent pas à préserver une hygiène de sécurité au sein de l'organisation. Si l'un de vos employés trouve une clé USB dans un bus et décide de la brancher par curiosité (un exemple parfait de mauvaise pratique en matière de sécurité), vous pourriez être confronté à de gros problèmes. C'est pourquoi il est important de mettre en place les restrictions adéquates.

Kaspersky Endpoint Security Cloud vous permettra ce qui suit :

- Être partout et rester protégé à l'aide d'une console basée dans le cloud
- Assurer la sécurité des données de votre entreprise, même en cas de perte ou de vol d'un appareil
- Connaître les ressources que vos employés utilisent afin que vous puissiez décider des mesures à prendre
- S'assurer que les appareils mobiles hors de votre champ de vision restent sécurisés grâce à un riche ensemble de fonctionnalités de gestion et de chiffrement

Cela ne signifie pas qu'il faut suivre le moindre mouvement des utilisateurs (nous laissons cela à Big Brother), mais qu'il faut assurer un niveau de cybersécurité de base dans l'ensemble de votre organisation, de sorte que les erreurs commises par vos employés restent involontaires.

Vos professionnels de l'informatique et/ou de la sécurité peuvent également renforcer leurs compétences en suivant des modules interactifs dédiés, et ainsi réduire rapidement votre cyber+risque.

Formation dédiée à la cybersécurité avec Kaspersky Endpoint Security Cloud

Pour les entreprises ambitieuses et à croissance rapide, comme les startups, il est essentiel de développer très tôt une culture de la cybersécurité. Plus vous encouragez la transparence, l'aversion au risque et le développement personnel, plus vous avez de chances d'éviter les cyberattaques et les violations de données. Et dans le pire des cas, vous serez en mesure de réagir rapidement et de façon appropriée, en minimisant les conséquences sur le plan financier et opérationnel ainsi que sur la réputation de l'entreprise.

Une réponse optimale aux incidents informatiques peut même renforcer la réputation de votre organisation, car les clients et les investisseurs considèreront votre entreprise comme compétente et fiable. C'est le cas de Norsk Hydro, une entreprise d'énergie renouvelable qui a été saluée par Time[30] et Microsoft[31] pour sa résilience lors d'une attaque par ransomware. Toutefois, la seule façon de répondre à un cyberincident de cette ampleur est de disposer des compétences nécessaires. Les ressources des petites entreprises étant limitées, il est essentiel que vous fassiez le meilleur usage possible des aptitudes de votre personnel et que vous encouragiez ceux qui ont une prédisposition pour la cybersécurité (par exemple, ceux qui font preuve de créativité, de logique et de persévérance) à passer à l'étape suivante.

C'est pourquoi nous incluons une **formation à la cybersécurité** avec Kaspersky Endpoint Security Cloud sans frais supplémentaires. Voici les sujets inclus.

Compétences informatiques pour protéger votre entreprise

Vos spécialistes informatiques ont probablement suivi une formation de sensibilisation à la sécurité, mais n'ont pas encore atteint le niveau le plus avancé. Nous avons condensé les **cyber-compétences essentielles** dont votre entreprise a besoin pour se défendre en six modules accessibles : logiciels malveillants, programmes potentiellement indésirables (PUP) et exploits, principes de base des enquêtes, phishing et renseignements en sources ouvertes (OSINT), sécurité des serveurs et sécurité d'Active Directory.

Expertise mondiale

Profitez des connaissances de l'équipe GReAT (Global Research and Analysis Team) de Kaspersky, mondialement reconnue, qui a découvert des programmes malveillants, des ransomwares et bien d'autres menaces depuis 2008.

Formation continue

Notre formation n'est pas un exercice ponctuel, mais une activité régulière qui renforce votre hygiène quotidienne en matière de sécurité. Cette formation est le moyen idéal pour commencer à développer une culture de la sécurité au sein de votre personnel.

Sur demande et sans frais supplémentaires

Nos modules de formation, conçus par des experts, sont disponibles à la demande sans frais supplémentaires, ce qui permet à votre personnel de se former n'importe où et n'importe quand. Tout le contenu est disponible à partir d'un tableau de bord unique, sans qu'il soit nécessaire de s'inscrire.

Conclusion

Si vous êtes resté jusqu'au bout de ce guide consacré à la cybersécurité, vous devriez à présent bien comprendre les risques courants auxquels votre entreprise est confrontée, les raisons pour lesquelles elle est la cible d'attaquants et ce dont vous avez besoin pour la protéger. Il est essentiel de protéger votre entreprise de manière efficace et abordable pour rester compétitif sur les marchés actuels, et la première étape consiste à choisir la bonne solution de cybersécurité.

Il existe de nombreuses façons de protéger les différentes composantes de votre entreprise, mais pour les PME, aucune n'est plus complète que Kaspersky Endpoint Security Cloud, une solution qui permet de protéger les données de votre entreprise, de sécuriser les travailleurs à distance et d'améliorer les compétences humaines au sein de l'entreprise. Complet ne signifie pas pour autant complexe. Une installation rapide dans le cloud vous permet de bénéficier de la protection de Kaspersky en l'espace de quelques heures, avec une maintenance minimale par la suite. Une solution judicieuse pour les entreprises soucieuses du temps, des coûts et de la sécurité.

En savoir plus ou commencer votre essai gratuit de Kaspersky Endpoint Security Cloud

Bibliographie

1. IBM et Morning Consult. (2020, 22 juin). Étude sur le travail à domicile. IBM.
2. Grand View Research. (2021). Rapport sur la taille du marché de l'informatique dans le cloud. Grand View Research.
3. Département pour le numérique, la culture, les médias et le sport. (2022, 11 juillet). Statistiques officielles : Sondage sur les violations de la cybersécurité 2022. Gouvernement britannique.
4. Tidy, J. (2020, 16 décembre). SolarWinds : Pourquoi le piratage Sunburst est si grave. BBC.
5. Thomas, I. (2022, 16 décembre). Le FBI redoute une vague de cybercriminalité à l'encontre des petites entreprises américaines. CNBC.
6. Coveware. (2022, 26 octobre). Le verdict concernant Uber soulève de nouveaux risques pour les paiements de rançon. Coveware.
7. Département pour le numérique, les médias, la culture et le sport. (2022, 3 mai). Compétences en matière de cybersécurité sur le marché du travail britannique en 2022. Gouvernement britannique.
8. NCSC. À propos de Cyber Essentials. NCSC.
9. Verizon. (2022). Rapport d'enquêtes sur les violations de données de 2022. Verizon.
10. Thales. (2022). Étude de Thales sur la sécurité du cloud de 2022. Thales.
11. Numérique. (2022, 28 mars). 51 % des petites entreprises admettent ne pas sécuriser les données de leurs clients. Digital.
12. Alliance nationale pour la cybersécurité. (2020). Le PDG d'un hôtel trouve des intrus dans sa messagerie électronique. NIST.
13. Svistunova, O. (2022, 6 décembre). Principales tendances et techniques de phishing et d'escroquerie. Securelist.
14. Kaspersky. (2022, 18 novembre). Évolution des menaces informatiques au troisième trimestre 2022. Les statistiques n'incluent pas les appareils mobiles. Securelist.
15. Pankov, N. (2021, 12 mai). Comment Colonial Pipeline a géré son attaque par ransomware. Kaspersky.
16. BBC. (2021, 14 mai). Une société pétrolière américaine a payé une rançon de 5 millions de dollars à des pirates informatiques. BBC.
17. Nazarov, N. Davydov, V. Shornikova, N. Burtsev, V. Nasonov, D. (2022, 23 juin). Les huit salopards : Le guide de Kaspersky sur les tactiques, techniques et procédures des ransomwares modernes. Securelist.
18. The Ponemon Institute. (2022). Coût des menaces internes en 2022 : Rapport mondial. Proofpoint.
19. Kaspersky Lab. Reconnaître les différents types d'initiés. Kaspersky.
20. Loukides, M (2021, 7 décembre). Le cloud en 2021 : l'adoption se poursuit. O'Reilly.
21. IBM. (2022). Rapport sur le coût d'une violation de données. IBM.
22. Suivi de l'application du RGPD. ETid-752. CMS.Law.

23. Suivi de l'application du RGPD. ETid-1318. CMS.Law.

24. Suivi de l'application du RGPD. ETid-876. CMS.Law.

25. Posey, C & Shoss, M. (2022, 20 janvier). Recherche : Pourquoi les employés violent les stratégies de cybersécurité. Harvard Business Review.

26. Kaspersky. (octobre 2021). Le bien-être des employés 2021 : apprendre de la nouvelle réalité. Kaspersky.

27. Burn, J. (2022, 2 novembre). Reconnaître notre relation d'amour-haine avec les certifications de sécurité. Forrester.

28. Kaspersky Lab. Kaspersky Endpoint Security Cloud. Kaspersky.

29. Kaspersky. (2022, 19 juillet). AV-TEST constate que les solutions de sécurité Kaspersky pour les entreprises offrent une protection à 100 % contre les ransomwares. Kaspersky.

30. Austin, P. (2021, 14 juillet). Cette entreprise a été victime d'une attaque par ransomware dévastatrice, mais au lieu de céder, elle a tout reconstruit. TIME.

31. Briggs, B. (2019, 16 décembre). Des pirates informatiques attaquent Norsk Hydro via un ransomware. L'entreprise a réagi en toute transparence. Microsoft.

32. Kaspersky. (2022, 25 octobre). Neuf employés sur dix ont besoin d'une formation de base en matière de cybersécurité. Kaspersky.

Plus de 25 ans
d'expérience
dans le secteur
de la cybersécurité

Plus de 400 millions
de clients utilisent
nos produits dans
le monde entier

Plus de 200 pays
distribuent nos solutions

À propos de Kaspersky

Kaspersky protège plus de 400 millions d'utilisateurs et 240 000 entreprises. Est. 1997.

Nous sommes une entreprise internationale privée dont la société holding est établie au Royaume-Uni.

Nous transformons nos connaissances de pointe dans le domaine de la sécurité en une protection réelle pour nos clients, en rendant plus sûre et plus fiable l'utilisation des technologies au quotidien et dans un contexte professionnel.

En savoir plus sur
Kaspersky Endpoint Security Cloud

Kaspersky
Endpoint Security
Cloud

Actualités des cybermenaces : securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.fr
Sécurité informatique pour les PME : kaspersky.com/business
Sécurité informatique pour les entreprises : kaspersky.com/enterprise

kaspersky.fr

Obtenez votre version d'essai OFFERTE de 30 jours sur **cloud.kaspersky.com**

Si vous décidez de conserver Kaspersky Endpoint Security Cloud, il vous suffira de payer la licence : inutile de redéployer des logiciels de terminaux.