Repensez votre stratégie de cybersécurité pour qu'elle s'adapte à ce nouveau monde

5 étapes pour sécuriser l'entreprise et se préparer à un avenir incertain

avanade

Repensez votre stratégie de cybersécurité pour qu'elle s'adapte à ce nouveau monde

La pandémie de COVID-19 a touché l'ensemble des secteurs, des entreprises et des employés. Ce que nous achetons, la façon dont nous vivons et celle dont nous travaillons ont **changé à jamais** et plus rapidement que nous aurions pu l'imaginer.

De nombreuses organisations ont dû mettre en œuvre de nouveaux modèles d'exploitation peu familiers et déployer rapidement des technologies qui prennent en charge ce nouvel environnement pour assurer la continuité des activités.

Les organisations repensent leur façon de procéder. Pour ce faire, nous vous encourageons à vous concentrer sur ces priorités clés : la maîtrise des coûts, la responsabilisation de vos employés, la protection des activités essentielles de votre entreprise, la prise en charge des besoins de vos clients et la réponse aux changements qui affectent votre portefeuille de produits. La mise en place d'une activité sûre et résiliente est essentielle à la réalisation de ces priorités.

Les récentes évolutions, telles que l'augmentation du travail à distance, signifient que les organisations sont confrontées à des défis de sécurité plus importants, avec une surface d'attaque plus large et une plus grande exposition aux menaces. Pour beaucoup, leur attitude face au risque a fondamentalement changé. C'est le moment idéal pour repenser votre stratégie de sécurité. Dans ce guide, nous allons décrire les étapes clés qui vous aideront à y parvenir - afin que vous puissiez protéger les activités essentielles de votre entreprise et permettre à vos employés de travailler en toute sécurité dans ce nouvel environnement.

Les cyberattaquants **profitent** de cette exposition accrue. Selon une nouvelle étude de **Microsoft**, les hackers ont lancé des cyberattaques liées au thème du coronavirus dans **241 pays** et **territoires.**

avanade

« … Nous considérons ces temps difficiles comme une occasion de repenser notre façon de faire des affaires… Il s'agira notamment de transformer votre entreprise afin d'améliorer l'expérience client et l'efficacité des opérations. »

MIT Sloan Centre for information Systems Research
mardi 31 mars 2020

La crise mondiale **exacerbe** les problèmes de sécurité

Dans cette nouvelle ère, les entreprises sont **confrontées** à de plus grands défis en matière de sécurité :

Ingénierie sociale

Les attaquants exploitent les craintes liées à la crise et utilisent le COVID-19 pour lancer des campagnes de phishing et diffuser des programmes malveillants. Ces types d'attaques ont connu une forte augmentation et cela va probablement se poursuivre.

Personnel à distance

L'augmentation du télétravail s'accompagne de risques liés à la sécurisation des appareils personnels, à la faiblesse des mots de passe, au Wi-Fi domestique mal sécurisé, aux routeurs et aux correctifs des systèmes distants. Les employés collaborent également de différentes manières à l'intérieur et à l'extérieur de l'entreprise, en utilisant souvent des plates-formes sensibles.

Cela a provoqué des vulnérabilités exploitables dans les outils de collaboration, entraînant une mauvaise expérience pour l'utilisateur et des préoccupations concernant la vie privée et la confidentialité. Les responsables de la sécurité sont également confrontés à une augmentation des coûts informatiques associés à la main-d'œuvre, avec une utilisation accrue des réseaux et des infrastructures.

Absence d'accès sécurisé

Les méthodes de contrôle de l'identité et de l'accès n'ont pas été à la hauteur des nouveaux modes de travail, notamment le télétravail et les périphériques multiples, avec une incapacité d'accéder aux applications clés. La quantité de données partagées s'est également multipliée et, par conséquent, de nombreuses entreprises se demandent si elles disposent de l'infrastructure et des mesures de contrôle de l'identité appropriées pour permettre à leurs employés d'accéder en toute sécurité aux informations dont ils ont besoin. Les collaborateurs à distance et les modèles d'entreprise à distance deviendront la nouvelle norme. Les biens et services seront échangés numériquement via l'économie de l'API, ce qui augmentera encore la surface d'attaque potentielle et les risques associés.

Manque d'agilité

La demande sans précédent d'accès à distance aux ressources des entreprises a mis une pression supplémentaire sur les points d'accès et les services de réseau privé virtuel (VPN). De nombreuses organisations n'ont pas été en mesure d'adapter en toute sécurité les systèmes et l'infrastructure VPN existants pour répondre à l'évolution des besoins, ce qui a affecté l'expérience et la capacité de travail des utilisateurs.

Microsoft suit quotidiennement **60 000** pièces jointes ou URL **malveillantes**

Naviguez à travers les méandres du changement

Nous prévoyons que les organisations traversent **trois vagues de changement**. Il est impératif que vous commenciez à prendre les bonnes mesures dès maintenant, afin **de protéger** les opérations essentielles de votre entreprise et de développer une activité **résiliente** et **évolutive**, adaptée à un avenir flexible.

Réagir

De nombreuses entreprises commencent à émerger de cette première phase. Au cours de cette période, les organisations ont surtout cherché à assurer la continuité des activités en permettant aux employés de travailler, aux clients d'accéder aux biens et aux services tout en maintenant leurs activités de base et leur chaîne d'approvisionnement.

Avec le passage au travail à distance, il est important de comprendre l'évolution de la position de votre entreprise face au risque.

Relancer

Nous voyons déjà de nombreux clients dépasser la phase de réaction pour adopter un état d'esprit de relance, afin de gérer le ralentissement économique en tant qu'entreprise plus légère et plus agile. Cela suppose probablement une reconfiguration du portefeuille de produits et la création rapide d'un modèle d'exploitation évolutif pour répondre à l'évolution des besoins du marché et des employés.

Au cours de cette phase, nous vous recommandons d'entreprendre une évaluation complète des risques, afin d'établir des priorités sur la manière de traiter les risques de sécurité identifiés, en commençant par les lacunes de sécurité les plus immédiates. En outre, vous devrez prévoir un cadre de sécurité fondé sur des architectures de confiance zéro et une réduction des coûts.

Renouveler

Au cours des 12 à 18 prochains mois, nous nous attendons à ce que les entreprises se préoccupent de plus en plus de la manière dont elles peuvent se renouveler et se positionner pour l'avenir. Elles chercheront à réinventer leur modèle pour répondre aux opportunités existantes et nouvelles avec une version plus robuste et plus résiliente.

Du point de vue de la sécurité, vous devez chercher à vous adapter en permanence à l'évolution du contexte business et à rester en conformité, en veillant à ce que toute modification des modèles, des technologies et des processus respecte les exigences réglementaires, ainsi que les nouvelles exigences de conformité. Ce serait également le moment idéal pour mettre en œuvre une nouvelle conception de la sécurité, basée sur une feuille de route solide qui soit cohérente avec les exigences de votre entreprise et de votre position face au risque.

5 étapes pour **repenser** votre stratégie de sécurité

Au cours de ces trois phases, il peut être difficile de savoir par où commencer pour vous assurer que vous prenez les mesures nécessaires afin de sécuriser votre entreprise maintenant et à l'avenir.

Nous vous présentons cinq étapes pour vous aider à vous lancer.

1. Adoptez une vision et un état d'esprit de **confiance zéro**

Ce concept repose sur la conviction qu'une organisation ne doit pas automatiquement faire confiance à quoi que ce soit venant de l'intérieur ou de l'extérieur de son périmètre et que tout doit être vérifié avant d'accorder l'accès aux systèmes. L'identité de chaque individu, compte administrateur, application, robot et processus doit être validée et gérée par le biais d'un processus de contrôle.

Nous vous recommandons également de vous doter d'outils qui répondent à vos besoins en matière de contrôle et d'administration de l'identité (IGA). L'accès aux services numériques à partir de différents lieux et plates-formes cibles doit être évalué en permanence pour soutenir les objectifs de résilience et de continuité des activités.

avanade

Étude de cas

Une sécurité de premier ordre pour exploiter pleinement le potentiel de l'environnement de travail

Défi : notre client voulait mettre en oeuvre un environnement de travail numérique évolutif et introduire une expérience de pointe pour les employés, avec une infrastructure sécurisée.

Solution : nous avons mis en œuvre un environnement de travail moderne sécurisé basé sur Microsoft 365, qui propose un large éventail de solutions, allant des services cloud sécurisés à un environnement de travail mobile et une solution collaborative de premier ordre.

Résultats : l'entreprise constate aujourd'hui que le projet donne des résultats convaincants :

- Deux principes clés **de sécurité**, l'« identité comme plan de contrôle » et l'approche « confiance zéro », sont pleinement pris en charge.
- Les employés sont plus **productifs** et peuvent profiter de la même expérience de travail sur divers appareils à distance et en toute sécurité.
- Des plates-formes de travail sécurisées et évolutives ont aidé le client à accélérer le délai de commercialisation et à améliorer **l'efficacité** de ses services informatiques.
- L'**expérience des employés** s'est considérablement améliorée, avec une collaboration accrue et la capacité de prendre de meilleures décisions commerciales.

2. Entreprenez une **évaluation complète des risques**

Si, comme de nombreuses entreprises, vous avez récemment subi une **évolution rapide** de l'architecture de votre entreprise et le déploiement de nouveaux outils de collaboration et de travail, le moment est venu de procéder à une évaluation des risques de votre environnement.

Il est difficile d'évaluer les risques dès le début, il convient donc de commencer par identifier les biens les plus précieux et de comprendre ce que vous voulez protéger. À partir de là, vous serez en mesure d'identifier les principaux risques liés à ces actifs et élaborer un plan tactique pour y faire face.

avanade

3. **Hiérarchisez** les projets, les budgets et les ressources de sécurité

La compréhension des risques pour votre écosystème nouvellement modifié vous permettra d'adopter une approche **mesurée** et **réfléchie** en matière de priorités, de ressources et de budget pour les projets de sécurité.

C'est également un bon moment pour examiner ou élaborer un cadre formel de gouvernance de la sécurité afin de s'assurer que votre nouveau modèle opérationnel est cohérent avec votre nouvelle position face au risque.

Comme pour la plupart des choses, il ne suffit pas d'investir de l'argent pour régler les problème de sécurité. Une approche axée sur les risques vous aidera à cibler votre budget et vos ressources. Beaucoup d'entreprises accordent désormais la priorité à leurs dépenses de sécurité dans les projets de transformation digitale et de migration vers le cloud afin de prendre en charge les employés à distante.

IDC a récemment signalé qu'on pouvait s'attendre à ce que les dépenses en matière de services professionnels et gérés liés à la sécurité restent élevées alors que les organisations tentent de maintenir leurs opérations pendant la crise de COVID-19. Cela souligne l'importance de la sécurité en tant que priorité stratégique pour les organisations par rapport aux autres domaines de l'informatique.

Selon IDC, le COVID-19 contribuera à souligner l'importance de disposer de plans de **réaction aux incidents** et de **résilience** en cas de crise.

Impact du COVID-19 sur les projections d'IDC
Dépenses relatives aux services de sécurité
13 avril 2020

4. **Simplifiez** et **améliorez** votre environnement de sécurité

Une approche à plusieurs niveaux de la sécurité avec les bons outils est essentielle, mais il faut aussi chercher **des opportunités** de réduire les contrôles inutiles.

Les architectures de sécurité excessivement hétérogènes sont difficiles à gérer, coûteuses et peuvent augmenter votre risque d'exposition. Il est donc important de tirer parti de toutes les fonctionnalités intégrées à la plate-forme de votre fournisseur de cloud.

Cette fonction est particulièrement utile lorsque vous devez réagir rapidement à une situation, par exemple pour permettre à une équipe distante de travailler. Veillez à tirer pleinement parti des fonctionnalités de sécurité intégrées, telles que celles incluses dans Microsoft 365, ce qui contribuera à réduire les coûts inutiles.

avanade

5. **Renouvelez-vous** pour concrétiser votre vision de la sécurité à long terme

Nous vous recommandons de mettre en œuvre une approche **globale** de la sécurité et d'en faire dès le départ un élément de la transformation digitale de votre organisation.

Intégrez la sécurité dans les solutions et les applications informatiques, plutôt que d'essayer d'y remédier avec la toute dernière solution de cybertechnologie, qui pourrait bientôt devenir superflue.

Quels que soient les systèmes que vous mettez en place, assurez-vous qu'ils sont sécurisés du point de vue du cloud et des applications et que vous avez une bonne compréhension du niveau de responsabilité que le prestataire (et vous) assumera, afin de garantir la sécurité dès la conception.

La sécurité doit être un facteur de développement de l'entreprise. Essayez donc d'équilibrer la sécurité et les contrôles pour éviter d'ajouter des obstacles et de nuire à la productivité des employés. Cela permettra à votre organisation de fonctionner avec agilité et de se préparer à la prochaine étape.

Faites du renforcement de la culture de la sécurité une priorité. Une formation et un enseignement complets et cohérents vous aideront à faire face aux risques de sécurité inhérents au comportement des employés. Cela peut nécessiter une approche de gestion du changement soutenue par un enseignement continu et une formation fondée sur les rôles des individus.

avanade

Pourquoi **Avanade** ?

Pour être leader sur le marché actuel, il faut adopter une approche de **l'extérieur vers l'intérieur** (outside-in)

Chez Avanade, nous avons activement aidé nos clients pendant cette période difficile. Depuis le déclenchement de la pandémie de COVID-19, nous avons migré plus **d'un million de comptes de travail à distance** pour nos clients. Nous aidons maintenant ces entreprises à adopter un nouveau modèle d'exploitation sécurisé, conçu pour les rendre adaptables et les protéger à l'avenir. Nos experts vous aideront à sécuriser vos écosystèmes informatiques Microsoft et hybrides.

Nos services de sécurité offrent une approche globale par le biais de services de conseil, de déploiement et de gestion. Nous pouvons vous aider à effectuer une **évaluation des risques** et à mettre en œuvre une **architecture sécurisée**. En tant que fournisseur de sécurité gérée, nous pouvons également **renforcer** votre équipe de sécurité et assurer la surveillance des événements 24 h/24, 7 j/7, ainsi qu'un **soutien opérationnel** continu pour vous aider à anticiper les risques de sécurité.

Nous proposons des méthodologies éprouvées, une expertise approfondie et une technologie de pointe, en tant que partenaire SI Microsoft Alliance de l'année depuis 14 ans.

AVANADE IS GOLD FOR MICROSOFT'S SECURITY COMPETENCY

MICROSOFT SECURITY 20/20 SECURITY ADVISORY OF THE YEAR WINNER

MICROSOFT PARTNER FOR OFFICE 365 FOR TEN CONSECUTIVE YEARS

MICROSOFT ALLIANCE PARTNER OF THE YEAR FOR 14 YEARS

avanade

Commencez dès **aujourd'hui**

Si, comme beaucoup de nos clients, vous avez dû **rapidement développer** le travail à distance, un bon point de départ est notre évaluation de la sécurité et notre workshop.

En collaboration avec vous, nous étudierons les moteurs de votre activité, l'infrastructure et les processus existants afin de procéder à une évaluation globale de votre environnement de sécurité et créer une feuille de route qui vous aidera à réaliser votre vision de la sécurité sur le long terme.

Nous proposons les services suivants :

Évaluation et workshop de sécurité Microsoft 365

- Nous évaluons votre environnement Microsoft 365 actuel du point de vue de la sécurité afin d'identifier les lacunes et les domaines de correction.
- Nous proposons une analyse et une feuille de route complètes basées sur les contrôles de sécurité et les exigences de votre entreprise.
- Un rapport et un tableau de bord Secure Score fournissent des détails sur la protection et la gouvernance des données.
- Une évaluation globale fournit des orientations sur l'atténuation des risques évolutifs en matière de cybersécurité.

Évaluation de l'infrastructure et des processus d'identité

- Nous fournissons une évaluation complète et une détection automatisée des risques.
- Nous évaluons votre infrastructure pour vous recommander des améliorations.

Contactez-nous pour en savoir plus ou rendez-vous sur **avanade.com/security**

Amérique du Nord
Seattle
Téléphone : +1 206 239 5600
America@avanade.com

Amérique du Sud
Sao Paulo
AvanadeBrasil@avanade.com

Asie-Pacifique
Australie
Téléphone : +61 (2) 9005 5900
AsiaPac@avanade.com

Europe
Londres
Téléphone : +44 (0) 20 7025 1000
Europe@avanade.com

France
Issy-les-Moulineaux
Téléphone : +33 (0) 1 81 89 89 00
Nous contacter >>

À propos d'Avanade

Avanade est le premier intégrateur mondial de solutions digitales innovantes fondées sur l'écosystème Microsoft. Forte de 38 000 professionnels dans 25 pays et acteur stratégique de l'Accenture Microsoft Business Group, Avanade accompagne les entreprises de tous secteurs d'activité, en favorisant une culture collaborative respectant la diversité. Détenue majoritairement par Accenture, Avanade a été fondée en 2000 par Accenture LLP et Microsoft Corporation. Pour en savoir plus : www.avanade.com/fr-fr

avanade


avanade