Les tendances en sécurité et gestion des risques à surveiller en 2021 selon Gartner

HUIT TENDANCES ONT ÉTÉ REGROUPÉES

Gartner dévoilait récemment la liste des tendances en sécurité et gestion des risques qui devraient modifier les façons de faire dans les entreprises au courant de l'année. Au total, huit tendances ont été regroupées sous trois catégories :

- **La sécurité indépendante de l'emplacement**, qui est liée à la hausse du télétravail et au fait que l'identité (et non l'emplacement) soit maintenant le périmètre de facto de l'entreprise.
- **L'évolution de la sécurité sur le plan organisationnel**, qui met l'accent sur l'évolution des processus en matière de risques, notamment par rapport aux employés (le fait de nommer des experts en cybersécurité à des postes de direction) et à l'infrastructure (le fait de consolider plusieurs produits de sécurité au sein de plateformes de sécurité uniques et centralisées).
- **L'évolution des technologies de sécurité**, qui se concentre sur les façons d'améliorer la confidentialité, la sécurité et la conformité à mesure que le travail migre vers le nuage.

Sans tenir compte de l'ordre de priorité, voici les huit tendances telles que répertoriées dans le rapport. Pour chaque tendance, nous avons ajouté les recommandations de Gartner à l'intention des gestionnaires informatiques responsables de la sécurité et de la gestion des risques.

Tendance : la sécurité indépendante de l'emplacement

1. Le maillage de cybersécurité

La pandémie de COVID-19 a accéléré la délocalisation des utilisateurs finaux et des actifs numériques, nous menant vers une approche moderne de la sécurité de l'information (aussi appelée maillage). Dans cette approche, les contrôles sont exécutés là où ils sont le plus nécessaires, de façon flexible, évolutive, résiliente et modulable (c'est-à-dire que les composantes peuvent être sélectionnées et assemblées selon plusieurs combinaisons pour répondre aux exigences spécifiques des entreprises).

Généralement, l'architecture de maillage est déployée à même le nuage (quoique des déploiements sur site soient également possibles). L'utilisation du nuage public prend en charge divers points d'exécution pouvant être associés à différents actifs. Ce modèle permet aux fournisseurs SaaS d'offrir aux clients des services fiables et performants.

Gartner recommande aux responsables TI de se concentrer sur les stratégies de maillage suivantes :

- Concentrez vos efforts, ressources et investissements vers des contrôles de cybersécurité infonuagiques et indépendants de l'emplacement.
- Choisissez des technologies de renseignement et d'analyses de sécurité extensibles (la structure interne et le flux des données ne devraient pas être affectés par l'ajout ou la modification de fonctionnalités) et interopérables (qui permettent la connexion et l'intégration de divers outils dans l'écosystème).
- Développez des modèles adaptatifs qui offrent des accès sécurisés et performants pour les applications infonuagiques.

- Choisissez des fournisseurs qui ont ouvert leurs politiques, question de ne pas obliger les entreprises à prendre des décisions stratégiques dans différents outils.

2. La sécurité axée sur l'identité

La gestion des identités et des accès (IAM) n'a rien de nouveau. Par contre, ce qu'il faut savoir, c'est que la COVID-19 l'a fait passer de « bonne pratique » à une « exigence quotidienne ». Effectivement, les entreprises ne fonctionnent plus dans un monde où c'est l'emplacement qui détermine le niveau (ou l'absence) des contrôles de sécurité. Maintenant, c'est toutes les ressources, applications, outils et zones de réseau qui sont considérés comme étant potentiellement vulnérables et à risque.

Gartner recommande aux responsables des TI de se concentrer sur les stratégies d'identité suivantes :

- Adoptez des contrôles comme l'authentification unique (SSO), l'authentification multifacteur et les réseaux Confiance zéro. Pour améliorer la visibilité et la sécurité, certaines entreprises peuvent également opter pour des proxys et des courtiers de sécurité d'accès au nuage (CASB).
- Auditez tous les cas d'utilisation des accès à distance et créez des architectures de référence pour les sécuriser.
- Examinez toutes les pratiques de journalisation, les processus et procédures de sécurité et, si nécessaire, augmentez la visibilité et le contrôle. L'idée, c'est d'être proactif plutôt que réactif.
- Déterminez si vous possédez suffisamment de talents spécialisés en cybersécurité à l'interne pour soutenir ces stratégies (et les autres). Sinon, faites du recrutement une priorité. Étant donné que la pénurie de main-d'oeuvre qualifiée en cybersécurité continue de prendre de l'ampleur, les entreprises, surtout les PME, sont encouragées à s'associer à un fournisseur de services gérés.

3. Le télétravail est là pour de bon

Le télétravail sous toutes ses formes existe depuis plusieurs années. Bien avant que survienne la pandémie, bon nombre d'employés et sous-traitants travaillaient à distance. La COVID-19 a cependant accéléré la migration vers le travail à distance. Bien que, dans certaines régions du monde, les bureaux accueillent progressivement les travailleurs, plusieurs d'entre eux resteront à la maison, du moins à temps partiel.

Résultat : les entreprises doivent réinventer leurs politiques et outils de « l'avant pandémie » pour leur donner un nouveau sens dans un environnement post-pandémique. Il faut développer des cas d'utilisation solides qui :

- Définissent les différents utilisateurs finaux (rôles et fonctions).
- Identifient le type d'appareils dont disposent les utilisateurs finaux (et à qui ils appartiennent).
- Déterminent à quelles applications, données et zones du réseau les utilisateurs finaux doivent accéder.
- Identifient où sont localisés les utilisateurs finaux.

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour mieux soutenir les travailleurs à distance (y compris les travailleurs hybrides à distance/sur site) :

- Profitez des architectures de sécurité modernes comme le maillage de cybersécurité et la sécurité axée sur l'identité (toutes deux décrites ci-dessus).
- Impliquez vos gestionnaires dans le choix des nouvelles technologies.
- Réduisez le risque de perte de données (intentionnelle ou accidentelle) en établissant des procédures pour contrôler l'accès aux applications et aux données et en définissant les contrôles de sécurité qui doivent être mis en place pour régir leur accès.
- Créez plusieurs profils de sécurité. Utiliser une formule générique du genre « one size fits all », ce n'est jamais une bonne idée.
- Envisagez des mesures qui encadrent un travail à distance pouvant être 100 % déconnecté du LAN. Pour faire simple : prenez chaque décision en ayant à l'esprit que le télétravail est là pour de bon.

Tendance : l'évolution de la sécurité sur le plan organisationnel

4. Un conseil d'administration bien informé

Les entreprises accordent de plus en plus d'attention à la cybersécurité, surtout depuis qu'ont été mises sous le projecteur des infractions de grande envergure comme l'attaque Solorigate. Elles se rendent compte, aussi, que peu de leurs dirigeants sont suffisamment qualifiés pour évaluer les risques de cybersécurité. Pour combler cette lacune, certaines entreprises ajoutent à leur conseil d'administration des spécialistes en la matière et vont même jusqu'à créer des comités exécutifs de cybersécurité.

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour soutenir un conseil d'administration compétent en matière de cybersécurité :

- Démystifiez les tendances du marché et les priorités de votre conseil d'administration pour aligner (dans la mesure du possible) les besoins de l'entreprise avec vos objectifs de cybersécurité.
- Demandez l'avis de parties prenantes d'expérience. Ces personnes clés pourront vous conseiller sur les changements à surveiller au conseil d'administration.
- Vulgarisez les risques de cybersécurité pour les personnes qui ont moins de connaissances en la matière, par exemple en recadrant vos observations et recommandations dans un contexte commercial.

5. La consolidation des fournisseurs de sécurité

Bien que la diversité soit un avantage au sein d'une entreprise, l'utilisation d'un trop grand nombre de produits de sécurité augmente non seulement la complexité, mais aussi les coûts. À défaut de pouvoir optimiser les fonctionnalités des outils existants, les entreprises en viennent souvent à accumuler les solutions, créant ainsi des doublons. Consolider les fournisseurs de sécurité simplifie les opérations tout en répondant aux exigences réglementaires et de conformité.

À ce sujet, Gartner précise que consolider les fournisseurs de sécurité n'exclut pas les risques pour autant, notamment : informations limitées sur les menaces potentielles, manque d'intégration des produits, verrouillage des fournisseurs ou conditions logiciels qui se chevauchent. Même les meilleurs fournisseurs de sécurité peuvent ne pas atteindre ce niveau d'excellence pour l'ensemble de leurs produits.

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour soutenir la consolidation des fournisseurs de sécurité :

- Ne vous attendez pas à ce que la consolidation se fasse du jour au lendemain. Ce genre de projet peut prendre jusqu'à deux ans à voir le jour.
- Analysez les facteurs internes et externes qui déclenchent votre besoin de consolider vos fournisseurs.
- Au moment de l'évaluation, misez plutôt sur un ensemble de paramètres comme la simplification des opérations, la réduction du coût des droits de propriété, la réduction du coût total de la sécurité et l'amélioration de la posture de risque.
- Travaillez avec plusieurs parties prenantes d'expérience, y compris les directeurs des systèmes d'information, ainsi que les responsables et les chefs de la sécurité, pour développer une stratégie et une approche personnalisées. Votre feuille de route doit être réaliste.
- Formez les employés sur la bonne façon d'utiliser les nouveaux produits de sécurité à leur plein potentiel. C'est à la fois un projet d'approvisionnement et un défi de gestion du changement.
- Supprimez complètement les produits qui ne vous sont plus utiles. Ne gardez pas des produits parce qu'ils représentent des coûts irrécupérables ou sous prétexte que « ça a toujours été comme ça ».

Tendance : l'évolution des technologies de sécurité

6. Les technologies pour améliorer la confidentialité (TAC)

Les fonctions comme le partage de données multipartite, le traitement des données et l'analyse des environnements non fiables sont de plus en plus complexes et risquées face à l'expansion des réglementations et de la législation en matière de confidentialité à l'échelle régionale (pays) et mondiale. Historiquement, les

tentatives d'établir une protection des données en cours d'utilisation (par opposition à la protection des données au repos ou en mouvement) ont toujours été difficiles.

La technologie améliorant la confidentialité est un concept qui vise à exploiter les technologies émergentes pour protéger les données utilisées au sein d'environnements fiables et non fiables. Gartner souligne trois niveaux sur lesquels les TAC peuvent être appliqués : au niveau des données (incluant les transformations comme la confidentialité différentielle et les transformations pour masquer les valeurs de données individuelles); au niveau logiciel (le fait de combiner des logiciels spécialisés avec des transformations de données); et au niveau matériel (mise en place de systèmes matériels sécurisés et d'environnements d'exécution fiables).

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour soutenir les technologies améliorant la confidentialité :

- Évaluez les activités de traitement des données qui utilisent des données personnelles. L'objectif est d'identifier les cas d'utilisation pour des TAC.
- Explorez la viabilité de plusieurs modèles comme le chiffrement homomorphe, le calcul multipartite sécurisé, le protocole *Private Information Retrieval*, etc.
- Expérimentez plus tôt que tard pour assurer une préparation à long terme.
- Établissez votre budget dès maintenant. Ça vous évitera des obstacles financiers au moment de l'approvisionnement et de la mise en œuvre.

7. La simulation de cyberattaques

Les cyberattaques d'aujourd'hui sont beaucoup plus coûteuses et dévastatrices qu'autrefois. Dans le passé, les pirates informatiques se concentraient surtout sur la destruction des appareils. Aujourd'hui, ils priorisent le vol de données et d'identités. Pour les empêcher d'envahir les terminaux et les réseaux, les entreprises doivent mettre leurs systèmes à l'épreuve. C'est là qu'entrent en jeu les outils de simulation de cyberattaques.

Ces outils évaluent constamment la posture défensive d'une entreprise, ce qui inclut l'état de préparation de ses produits de sécurité, de même que les effectifs. Même si ces outils sont très importants, ils doivent être utilisés de pair avec d'autres outils d'évaluation des menaces, dont les tests d'intrusion, les primes aux bogues et l'analyse/hiérarchisation des vulnérabilités.

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour les simulations de cyberattaques :

- Alignez les tests avec le déploiement et les mises à niveau des systèmes clés, des applications et de la nouvelle infrastructure.
- Mettez en œuvre des exercices spécialisés qui vont révéler les chemins potentiels des pirates vers les actifs de grande valeur.

- Profitez de l'occasion pour évaluer l'efficacité des contrôles de sécurité, des capacités de détection et des plans de réponse aux incidents.
- Profitez-en pour mieux prioriser vos futurs investissements.

8. La gestion des identités des machines

Les entités non humaines renforcées par l'intelligence artificielle et l'apprentissage automatique, dont les appareils, applications, passerelles, services infonuagiques, machines virtuelles, RPA / bots et autres solutions SaaS et IaaS, sont à l'avant-scène de la transformation numérique. Pour gérer les identités des machines – et donc la sécurité – il faut établir la confiance. Cette approche comprend l'utilisation de clés, de certificats X.509, de secrets et d'autres matériels cryptographiques.

Gartner recommande aux responsables TI de se concentrer sur les stratégies suivantes pour assurer la gestion des identités des machines :

- Déterminez comment la propriété et les informations d'identification des appareils doivent être gérées au sein de l'entreprise.
- Déterminez les cas d'utilisation actuels de la gestion identités des machines. Puis, comparez-les avec ceux pouvant être évalués.
- Intégrez les exigences réglementaires dans les cas d'utilisation existants et à venir.

Ce qui s'en vient

Après avoir vécu une année comme 2020, la seule chose qu'on peut prévoir en 2021, c'est l'incertitude. C'est dans le chaos et le changement que ces huit tendances Gartner changeront l'histoire de la sécurité et de la gestion des risques. Chose certaine, les entreprises qui adopteront ces stratégies se trouveront dans une position beaucoup plus sûre et avantageuse dans les années à venir.

Pour en savoir plus, téléchargez le rapport complet de Gartner : https://www.gartner.com/en/publications/security-risk-top-priorities-for-it-leadership-vision-2021. Le téléchargement est gratuit, mais une adresse courriel professionnelle vous sera demandée.