Gartner publie les 10 meilleurs projets de sécurité pour 2019

Devolutions

LES ENTREPRISES POURRONT ACCROÎTRE LEUR IMPACT COMMERCIAL TOUT EN RÉDUISANT LEURS RISQUES.

Gartner a fait paraître son top 10 des projets de sécurité pour 2019. Il s'agit de mesures que devraient adopter au plus vite les organisations qui ont déjà implanté des mesures de sécurité fondamentales. Selon la firme de conseil et de recherche, en adoptant ces mesures, les entreprises pourront accroître leur impact commercial tout en réduisant leurs risques.

1. Gestion des accès privilégiés (PAM)

Le link:https://info.varonis.com/hubfs/2018 Varonis Global Data Risk Report.pdf[rapport Global Data Risk de 2018] a révélé que 88 % des entreprises qui comptent plus d'un million de dossiers ne disposent pas de limitations d'accès appropriées, tandis que 58 % d'entre elles ont plus de 100 000 dossiers accessibles à tous les employés. De plus, un sondage distinct réalisé par Centrify auprès de professionnels des TI a révélé que près des deux tiers de toutes les infractions concernent l'accès à des comptes privilégiés. Gartner recommande que les projets PAM incluent à la fois des systèmes et des comptes humains et non humains. Ils devraient également prendre en charge une combinaison d'infrastructures infonuagiques, sur site et hybrides, ainsi que des interfaces de programmation applicative (API) pour l'automatisation.

Les solutions PAM disponibles actuellement sur le marché sont très dispendieuses et la plupart des PME ne peuvent pas justifier une telle dépense. De plus, celles qui peuvent se permettre l'achat d'un tel outil n'ont habituellement pas l'expertise technique interne pour comprendre les différences entre les exigences de base et les parties non essentielles d'une solution PAM.

Chez Devolutions, nous nous sommes donné comme mission de changer cela et nous sommes heureux d'avoir lancé une plateforme PAM robuste et complète, spécialement conçue pour les PME.

2. Gestion de la vulnérabilité via la méthode CARTA

Évaluation continue adaptative du risque et de la confiance (de l'anglais Continuous Adaptive Risk and Trust Assessment ou CARTA) incite les équipes de sécurité à adapter continuellement leur approche en matière de sécurité, puisqu'il est tout simplement impossible de maîtriser toutes les vulnérabilités. Gartner conseille aux entreprises qui adoptent l'approche CARTA de commencer par établir la valeur de leurs actifs informatiques et des risques qui y sont associés, puis de bien comprendre la topologie du réseau et les modifications apportées à l'infrastructure. Cette dernière exigence est un défi de taille. Un récent sondage a d'ailleurs démontré que seulement 64 % des décideurs TI connaissent l'ensemble de leur portefeuille de logiciels et que 66 % estiment que leurs logiciels sont à jour.

3. Détection et intervention

Les capacités de détection et d'intervention englobent plusieurs aspects, notamment les outils permettant de surveiller le comportement, les personnes, l'accès aux données, leur utilisation et les technologies d'infrastructure (par exemple les réseaux et les points d'extrémité). Gartner conseille aux organisations de se poser les questions clés suivantes :

- Comment recueillons-nous et stockons-nous les données pour soutenir nos capacités de détection et d'intervention?
- La technologie dont nous disposons (ou que nous envisageons de nous procurer) prend-elle en charge une large gamme de fonctionnalités de détection et d'intervention, ainsi que la possibilité d'utiliser des indicateurs de compromission?
- Est-ce que nous vérifions si les fournisseurs qui prétendent utiliser l'intelligence artificielle ou l'apprentissage automatique (machine learning) disent vrai?

Une détection des menaces et une intervention efficaces sont essentielles pour réduire l'écart entre la vitesse de détection et la vitesse de compromission. Il devient toutefois de plus en plus ardu de le faire. En effet, selon une étude de l'ESG, 76 % des professionnels de la cybersécurité déclarent que la détection des menaces et la réponse à ces menaces sont plus difficiles aujourd'hui que ce ne l'était il y a deux ans, principalement en raison d'un labyrinthe d'outils ponctuels déconnectés.

4. Cloud Access Security Broker (CASB)

Un CASB est un point d'application de la politique de sécurité. Positionné entre les utilisateurs et les fournisseurs de services en nuage, le CASB offre une visibilité sur toutes les applications qu'il héberge. Il fonctionne essentiellement comme un contrôleur d'accès qui permet aux organisations d'étendre les stratégies de sécurité au-delà de leur propre infrastructure.

Gartner conseille aux entreprises de commencer par rechercher les applications dans le nuage afin de révéler les shadow IT, des projets informatiques gérés en dehors du département informatique – sans que celui-ci le sache. Puis, les entreprises devraient déterminer le niveau de contrôle nécessaire pour chaque application SaaS (logiciel en tant que service) et conclure des accords à court terme avec des fournisseurs de services en nuage qui promettent de sécuriser les données sensibles.

5. Système de gestion de la posture de sécurité en nuage (CSPM)

D'ici 2023, 99 % des défaillances de sécurité sur le nuage seront dues aux clients. Un système CSPM réduit considérablement les erreurs commises par les clients, les erreurs de gestion ou les erreurs de configuration, tout en réduisant le problème de « fatigue sécuritaire » avec lequel de nombreuses équipes TI doivent jongler.

Gartner conseille aux entreprises qui utilisent une seule plateforme d'infrastructure en tant que service (IaaS) de contacter leur fournisseur actuel pour voir s'il dispose d'offres CSPM. Dans le cas contraire, de nombreuses options CSPM en nuage sont disponibles sur le marché, y compris celles fournies par les CASBs.

6. Compromission de la messagerie en entreprise

Selon le rapport du FBI sur les crimes commis sur le Web, les pertes imputées aux compromissions de la messagerie d'entreprise ont atteint 1,3 milliard de dollars en 2018, soit plus du double de 2017. Pour éviter d'en être victime, Gartner conseille aux entreprises de :

- Corriger les défaillances des processus;
- Augmenter les contrôles techniques;
- Intégrer des systèmes intelligents et personnalisables de sécurité de messagerie;
- Déployer des protections des points d'extrémité;
- Fournir une formation de sensibilisation à la sécurité.

Cette dernière directive est particulièrement importante, étant donné que 70% des employés ne comprennent pas les bonnes pratiques en matière de confidentialité et de sécurité.

7. Gestion des données noires

Les données noires (ou les dark data en anglais) sont des informations que les organisations créent à l'interne et stockent de manière passive dans le cadre de leurs activités commerciales normales. Bien que ces informations aient peu de valeur pour l'organisation, elles peuvent poser un risque si elles sont utilisées et exploitées par des pirates informatiques ou d'autres acteurs malveillants. Gartner conseille aux entreprises de cibler les données noires hébergées dans plusieurs silos et de choisir des fournisseurs offrant un support étendu de répertoire de données pour les systèmes accumulant des données sensibles.

8. Rapport d'incident de sécurité

Dans le sondage 2018 sur les réponses aux incidents effectué par SANS, un tiers des participants ont admis qu'ils ne savaient pas combien d'incidents de sécurité n'avaient pas été traités et 15 % avaient déclaré ne pas savoir si certains incidents de sécurité avaient entraîné des violations de données.

Un processus robuste de rapport d'incidents de sécurité améliore la visibilité et les capacités d'intervention. Gartner conseille aux entreprises d'évaluer si leur plan d'intervention actuel pourrait être amélioré et d'explorer la possibilité de collaborer avec un fournisseur qui bâtira un service de réponse aux incidents qui répond à leurs besoins et à leur budget.

9. Solutions de conteneurisation

La sécurité des conteneurs a pour but de protéger le pipeline et l'application des conteneurs, ainsi que l'environnement et l'infrastructure dans lesquels ils se déploient. Gartner conseille aux entreprises de s'assurer que leur projet de sécurité des conteneurs s'intègre aux outils de développement communs et au pipeline CI/CD. Gartner propose aussi de tirer parti des interfaces de programmation applicative pour prendre en charge plusieurs outils de sécurité. Les entreprises doivent commencer par rechercher les vulnérabilités connues dans les pipelines, puis employer la même stratégie dans l'environnement de production.

10. Service d'évaluation de la sécurité

Les services d'évaluation de la sécurité (SRS) produisent une note en continu et en temps réel des évaluations internes, des achats, des partenariats et des activités de fusion et d'acquisition. Gartner avertit les organisations que les systèmes SRS peuvent seulement renforcer la visibilité en mettant de l'avant les services clés. Ils ne fournissent pas une vue à 360 degrés de l'ensemble de l'écosystème numérique.