L'invasion des bots sur Internet et autres tendances pour 2019
Internet
Posté par : JulieM
Publiée le : 4/12/2018 13:00:00

Il est essentiel d'avoir une longueur d'avance sur les cybercriminels lorsqu'il s'agit de protéger les données de l'entreprise et des clients. Dans cette optique, il est nécessaire de suivre attentivement les tendances de cybersécurité à court et long termes.

Que nous réserve 2019 ? Les bots plus intelligents, les clouds complexes, les risques liés à l'IoT et les réglementations sur les données seront les thèmes abordés dans tous les conseils d'administration. Voici un résumé des tendances qui, selon moi, perturberont l'année à venir aussi fortement que cette année passée :

1. Les cyberattaques augmenteront et se développeront lentement

Les entreprises verront une augmentation des cyberattaques « faibles et lentes », plutôt que des incidents brusques tels que des attaques DDoS. Lancées par des botnets, ces attaques « faibles et lentes » ont pour but de rester indétectables le plus longtemps possible, afin de voler un maximum de données.

Elles prennent souvent la forme d'attaques de « credential stuffing », dans lesquelles les informations d'identification volées sont utilisées pour accéder à des comptes associés et voler encore plus de données personnelles, telles que des adresses et des coordonnées bancaires.

Pour se protéger, les entreprises devront adopter des solutions de gestion des bots, pour identifier, catégoriser et répondre aux différents types de bots. Cette technologie est basée sur la détection de bots selon le comportement et une analyse continue des menaces pour différencier les personnes des bots.

2. Les bots devanceront le trafic Web humain

Plus de 50 % du trafic Web proviendra de ces bots de plus en plus sophistiqués. Akamai a déjà constaté que 43 % de toutes les tentatives de connexion proviennent de botnets malveillants.

Ce chiffre est amené à augmenter car les attaques de « credential stuffing » et les attaques « faibles et lentes » tendent à se développer. Ces bots plus sophistiqués seront capables d'imiter avec précision le comportement humain en ligne, rendant plus difficiles leur détection et le blocage de leurs activités par les solutions de sécurité.

Les outils de gestion efficaces des bots sont indispensables pour contrer cette menace. Ces outils sont capables d'utiliser des informations contextuelles, telles que les adresses IP et les données comportementales passées de l'utilisateur (interaction neuromusculaire), afin de déterminer si un visiteur est un bot ou un humain et appliquer des actions en conséquence.

3. Les stratégies multi-cloud compliqueront la gestion de la sécurité sur les plateformes

Les entreprises adoptant des stratégies multi-cloud devront faire face à des défis de plus en plus complexes pour garantir le déploiement continu et efficace de leur sécurité. Gartner prévoit que le multi-cloud sera la stratégie de Cloud la plus fréquemment utilisée l'année prochaine.

Les entreprises ayant réussi à mettre en place un Cloud sécurisé devront reproduire leur modèle à travers tout leur portefeuille de clouds, pour s'assurer que les vulnérabilités sont corrigées et que rien ne s'insinue à travers les failles.

De nombreuses entreprises ont déjà connu des failles ou des violations de leurs solutions provenant d'un seul et même fournisseur. Nous pensons que ces entreprises rechercheront des solutions de sécurité indépendantes du cloud pour simplifier le déploiement et la gestion à travers l'entreprise.

4. Les utilisateurs continueront à privilégier la commodité plutôt que la sécurité

Même si la prise de conscience de l'insécurité des terminaux IoT augmente, des millions d'utilisateurs continueront d'ignorer les risques, en achetant et utilisant des dispositifs sans solutions de sécurité complètes, des applications de fitness aux terminaux domestiques connectés.

Cela pourrait faire gonfler les armées de bots, déjà utilisées pour cibler les entreprises. On prévoit que d'ici 2020, plus de 25 % des attaques d'entreprises identifiées impliqueront l'Internet des objets (IoT), alors que l'IoT ne représente que 10 % des budgets de sécurité informatique.

Si certains gouvernements ont commencé à appliquer des normes de sécurité pour les terminaux connectés, il reste encore un long chemin à parcourir pour atteindre une sécurisation adaptée des terminaux.

5. Les marchés asiatiques suivront la voie de la cybersécurité

Avec le lancement du règlement RGPD en mai dernier, la directive PSD2 (directive sur les services

de paiement révisée) et une réforme plus large sur la sécurité, l'Union européenne a montré l'exemple en matière de réglementations sur la cybersécurité et continue sur sa lancée.

Certains pays asiatiques ont déjà commencé à suivre cette voie, en implémentant leurs propres règlements, et leur nombre tendra à augmenter en 2019.

Alors que des pays comme la Chine se placent en rivaux digitaux des pays occidentaux, les questions liées à la réglementation et à la protection des données font leur apparition dans les programmes gouvernementaux.

Certains pays asiatiques se sont longtemps opposés aux réglementations sur les données dans le passé, mais les violations de données de grande envergure les ont encouragés à adopter une approche plus proactive de la réglementation sur les données.

6. La cybersécurité sera remplacée par la cyber-résilience

En 2019, les entreprises intelligentes ne considéreront plus la cybersécurité comme une fonction distincte du service informatique, mais comme un modèle à adopter pour toute l'entreprise.

Ce concept de « cyber-résilience » regroupe la sécurité de l'information, la continuité de l'activité et la résilience dans le but de former des systèmes sécurisés de par leur conception, et non suite à une réflexion après coup.

Les entreprises peuvent ainsi se concentrer sur leurs capacités à exploiter leurs activités en continu, malgré les cyberattaques ou les incidents.

7. La sécurité Zero Trust supprimera les VPN d'entreprise

Pendant des années, les réseaux privés virtuels (VPN) ont été le pilier de l'accès authentifié à distance. Toutefois, avec le déplacement des applications vers le cloud, l'écosystème des menaces s'étend et les exigences d'accès se diversifient. L'approche de sécurité de type « tout ou rien » doit donc évoluer.

Le principe Zero Trust, dans lequel chaque application est mise en conteneur et nécessite une authentification séparée, se développe pour s'adapter à la sécurité du 21e siècle.

En 2019, les entreprises opteront de plus en plus pour une infrastructure sur le cloud afin de disposer d'un accès aux applications adaptatif et basé sur l'identité et d'une protection basée sur le cloud contre le hameçonnage, les logiciels malveillants et les ransomware, permettant d'améliorer l'expérience utilisateur et supprimant peu à peu les VPN.

8. La technologie des blockchains passera des crypto-devises aux paiements courants

Aujourd'hui, la plupart des utilisateurs associent les blockchains aux crypto-devises et aux paiements en ligne plus ou moins légitimes. Pourtant, en 2019, les réseaux de paiement basés sur les blockchains deviendront la norme, car ils permettent une évolution rapide des transactions monétaires de nouvelle génération.

La sécurité inhérente intégrée aux blockchains pourra simplifier le processus de paiement en ligne, réduire la friction, augmenter la vitesse et améliorer l'expérience utilisateur. Au cours de l'année à venir, de plus en plus de plateformes de paiement basées sur les blockchains et bénéficiant d'une haute évolutivité et d'une grande vitesse seront adoptées par de grandes banques et sociétés financières.