

LE FACTEUR CONFIANCE

La cybersécurité, un rôle-clé dans la préservation du dynamisme commercial des entreprises

Résumé

Face aux cyber-attaques en 2018, les enjeux ont été plus importants que jamais : tandis que les incidents de données continuaient de faire les gros titres, notamment l'attaque par déni de service distribué la plus importante jamais enregistrée (avec un débit de 1,7 Tbit/s¹), l'Union européenne a lancé son Règlement général sur la protection des données (RGPD) le 25 mai 2018, imposant de nouvelles règles strictes sur la collecte, le traitement et le contrôle de informations permettant d'identifier des personnes. Cette année aura aussi vu des cryptominers s'infiltrer dans les réseaux, en quête de prises faciles.

Nous sommes aujourd'hui entrés dans l'ère de la « post-vérité », une ère dans laquelle les entreprises comme les individus se montrent de plus en plus méfiants face aux promesses de sécurité. Aujourd'hui, tout consommateur fait systématiquement un choix lorsqu'il interagit avec une marque : celui de faire suffisamment confiance à l'entreprise derrière cette marque pour lui confier ses données personnelles... ou non. Toute cyber-attaque qui parvient à tromper les défenses d'une entreprise détruit la confiance que celle-ci a parfois consacré beaucoup de temps et d'efforts à établir avec ses clients. Dans ce contexte, les attaques et leurs ramifications ne sont plus du seul ressort des professionnels de la sécurité aujourd'hui : les cadres dirigeants doivent aussi en assumer la responsabilité.

Radware produit chaque année un rapport sur la sécurité des applications et des réseaux à l'échelon mondial afin de les renseigner sur la complexité de tous ces défis. Dans sa huitième édition, ce rapport comprend les résultats des recherches réalisées par Radware, les données d'attaques réelles, les analyses sur les tendances et technologies émergentes, ainsi que les résultats d'un sondage global réalisé auprès des entreprises.

Il discerne les impacts commerciaux et technologiques de la cybersécurité, notamment les suivants :

- ▶ Enseignements des attaques les plus récentes ;
- ▶ Coûts véritables, quantitatifs et qualitatifs, des cyber-attaques ;
- ▶ Vue d'ensemble du paysage des menaces applicatives et réseau ;
- ▶ Analyse des vulnérabilités des technologies émergentes ;
- ▶ Prédications pour 2019.

INFORMATIONS CLÉS

Calcul du rapport coûts / risques

Pour se protéger face aux cyber-attaques, les entreprises doivent engager des investissements significatifs, qui s'ajoutent à leurs dépenses d'exploitation. Par nature, elles sont aussi toujours en quête de sources d'économies. Dans ce contexte, comment peuvent-elles faire le bon calcul face au risque de voir des cyber-attaques pénétrer leurs défenses et impacter leurs activités ?

Un risque mis en évidence par l'enquête globale réalisée par Radware en 2018-2019 :

- ▶ En tout juste un an, les coûts initiaux attribuables à des cyber-attaques ont augmenté de 52 %, pour atteindre 1,1 million de dollars
- ▶ Les entreprises qui ont modélisé les coûts globaux des cyber-attaques sur leurs activités ont estimé que leur montant était proche du double par rapport à celles qui ne l'avaient pas fait
- ▶ Deux entreprises sur cinq ont fait part d'expériences clients négatives et d'un impact négatif sur leur réputation suite à des attaques réussies
- ▶ 93 % des personnes sondées ont indiqué avoir subi une cyber-attaque au cours des douze derniers mois ; seules 7 % d'entre elles n'avaient aucune attaque à signaler
- ▶ Les cyber-attaques se produisent sur un rythme hebdomadaire pour un tiers des entreprises
- ▶ Le plus souvent, les cyber-attaques provoquent une interruption de service : une conséquence signalée par la moitié des personnes interrogées. Les attaques qui ont conduit à une interruption de service partielle ou complète ont augmenté de 15 %, affectant la productivité des entreprises touchées
- ▶ La cyber-rançon continue d'être la principale motivation derrière les attaques (51 % d'entre elles)

Vecteurs d'attaque émergents

Les pirates informatiques font appel à des techniques performantes pour provoquer des dénis de service (attaques par rafale, d'amplification, attaques cryptées ou botnets IoT) et ciblent la couche applicative pour provoquer davantage de dégâts.

- ▶ Les attaques contre la couche applicative sont celles qui causent le plus de dégâts. Les deux tiers des personnes interrogées ont indiqué avoir subi des attaques applicatives. Un tiers d'entre elles voit dans les failles applicatives l'une de leurs principales préoccupations en 2019, en particulier dans les environnements Cloud. Plus de la moitié des personnes interrogées apportent des modifications et mises à jour à leurs applications à une fréquence mensuelle. Les autres personnes apportent des mises à jour encore plus fréquemment, ce qui accroît d'autant le besoin d'automatisation de la sécurité.
- ▶ Les cyber-attaques ayant mené à une interruption complète de service ont augmenté de 15 %; une entreprise sur six a indiqué avoir subi une attaque à 1 Tbit/s.
- ▶ En 2018, les hackers ont développé de nouvelles tactiques pour venir à bout des réseaux et centres de données : les inondations HTTPS ont cru de 20 %, les attaques DNS et par rafale de 15 % et les attaques par bot de 10 %.
- ▶ Un tiers des représentants d'entreprise interrogés ont indiqué avoir subi des attaques dont ils n'ont pas été en mesure d'identifier la motivation.

Se préparer pour les futures menaces

Si les représentants d'entreprises estiment comprendre l'évolution du paysage de menace et prennent des mesures afin de protéger leurs ressources numériques en conséquence, ils ne s'en sentent pas moins accablés par l'ampleur de la menace.

- ▶ Près de la moitié d'entre eux se sentent mal préparés pour se défendre contre tous les types de cyber-attaques, malgré les solutions de sécurité déployées.
- ▶ 86 % des entreprises ont testé des solutions d'apprentissage automatique et d'intelligence artificielle (IA) au cours des douze derniers mois, principalement motivées par la recherche de meilleurs délais de réponse face aux cyber-attaques (pour près de la moitié des personnes interrogées). La part des entreprises utilisant la blockchain dans leur activité a augmenté de 44 %.
- ▶ Les entreprises dans l'ensemble continuent de répartir leurs opérations réseau entre plusieurs fournisseurs de services Cloud : deux entreprises sur cinq utilisent des solutions hybrides combinant protections sur site et basées dans le Cloud.
- ▶ 49 % des entreprises basées dans la région EMEA ont indiqué ne pas se sentir bien préparées pour la mise en conformité avec le RGPD.

La réussite, seule option possible

Le coût potentiel des cyber-attaques est trop important pour qu'une entreprise puisse se permettre de ne pas parvenir à contrer chacune des menaces la ciblant, à tout moment. Si elle y échoue, elle court le risque de voir la confiance des clients disparaître en quelques instants, avec à la clé un impact sur sa réputation et de nouveaux frais à engager pour regagner des clients. Le RGPD et les autres réglementations mises en place par les états ont le potentiel d'obliger les entreprises qui ne s'y conforment pas à mettre la clé sous la porte.

Il est donc essentiel pour toute entreprise d'intégrer la cybersécurité dans ses plans de croissance à long terme, et de ne plus déléguer la sécurité des ressources numériques au seul département informatique. La planification de la sécurité doit être infusée dans toutes ses offres de produits et services, ainsi que dans l'ensemble de ses plans de développement et de sécurité et ses nouvelles initiatives commerciales. Le CEO et l'équipe de direction doivent montrer la voie et s'impliquer dans la sécurisation de l'expérience des clients.



C-Suite Perspective

Les CEO, nouveaux garants de confiance de l'entreprise

Peu à peu, la cybersécurité s'impose comme un sujet hautement personnel dans l'agenda des dirigeants de l'entreprise : pour construire et entretenir des relations solides avec les clients, les CEO doivent en effet investir un nouveau rôle, celui de garants de confiance de l'entreprise. À une époque dans laquelle la stratégie de marque la plus soignée court le risque d'être annihilée par une seule cyber-attaque, il n'est plus envisageable de laisser la stratégie de sécurité entre les seules mains du responsable de la sécurité de l'information (CISO). Les enjeux sont bien trop importants.

Pensez à ce que sont devenus les CEO de ces entreprises qui ont subi des violations de données très médiatisées ces dernières années : Equifax, Yahoo, Moller-Maersk, Anthem Healthcare. Suite aux attaques, les clients ont perdu confiance et tout le travail que ces entreprises avaient consacré à valoriser leurs marques depuis des années s'est comme évaporé. Peu de temps après, on a vu les CEO quitter le navire, officiellement « pour poursuivre de nouveaux projets ».

Pour veiller à ce que la cybersécurité soit intégralement inscrite dans les modèles commerciaux de leur entreprise, les CEO doivent superviser les efforts et piloter le financement de mesures de protection. Tout CEO qui choisit de déléguer la stratégie de sécurité sans supervision le fait à son propre péril.



Télécharger le rapport gratuit

Rapport 2018-2019 sur la sécurité des applications et des réseaux à l'échelon mondial

Ce document est fourni à titre d'information uniquement. Il peut contenir des erreurs, ne fait l'objet d'aucune garantie et n'est soumis à aucune condition, qu'elle soit exprimée oralement ou implicite sur le plan légal. Radware rejette expressément toute responsabilité en lien avec ce document, ainsi que toute obligation contractuelle qui en découlerait, directement ou indirectement. Les technologies, fonctionnalités, services ou processus décrits dans le présent document sont susceptibles d'être modifiés sans préavis.

© 2019 Radware, Ltd. Tous droits réservés. Les produits et solutions Radware mentionnés dans ce document sont protégés par des marques commerciales, des brevets ou des demandes de brevet en cours de Radware aux États-Unis et dans d'autres pays. Pour plus d'informations, consultez : <https://www.radware.com/LegalNotice/>. Toutes les autres marques commerciales et noms sont la propriété de leurs détenteurs respectifs.