Cybersécurité 2021 : à quoi doivent s'attendre les entreprises ?

Forrester Research a livré ses prévisions de cybersécurité pour 2021 à l'attention des professionnels de la sécurité IT et de la gestion des risques.

Les répercussions de la pandémie de Covid-19, la massification du travail à distance et la dispersion des effectifs marquent cette édition.

À quoi doivent s'attendre les entreprises ? Les analystes proposent les 5 clés suivantes :

Menaces internes et clients finaux

1. RSSI sous pression >

2021 pourrait être une année difficile pour des responsables de la sécurité des systèmes d'information (RSSI) sous pression, au risque « d'alimenter ou de tolèrer » une culture d'entreprise « toxique » pour les équipes dont ils ont la charge. Ces responsables pourraient être remerciés, y compris au sein d'entreprises classées au Global 500.

2. Menaces internes >

Outre le risque externe, élevé, le partage de données par des initiés aux intentions malveillantes ou d'employés « négligents » est un risque à ne pas sous-estimer.

Aussi, Forrester prévoit que 33% des violations de données auront pour origine des initiés en 2021, contre 25% cette année.

3. « Direct-to-consumer »>

Les secteurs du commerce de détail (retail) et de la production (manufacturing) devraient être davantage touchés que d'autres par ces violations. Une tendance qui s'explique, selon Forrester, par la diffusion du modèle de relation directe entre une marque et ses clients finaux (« direct-to-consumer » ou D2C), plutôt que par le biais d'intermédiaires.

« Si votre entreprise passe au D2C, donnez la priorité à la sécurité des produits/applications, créez un programme développeurs et explorez le potentiel des outils de simulation d'attaques et de brèches de sécurité », recommande la firme.

Financer la cybersécurité

4. Justifier les dépenses >

« En 2021, la stagnation ou la baisse des budgets impliqueront une solide justification des dépenses », avec des outils de quantification des risques, prévoit l'entité.

Ces solutions fournissent un aperçu de la criticité des actifs et de l'impact potentiel d'un problème en temps réel. Ils peuvent aider les professionnels concernés à se prononcer sur l'acceptabilité des risques, au-delà de l'analyse de rentabilisation de base.

5. Capital-risque >

Forrester s'attend à ce que le financement en capital-risque d'entreprises de cybersécurité basées hors des États-Unis augmente de 20% en 2021, par rapport à son niveau de 2019 (4,3 milliards $ sur les 11,3 milliards $ levés dans le monde cette année là).

(crédit photo : by Kevin Ku from Pexels)