Les 10 erreurs de cybersécurité des startups technologiques

Non, accomplir quelques actions de cybersécurité juste avant les phases de lancement ou d’évolution des produits technologiques ne suffit pas. Non, utiliser un service d’hébergement cloud dit sécurisé ne veut pas dire que le produit technologique soit automatiquement quasiment sécurisé. Cap sur les 10 erreurs de cybersécurité les plus communes des startups technologiques !

Republication d’un article du 31 août 2020

Est-ce que vous vous reconnaissez, vous ou l’un de vos proches, dans l’un ou dans plusieurs des profils suivants ?

> Ceux qui sont convaincus qu’il est nécessaire de faire de la cybersécurité mais juste avant les phases de lancement ou d’évolutions des produits technologiques
>
> Ceux qui cantonnent la cybersécurité à des sujets spécifiques
>
> Ceux qui croient, dur comme fer, que leurs produits technologiques sont automatiquement quasiment protégés car ils utilisent des services

d’hébergement Cloud dit sécurisés et/ou qu’ils utilisent un ou deux produits de cybersécurité.

Ceux qui la considèrent comme un non-sujet et uniquement applicable s’ils reçoivent une demande explicite d’un client, d’un investisseur, d’un partenaire ou d’un régulateur.

Alors, oui ? Avec plus ou moins de nuances ? Allez, embarquez avec nous dans la revue dans 10 erreurs de cybersécurité des startups technologiques. Faire de la cybersécurité, oui, mais juste avant les phases de lancement ou d’évolutions des produits technologiques

Erreur 1 : “On fera de la cybersécurité juste avant les mises en production. Cela ne sert à rien avant ce jalon car les chantiers techniques sont en cours.”

Que nenni. La cybersécurité ne se résume pas à faire des tests d’intrusion avant les mises en production d’un produit technologique. Puis à réaliser les actions de remédiation relatives aux failles trouvées.

La cybersécurité, c’est de la gouvernance, de la gestion de risques, de l’humain et de la technologie qui s’articulent tout au long du cycle de vie de votre startup et de ses produits technologiques. Tout en s’adaptant à sa taille et à son stade d’avancement. Faire de la cybersécurité presque uniquement avant les phases de mise en production c’est risquer de lancer des produits technologiques gardant une surface d’attaque importante. Car les résultats des tests d’intrusion sont contraints par les limitations de temps, de périmètre, d’accès, de méthodes et de compétences des “pentesters”.

Alors qu’une gestion au fil de l’eau de la cybersécurité permet une plus grande maîtrise du niveau de cybersécurité de votre startup. Et les coûts en termes de temps et d’argent peuvent être, contrairement à ce qu’on pense, très raisonnables surtout si on planche sur la cybersécurité dès la phase de conception.

Erreur 2 : Spécifiquement pour les

“early-stages” : C’est un non-sens de faire de la cybersécurité pour nous, on ne se sait pas encore si le produit va intéresser les clients.

La cybersécurité n’est pas une cerise sur le gâteau. Les clients font preuve de confiance lorsqu’ils utilisent votre produit technologique même si c’est un MVP (Minimum Viable Product – Produit minimum viable). Ils s’attendent, entre autres, à ce que leurs données soient protégées. Faire de la cybersécurité dès la phase de conception, c’est, entre autres, faire preuve de considération aux attentes de vos clients actuels ou que la meilleure façon de se mettre en conformité avec les réglementations en vigueur.

Ce qui nous importe en termes de cybersécurité, c’est ce sujet spécifique :

Erreur 3 : On est juste intéressé par la gestion des accès

Clairement, la question de la gestion des accès est importante. Mais lorsqu’on creuse le sujet, on se rend compte que c’est perçu comme “le” moyen d’éviter la fuite de données notamment par des employés ou ex-employés mécontents. Ceci est un exemple de la vision parfois parcellaire de la cybersécurité. En effet, par exemple, une application web mal protégée peut résulter également en une fuite de données vers des mains malveillantes. Donc il est nécessaire de se donner les moyens d’avoir une vision holistique de la cybersécurité afin de réduire efficacement la surface d’attaques de sa startup.

À lire aussi

Comment identifier vos besoins en cybersécurité ?

Erreur 4 : On est juste intéressé par

l’application au RGPD (Règlement Général sur la Protection des Données)

Et c’est super. En effet, c’est primordial de se conformer au RGPD mais cela ne fait pas tout en termes de cybersécurité. Car le RGPD concerne la gestion des risques relatifs au droit fondamental d’une personne physique sur ses données personnelles. Alors que des normes comme l’ISO 27001, entre autres, vont bien au-delà des données personnelles, comme par exemple les données qui relèvent de la propriété intellectuelle et les données de production confiées par des tiers comme vos clients. Par ailleurs, le RGPD ainsi que des normes comme l’ISO 27001 répondent au principe des vases communicants. Ainsi, appliquer le RGPD permet de renforcer son niveau de cybersécurité mais n’est pas suffisant pour couvrir tous les points d’attention importants à adresser. Et notons que des normes comme l’ISO 27001 sont suffisamment agiles pour s’adapter au contexte des startups.

Mais si, on est sécurisé ! On utilise tel service d’hébergement Cloud dit sécurisé et/ou tel produit de sécurité. Ou encore, on n’a pas mis de clauses cybersécurité dans les contrats avec nos sous-traitants mais on a confiance en eux.

Erreur 5 : On est sécurisé parce que notre hébergeur Cloud est dit sécurisé ou/et qu’on utilise un ou deux produits de cybersécurité.

Il existe un certain nombre de services d’hébergement Cloud qui font sérieusement de la cybersécurité. Mais utiliser un tel service d’hébergement Cloud ne veut pas dire que le produit soit automatiquement sécurisé. C’est un bon début mais cela ne suffit pas. Imaginez que l’interface d’administration de votre produit soit accessible via des mots de passe faibles. Ou que des hackers manipulent vos collaborateurs, via des e-mails, dans le but d’accéder à votre interface d’administration ? Et je pourrai encore lister maintes autres exemples.

Erreur 6 : On n’a pas mis de clauses de

cybersécurité dans les contrats avec nos sous-traitants mais on a confiance en eux

La confiance n'exclut pas le contrôle. Et oui, vous avez tout à fait le droit et même le devoir d'inclure des clauses de cybersécurité dans les contrats avec vos sous-traitants. Il y va de la cybersécurité de votre startup ainsi que de la cybersécurité de vos clients. En effet, les hackers peuvent utiliser vos failles de cybersécurité pour rebondir et pirater les systèmes d'information de vos clients. Avec les conséquences très fâcheuses que cela pourrait avoir pour toute la chaîne de responsabilité. Par ailleurs, l'article 28 du RGPD impose que la sous-traitance d'un traitement de données personnelles soit encadrée formellement via un contrat ou via un autre acte juridique contraignant. Et bien sûr, il est nécessaire d'adapter les clauses de cybersécurité selon le type des sous-traitants.

La cybersécurité ? Ce n'est pas pour nous. Mais bon, on le fera si on reçoit une demande explicite de l'une de ces parties prenantes : clients, investisseurs, partenaires et régulateurs.

Erreur 7 : On est trop petit pour les hackers, ce n'est pas un sujet pour nous

Selon le rapport Hiscox 2019, 47% des entreprises de moins de 50 collaborateurs ont été touchées par un cyber-incident. En effet, entre autres, les hackers les considèrent comme des "proies" plus faciles que les grandes entreprises. D'autant plus que, comme spécifié précédemment, les hackers peuvent les "utiliser" pour rebondir et pirater plus "facilement" les systèmes d'information de leurs clients.

À lire aussi

Cybersécurité : quel hacké·e êtes-vous ?

Erreur 8 : On fera de la cybersécurité si on reçoit une demande explicite de l'une de ces parties prenantes : clients, investisseurs, partenaires et régulateurs

Tôt ou tard, et c'est de plus en plus tôt, vous aurez des clients, des partenaires, des investisseurs ou des régulateurs qui vous demanderont où vous en êtes d'un point de vue cybersécurité. Vous ne pouvez pas vous permettre de leur dire : "Veuillez nous laisser un message avec vos doléances et nous reviendrons vers vous, au mieux, dans quelques semaines une fois qu'on aura fait de la cybersécurité". Par ailleurs, faire de la cybersécurité, dès la phase de la conception, vous aidera, entre autres, à détecter rapidement les failles. Ce qui vous fera économiser beaucoup de temps, d'argent par rapport aux coûts de remédiation relatifs à la détection de failles juste avant la phase de lancement.

Erreur 9 : Nous avons des clients et personne nous a demandé notre niveau de cybersécurité. Donc pourquoi en faire ?

Ici, j'insiste encore une fois sur la notion de confiance. Même si ce n'est pas explicitement exprimé par les clients, ils s'attendent à ce que vous ne mettiez pas leurs données à la merci des hackers. Sans parler des impacts en termes financiers, image, juridique qu'une cyberattaque pourrait avoir sur votre startup.

Erreur 10 : Nous sommes en phase de levée de fonds et les investisseurs ne nous ont pas posé des questions sur notre cybersécurité. Donc pourquoi en faire ?

Et si la cybersécurité vous permettait d'avoir une meilleure valorisation de votre startup ? La valorisation d'une startup est décidée au terme de

négociations avec des investisseurs potentiels et les perspectives en termes de marché pour les startups sérieuses en termes de cybersécurité sont plus crédibles et variées. Par ailleurs, le “Centre pour la cybersécurité” du “World Economic Forum” a élaboré des principes et un cadre d’évaluation de la due diligence en matière de cybersécurité pour la communauté des investisseurs. Ce qui, entre plus de l’appétence grandissante de l’AMF (L’Autorité des marchés financiers (AMF) pour la cybersécurité, va conduire de plus en plus d’investisseurs à mettre le sujet de la cybersécurité sur la table des négociations lors de la valorisation des startups.

En résumé, la cybersécurité vous concerne et vous veut du bien. Alors, allez-y, sécurisez vos startups et le plutôt le mieux.

Aroua Birir est ingénieure, docteure et entrepreneure dans la cybersécurité

Article écrit par AROUA BIRI