La vision des spécialistes

'La cyber-sécurité exige une approche à l'échelle mondiale'

L'utilisation de sites web et applis sur nos ordinateurs, tablettes et smartphones implique le stockage de gros volumes de données personnelles. La sécurité et le respect de la vie privée constituent dès lors des défis sans cesse majeurs dans notre société numérique. 'L'internet n'a pas de frontière', explique Chris Verdonck, partenaire et cyber leader chez Deloitte Belgique. 'En tant qu'utilisateur de services en ligne ou d'outils mobiles, vos données sont stockées – en général de manière non voulue – sur une plate-forme mondiale. Vous êtes donc beaucoup plus vulnérable que par le passé, lorsque votre carte client était conservée dans une boîte sur le comptoir.'

La proximité numérique générée par l'internet ouvre cependant un éventail d'opportunités pour les organisations qui souhaitent développer leurs activités à une échelle globale. Les distances sont devenues relatives: le monde est aujourd'hui à portée de main pour les entreprises. Plus la 'digital proximity' est grande, plus la valeur d'une entreprise opérant à l'échelle internationale est élevée. Mais dans le même temps, cette évolution implique toute une série d'obligations, à savoir de gérer correctement les données collectées.

Quête d'une meilleure sécurité

La vitesse à laquelle la numérisation conquiert le monde implique des défis supplémentaires. En à peine dix ans, les smartphones et réseaux sociaux ont acquis une place importante dans notre vie. Utilisateurs, entreprises et administrations sont à présent confrontés aux problématiques de sécurité et de respect de la vie privée, sans pouvoir s'appuyer sur un vaste historique ou une expertise afin de pouvoir maîtriser cette évolution ultra-rapide. La quête d'une plus grande sécurité se fait donc par tâtonnements. Le fait que les pouvoirs publics n'aient posé que très récemment des questions concrètes sur la politique de respect de la vie privée de Facebook est exemplaire à cet égard.

Chris Verdonck, partenaire et cyber leader chez Deloitte Belgique.

'L'internet n'a pas de frontières. Pas davantage pour les acteurs malveillants.'

De même, l'accessibilité croissante de l'internet rend les utilisateurs plus vulnérables encore. 'Naguère encore, il était uniquement possible de surfer vers des sites web avec un ordinateur', rappelle Verdonck. 'Pour ce faire, il fallait au préalable se connecter via une ligne téléphonique. Après quoi il fallait littéralement 'débrancher' l'internet. Aujourd'hui, même nos enfants sont reliés en permanence au world wide web via toutes sortes d'appareils – qu'il s'agisse d'un smartphone, d'une Xbox, de la télévision par internet ou de wearables. Les dangers de cette 'connectivité' permanente ne doivent pas être sous-estimés.'

Nécessité d'un cadre légal

Un cadre légal en matière de protection des données des utilisateurs s'impose donc. En l'occurrence, les pouvoirs publics se doivent de mettre en place une politique à l'échelle tant régionale qu'internationale. Chris Verdonck: 'Des mesures concrètes doivent être prises à grande échelle. Car la 'digital proximity' sous-entend également que des acteurs malveillants sont présents partout. Une cyber-attaque est un phénomène totalement virtuel: une personne à un endroit A peut, via un serveur à un endroit B, attaquer une entreprise à un endroit C. On peut la comparer au virus Ebola: une telle menace ne se combat que grâce à une approche internationale structurée.'

VOICI COMMENT PROTEGER VOTRE ORGANISATION

Les organisations considèrent les cyber-risques souvent sous un angle strictement technique. Pourtant, il s'agit bien davantage d'un problème business. Deloitte Belgium a mis au point une méthodologie destinée à protéger le métier des cyber-dangers, méthodologie appliquée désormais dans le monde entier. Celle-ci recommande d'identifier d'abord les menaces pertinentes pour l'organisation et de déterminer les départements vulnérables à quel(s) type(s) de cyber-menace(s). Après quoi il conviendra de vérifier dans quelle mesure l'organisation est déjà parée contre ces cyber-risques. Ensuite, il faudra déterminer quelles mesures doivent être prises à quel endroit, et les budgets nécessaires à cet égard. Les tableaux de bord obtenus offrent aux dirigeants et au comité de direction une vue précise de la situation actuelle et permettent d'établir une feuille de route des priorités.

'Les risques et acteurs peuvent d'ailleurs différer selon les différentes industries et même entre les services business au sein d'une même entreprise', précise Chris Verdonck. 'Prenez une banque: l'un des risques potentiels avec l'internet banking est le phishing, alors que les risques lors d'un retrait d'argent à un distributeur automatique de billets sont le shoulder surfing et le skimming. Toute la question est donc à nouveau de cartographier les vulnérabilités de chaque élément de votre organisation et ensuite de définir une cyber-stratégie adaptée.'

Vous souhaitez davantage d'informations sur la campagne Tomorrow is Today?
*Visitez **www.tomorrowistoday.be**.*
La semaine prochaine, nous nous intéresserons au Digital Smart Banking.

Deloitte.