Dirigeants, reprenez la main sur la cybersécurité

La sécurité informatique n'est pas la chasse gardée de la DSI ou du RSSI. Pour protéger efficacement l'entreprise, la direction doit embrasser ce sujet en prenant des décisions éclairées et adaptées.

La plupart des entreprises disposent aujourd'hui de responsables informatique ou cybersécurité chargés de protéger l'organisation contre les attaques et les fuites de données. Mais c'est à la direction de prendre les décisions nécessaires pour réduire le risque numérique, car c'est bien l'entreprise qui sera mise en cause en cas de défaillance.

Avec des textes comme le RGPD, les données personnelles sont de mieux en mieux protégées. Toutefois, ce cadre réglementaire fait peser un risque sur les entreprises qui se seraient montrées négligentes en matière de protection des données personnelles de leurs clients. Les sanctions peuvent aller jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros. Ajoutez à ceci les sanctions pénales ; jusqu'à 5 ans d'emprisonnement. Ceci sans compter l'impact sur l'image de marque de l'entreprise, qui peut leur être fatal.

Bref, les professionnels doivent passer à la vitesse supérieure dans le secteur de la sécurité informatique… sous l'impulsion et avec le support actif de leur direction.

Définir des règles strictes

La sécurité peut être contraignante et ne sera donc pas acceptée naturellement par tous.
Attacher sa ceinture est devenu aujourd'hui un réflexe pour les automobilistes et leurs passagers. Mais ce changement dans les mentalités ne s'est pas fait en un jour. L'obligation du port de la ceinture de sécurité a été progressive, tout comme l'augmentation des sanctions appliquées aux récalcitrants.

Pour que l'application de règles de sécurité informatique devienne un réflexe pour tous, elles doivent venir de la direction générale. Afin de vaincre la résistance au changement, ces règles doivent être compréhensibles, appuyées d'explications, voire de formations, et imposées au travers de contrôles et de l'application d'éventuelles sanctions en cas de négligence grave d'un collaborateur.

Ces exigences doivent aussi s'appliquer aux sociétés tierces. Le non-respect des standards de sécurité de l'entreprise doit faire partie des critères d'exclusion des prestataires, fournisseurs et sous-traitants. En particulier si ces derniers ont accès à des données stratégiques.

Prendre en compte les risques

Le time-to-market est essentiel pour les entreprises. Mais à quoi bon faire vite, si l'on ne fait pas bien ? Un produit qui est disponible avant celui d'un concurrent connaîtra-t-il le succès s'il est retiré

du marché 3 mois après sa sortie du fait de risques mal pris en compte ?

Il est indispensable de mettre la sécurité au cœur de chaque nouveau processus ou produit, en particulier lors de la phase de conception, sous peine de devoir reprendre cette dernière à zéro. Mais aussi dans les phases de production et d'exploitation. Bref, tout au long du cycle de vie du processus ou du produit.

À cet effet, les experts en informatique et cybersécurité doivent plus que jamais savoir parler le langage des métiers, afin de les sensibiliser à la problématique de la sécurité informatique et de les aider à identifier les points de vigilance.

Connaître les risques c'est aussi savoir les accepter. Lorsque l'entreprise doit répondre à une problématique dans l'urgence, elle peut décider d'accepter le risque, en particulier si son impact financier éventuel reste limité au vu des avantages attendus. Mais elle doit le faire en connaissance de cause : le risque est soit traité, soit délégué, soit assumé, mais jamais ignoré. Bien évidemment, seule la direction est en mesure de prendre la décision d'accepter un risque.

Rester en éveil

Le nombre de cyberattaques croit de façon démesurée depuis le début de l'année 2021. Ceux qui passent entre les gouttes pourraient souffrir du syndrome du survivant et se croire ainsi à l'abri de toute menace. Les entreprises bien protégées ne doivent pas baisser la garde (et baisser leur budget sécurité par la même occasion) sous peine de se faire rattraper par les cybercriminels.

Le DSI ou le RSSI se doivent de rester vigilants. En informant tout d'abord la DG sur les attaques bloquées aux portes de l'organisation. Mais aussi sur ce qui se passe chez la concurrence ou dans d'autres industries. Cela permettra de maintenir l'attention et de justifier des opérations préventives. Informée et alertée régulièrement sur les risques existants, la direction pourra prendre des décisions éclairées visant à améliorer les défenses de l'entreprise.