Cinq questions importantes à se poser en matière de cybersécurité

	Cinq questions importantes à se poser en matière de cybersécurité

Pas un jour ou presque ne se passe sans que le sujet de la cybersécurité ne soit traité dans les médias. Entre les « cyberattaques », les « cybermenaces » et la nécessité de « connaître son adversaire », on pourrait croire que les entreprises sont en état de siège permanent.

Les cybermenaces revêtent plusieurs formes : États-nations qui se livrent à des activités d'espionnage, cybercriminels qui cherchent à dérober de précieuses informations en vue de les exploiter, ou encore groupes aux motivations diverses qui cherchent à perpétrer des vols ou à causer des perturbations.

Il peut même s'agir d'une personne interne de confiance qui vole des données de clients ou d'entreprise ou d'un employé bien intentionné qui, en effectuant son travail, perd sans le vouloir de précieuses données de clients ou d'entreprise. Nul doute que les cybercriminels peuvent être très adaptables et innovants, mais le contexte de menace est un fait établi. C'est la manière dont vous gérez le risque qui est importante.
Dans un environnement cacophonique, il est important que les dirigeants d'entreprise gardent les choses en perspective. L'environnement est inondé de toutes sortes de solutions techniques, promettant de vous donner un avantage en matière de détection et de prévention. Toutefois, il est essentiel que tous les dirigeants d'entreprise prennent du recul et se rappellent que le cyber risque n'est pas un risque informatique, mais un risque d'entreprise et, à l'instar de tout autre risque d'entreprise, il doit être géré.

La menace ne peut pas être éliminée, mais le risque peut être géré

Il est également important de comprendre que cette menace ne peut pas être éliminée, mais que le risque peut être géré. Il est facile de se laisser tenter par une « structure du risque », mais comme de nombreuses structures, elle peut nécessiter d'investir beaucoup de temps et d'efforts pour des résultats de sécurité négligeables.
Trop souvent, la cybersécurité est évoquée à l'aide de jargon technique ou militaire, mais cela ne fait que dissiper l'attention et la compréhension des dirigeants. Il est vital que les professionnels de la sécurité expliquent le contexte de menace et le défi de la cybersécurité dans un langage accessible. C'est pourquoi il est important de comprendre le cyber risque auquel votre entreprise est confrontée. Tous les dirigeants doivent pouvoir poser les questions simples et non techniques suivantes et obtenir des réponses.
1. **Connaissez la valeur de vos données :** savez-vous de quelles données de valeur dispose votre entreprise ? Sont à inclure les données qui ont de la valeur non seulement pour vous, mais aussi pour les cybercriminels qui peuvent vouloir les voler. Quelles sont les données qui vous causeraient le plus grand préjudice si vous deviez les perdre ? Vous devez avoir une liste de vos données de valeur.
2. **Sachez qui a accès à ces données de valeur :** qui possède les droits d'administration ou l'accès aux informations ? Toutes vos « personnes internes de confiance » ont-elles besoin d'avoir accès aux données de valeur pour effectuer leur travail ? Cette question est essentielle, car l'accès aux données de valeur doit être étroitement surveillé. Vous ne confieriez pas les clés de votre domicile à n'importe qui, alors surveillez de près les personnes qui ont accès à vos données de valeur.
3. **Sachez où se trouvent vos données de valeur :** vous devez savoir où elles sont stockées et comment vous y accédez. Vos données de valeur sont-elles délocalisées au loin, dans le pays, dans le cloud ou même stockées chez un tiers ? Allez plus loin et demandez-vous si vos fournisseurs ont partagé vos données de valeur avec des sous-traitants.
4. **Sachez qui protège vos données :** vous devez savoir qui protège vos données de valeur. Cet aspect est extrêmement important. Où se trouvent ces personnes ?
5. **Sachez dans quelle mesure vos données sont protégées :** vous devez savoir ce qui est fait par les professionnels de la sécurité pour protéger vos données 24 h/24 et 7 j/7. Les tiers qui ont accès à vos données les protègent-ils de manière adéquate ?
C'est seulement une fois que vous aurez la réponse à ces questions que votre entreprise sera préparée à comprendre le niveau de cyber risque et l'efficacité avec laquelle il est géré… [Lire la suite]

Réagissez à cet article

Source : *Cinq questions importantes à se poser en matière de cybersécurité – ZDNet*