Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

	Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

Un responsable informatique sur trois et un salarié sur cinq tiendrait pour responsable son dirigeant en cas de fuite importante de données dans lentreprise.

Tel est le constat dressé par VMware qui vient de publier les résultats d'une enquête menée par le cabinet d'études de marché Vanson Bourne. Celle-ci pertmet aussi d'établir que plus d'un tiers des entreprises s'attendent à subir une cyberattaque importante dans les trois prochains mois, qu'un quart des responsables informatiques français n'informent pas ses dirigeants en cas de cyberattaque et que seulement 11 % des dirigeants français considèrent la cybersécurité comme une priorité au détriment d'initiatives visant à revoir la sécurité de leur système d'information.
Près d'un tiers (29 %) des responsables informatiques et près d'un cinquième (21 %) des employés en France considèrent donc que leur dirigeant devrait être tenu responsable en cas d'importante fuite de données. Pourtant, un quart (25%) des responsables informatiques admet ne pas informer son dirigeant en cas d'incident de ce type. Ce manque de transparence prive donc les dirigeants, considérés comme principaux responsables, d'une visibilité réelle sur les risques que représentent les fuites de données pour leur entreprise.

L'ampleur de ce constat est encore plus frappante dans une autre enquête menée par l'Economist Intelligence Unit pour le compte de VMware en début d'année. Celle-ci révélait en effet que seuls 8 % des dirigeants d'entreprises dans la région EMEA (11% en France) considéraient la cybersécurité comme une priorité. Alors que les cyberattaques s'intensifient et deviennent de plus en plus préjudiciables pour les entreprises – avec à la clé le risque de perte de propriété intellectuelle, de positionnement concurrentiel, et de données clients – l'impact sur la performance et l'image de marque peut être considérable.

Une nouvelle approche de la sécurité s'impose
Les entreprises sont de plus en plus menacées par de graves cyberattaques : plus d'un tiers (37 %) des répondants dans la région EMEA (seulement 28 % en France) s'attendent à en être victimes dans les 3 prochains mois. Malheureusement, les approches de sécurité actuelles ne sont pas adaptées à un monde toujours plus tourné vers les technologies numériques. Ainsi, plus d'un responsable informatique français sur trois (35 %) estime que l'un des principaux risques pour son organisation réside dans le fait que les menaces évoluent plus vite que les systèmes de défense mis en place.
« Le fossé entre dirigeants et responsables informatiques est symptomatique. Il symbolise le défi que doivent relever les entreprises cherchant à repousser leurs limites, à se transformer, à se différencier et à se protéger de menaces en constante évolution », déclare Sylvain Cazard, directeur général de VMware France. « Aujourd'hui, les organisations les plus performantes sont celles qui sont capables de réagir rapidement et de préserver aussi bien leur image de marque que la confiance de leurs clients. Les applications et données des utilisateurs étant présentes sur un nombre d'appareils sans précédent, ces entreprises ont abandonné les approches traditionnelles de sécurité informatique incapables de protéger les entreprises numériques d'aujourd'hui. »

Les employés et les processus aussi problématiques que les technologies
L'un des principaux risques pour la sécurité d'une entreprise provient de l'intérieur. Ainsi, pour 45 % des responsables informatiques de la région EMEA (et 37 % en France), la négligence ou le manque de formation des employés en matière de cybersécurité représente le principal défi pour leur entreprise. L'enquête montre également jusqu'où les salariés sont prêts à aller pour accroître leur productivité : 15 % d'entre eux (contre 21% au niveau EMEA) utilisent leurs appareils personnels pour accéder à des données professionnelles, tandis que 14 % (17% en EMEA) sont prêts à enfreindre la politique de sécurité de leur entreprise afin de travailler plus efficacement.
« La sécurité n'est pas qu'une question de technologie. Comme le montrent les résultats de notre enquête, les décisions et les comportements des employés ont également un impact sur l'intégrité d'une entreprise » remarque Sylvain Cazard. « Malgré tout, la solution n'est pas non plus de tout verrouiller et d'instaurer une culture de la peur. Les organisations qui adoptent des approches intelligentes proposent plus de moyens et non de restrictions à leurs employés, leur permettant de s'épanouir, d'adapter les process et de transformer leur activité pour réussir.»
« Les entreprises tournées vers l'avenir sont conscientes du fait que les stratégies de sécurité réactives d'aujourd'hui ne sont plus efficaces pour protéger leurs applications et données. Adopter une approche software-defined garantissant l'omniprésence de la sécurité leur offre la flexibilité nécessaire pour réussir en tant qu'entreprises numériques », conclut Sylvain Cazard.
Source: infoDSI.com

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise