La cybersécurité un problème sous estimée par les chefs d’entreprises

	La cybersécurité un problème sous estimée par les chefs d’entreprises

Les entreprises se jugent souvent prêtes à résister aux cyber-attaques alors que la réalité est bien souvent moins reluisante.

Plusieurs études sorties récemment convergent pour montrer un tableau assez catastrophique de la cybersécurité des entreprises alors que la perception affichée par celles-ci est plutôt marquée par l'optimisme. Ou bien faut-il mieux parler d'inconscience ? Ainsi, 62% des entreprises ont déjà subi une tentative de fraude selon une étude de Sage. 12% en ont même subi au moins cinq. La fraude la plus courante reste la fameuse *fraude au président*(usurpation d'identité d'un dirigeant pour obtenir un virement à l'étranger) : 80% des entreprises affectées l'ont rencontrée. 18% ont été victimes d'un *test bancaire* et 14% d'une fraude interne (cas classique : substitution de RIB).

Les trois quarts des DAF craignent avant tout les fraudes d'origines externes. La*fraude au président* et la falsification de RIB sont largement cités avant des cyber-attaques sur des données financières (un quart seulement des répondants). Des processus métier ont été mis en place pour parer ces fraudes non-technologiques comme la séparation créateur/valideur d'un paiement, la double signature… Le respect des procédures et la vigilance interne ont suffi à détecter des fraudes dans de nombreux cas. Mais 30% des entreprises continuent de valider leurs virements par un simple fax ! Suivant les recommandations des organismes professionnels, la bascule vers les traitements informatisés (EBICS TS, via les portails bancaires, etc.) est malgré tout bien engagée.

Une méconnaissance des bonnes pratiques et des règles

Mais il n'en demeure pas moins que la méconnaissance des bonnes pratiques pour sécuriser l'information reste importante. Selon une étude Solucom/Conscio, 46% des collaborateurs ne sont pas préparés à réagir à de l'ingénierie sociale dont la *fraude au président* n'est qu'un exemple caricatural. Pourtant, selon les auteurs de l'étude, l'ingénierie sociale est la méthode principale pour s'introduire dans les systèmes d'information des entreprises ou réaliser des fraudes, notamment par usurpation d'identité ou de couple identifiant/mot de passe.

Si 88% des collaborateurs sont sensibilisés aux règles pour gérer les mots de passe, 47% seulement les adoptent. Un mécanisme technique est donc nécessaire pour obliger à respecter les bonnes pratiques. Enfin, la même étude mentionne que la réglementation sur les données personnelles est méconnue par la majorité des collaborateurs, entraînant de ce fait un important risque juridique pour leurs entreprises.

Bienvenue aux malwares

L'ingénierie sociale est décidément bien ancrée dans les pratiques des cyber-criminels. Cibler précisément les attaques permet notamment, selon l'étude publiée par Cisco, d'introduire des #ransomware. Ce type d'attaque génèrerait 34 millions de dollars par an et par campagne. Etre victime de tels pratiques est assez gênant, ce qui explique sans doute que seules 21% des entreprises informent leurs partenaires, 18% les autorités et 15% leur compagnie d'assurance.

Bien entendu, les fondamentaux du cybercrime sont toujours d'actualité avec des variantes pour les maintenir au goût du jour. La compromission de serveurs est ainsi un classique pour mener des attaques indirectes, notamment via des CMS mal mis à jour. La compromission de domaines WordPress a ainsi augmenté de 221% entre février et octobre 2015. Parmi les mauvaises pratiques qui se développent, la non-mise à jour des infrastructures est en croissance.

La fuite de données via les navigateurs, souvent négligée, est pourtant en pleine croissance : des extensions malveillantes affecteraient 85% des entreprises. Les attaques à base de DNS sont également en plein boum, d'autant que les experts DNS ne travaillent que rarement avec les experts en sécurité. Malgré tout, il est estimé que la rapidité de détection d'une intrusion a augmenté même si elle reste dans une fourchette de 100 à 200 jours.

La cybersécurité sera le sujet de la Matinée Stratégique de CIO le 16 février 2016 : Cybersécurité : Les nouvelles menaces contre le système d'information. … [Lire la suite]

Réagissez à cet article

Source : *La cybersécurité reste une problématique sous estimée dans les entreprises – Le Monde Informatique*