Cyberattaques : les investissements en startups menacés ?

Les conséquences des cyberattaques ne cessent de prendre de l'ampleur. Bien que les réactions n'adviennent qu'après les attaques, les dirigeants des entreprises commencent à être vigilants avant d'investir dans un objet connecté ou un outil numérique.

Temps de lecture : minute

17 octobre 2018

Après Fed/Ex, Merck et Maersk l'an dernier, c'était au tour de Facebook, il y a deux semaines, de voir 50 millions de ses comptes piratés. Petites, moyennes ou grandes entreprises, particuliers ou dirigeants, personne n'est à l'abri d'une attaque informatique. Une étude menée en 2018 par Mazars, groupe international d'audit et de conseil, auprès de 203 dirigeants de grandes entreprises et d'ETI, montre que 40% des entreprises industrielles ont déjà subi une cyberattaque.

En outre, 50 000 PME françaises ont déjà été victimes de cyberattaques et près d'un tiers d'entre elles ont subi un dommage financier en 2017, selon une étude SystemX. Les entreprises se sentent de plus en plus menacées, 74% déclarant que leur entreprise est exposée aux attaques informatiques. Le sujet a été longuement débattu lors de la 18ème édition des assises de la Sécurité à Monaco du 10 au 13 octobre dernier.

Des attaques de plus en plus pointues

En cause : une évolution et une professionnalisation des pratiques. Les

pirates attaquent les systèmes d'informations pour accéder aux données confidentielles et détourner des fonds. Malgré les barrières de sécurité établies par les entreprises, leurs attaques deviennent de plus en plus ingénieuses et combinent différentes méthodologies, à l'image du rançongiciel, un virus qui bloque l'accès à un ordinateur, voire à tout un système, et exige le paiement d'une rançon pour restituer les données - et le contrôle des appareils. Une technique qu'un rapport récent du Forum économique mondial décrivait comme une véritable arme numérique.

Ainsi, 78% des dirigeants enquêtés par Mazars redoutent aujourd'hui que la transformation numérique de leur organisation aboutisse à une exposition accrue aux attaques informatiques. En effet, les mesures ne sont prises qu'après les attaques mais aucune précaution n'est prise pour les stopper. "*Les pirates ont toujours une longueur d'avance par rapport aux entreprises*", alerte David Luponis, associé expert cybersécurité et sécurité IT chez Mazars.

Des conséquences sur les investissements

Actuellement, l'image des startups est, elle aussi, menacée auprès des investisseurs. Ces derniers craignent en effet que des attaques ne surviennent qu'après que leur nom ait été apposé à celui d'une startup. Un problème qui se pose d'autant plus lorsqu'il s'agit d'objets connectés, de plateformes numériques ou d'applications dont les datas développées et conservées par les startupeurs, ne profitent pas toujours d'un système de sécurité fiable. "*La crédibilité des startups serait remise en question*", s'inquiète David Luponis, qui précise que la solution miracle n'existe cependant pas, malgré tout l'inventivité dont peuvent faire preuve les éditeurs et fournisseurs. "*La précaution à prendre serait de mettre en place une résistance à l'attaquant, le plus de barrière possible avant l'accès au système d'informations*".

Les experts s’entendent pour dire que seulement 2 à 3 % des budgets

informatiques sont dédiés à la cybersécurité, alors qu’il faudrait y consacrer plus de 10 %. Pour se prémunir face aux risques de cyberattaques, 56% des dirigeants considèrent qu'investir dans la sécurité de leur système informatique est la priorité. Les actions se porteront surtout sur la formation et les échanges d'expériences des employés pour qu'ils puissent acquérir les connaissances et compétences nécessaires sur les outils numériques. Ce qui leur permettra par la suite de faire face aux risques de cyberattaques.

Article écrit par Ny Ando Randrianarisoa