

Attaques informatiques : Comment s'en protéger ?

**Attaques ,informatiques, :
Comment s'en protéger ?**

Les cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.

Tous les quinze jours en moyenne, une attaque sévère – où des données sont exfiltrées – est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les entreprises. Julien Robert, directeur de la sécurité chez SFR, résume les trois facteurs agissant sur la sécurité : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les fournisseurs d'accès et l'encadrement d'un data center externe fortement conseillé.

Prévention

« *Il est difficile d'agir lorsque l'attaque a déjà eu lieu* », précise Sylvie Sanchis, chef de la Becti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

Tous les salariés doivent par ailleurs être formés car certaines intrusions sont rendues possibles par leur comportement, sans qu'ils en soient conscients, notamment par leur exposition sur Internet.

Les modes opératoires

Les modes opératoires d'exfiltration des données se diversifient et se sophistiquent au fil des années. Certains se veulent discrets afin que l'entreprise ne prenne connaissance de l'attaque que très tardivement, d'autres relèvent du chantage ou de la demande de rançon.

L'attaque peut venir d'un mail qui, à son ouverture, téléchargera un virus sur l'ordinateur de l'employé. Les données peuvent également être extraites grâce au social engineering, pratique qui exploite les failles humaines et sociales de la cible, utilisant notamment la crédulité de cette dernière pour parvenir à ses fins (arnaque au patron). Quant aux ransomwares, il s'agit de logiciels malveillants permettant de rançonner l'entreprise pour qu'elle récupère ses données. Dans ce cas, Anne Souvira, chargée de mission aux questions liées à la cybercriminalité au cabinet du préfet de police de Paris, précise que « *même si l'entreprise paye, il est très rare de récupérer toutes les données.* » Si elle peut être tentée de payer la rançon sans prévenir les autorités compétentes pour une somme modique, il n'y a aucune garantie de récupérer les données et les traces de l'attaque seront perdues. D'autres techniques de chantage sont utilisées, comme lorsque l'on se voit menacer d'une divulgation des vulnérabilités du système.

L'importance de porter plainte

La réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « *C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie* », selon Cirył Piat, lieutenant-colonel de la gendarmerie nationale. Suite à une cyber-attaque, la plupart des entreprises sont réticentes à porter plainte, par peur d'une mauvaise réputation ou par scepticisme vis-à-vis de la réelle utilité de cette procédure. Alice Cherif, chef de la section « cybercriminalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'investigation qui permettront de remonter au cybercriminel. « *Toute autre alternative est bien moins efficace et fait perdre un temps précieux à l'entreprise ainsi que des éléments d'investigation.* »

L'utilité du cloud

L'une des façons de sécuriser ses données est de les confier à un tiers spécialiste qui les stockera en ligne sur un cloud. « *Il s'agit d'un système complexe connecté sur Internet, où les données sont stockées sur des disques durs physiques situés dans des salles d'hébergement, les fameux data centers* », explique Julien Levrard, chef de projet sécurité chez OVH. Le cloud rend l'accès plus difficile aux malfaiteurs d'autant qu'ils ignorent la localisation de la donnée. Vigilance et prévention : les maîtres mots en matière de cybercriminalité.

Article original de Emilie Smelten

(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



Réagissez à cet article

Original de l'article mis en page : Cybercriminalité : comment se protéger ? – Magazine Decideurs