Le Cabinet ACDL Expertise vous informe :

Cybermenaces 2019: 4 tendances à surveiller

Cibles privilégiées des pirates, les entreprises doivent prendre conscience de l'importance de se protéger pour éviter des pertes financières et une dégradation de leur image. Le risque cyber est difficile à gérer car les attaques des pirates évoluent. Tour d'horizon des prochaines cybermenaces.

Cybermenaces 2019 tendance n°1 : les attaques de rançonlogiciels en baisse

L'année 2017 a été marquée par les attaques WannaCry et NotPetya qui ont eu une ampleur mondiale. Et les PME n'ont pas été épargnées, en 2017 50 000 d'entre elles ont subi une cyberattaque selon la Confédération des PME. En 2018, la menace reste active avec Gandgrab et SamSam. Pourtant les attaques de rançonlogiciels ont baissé de 30% entre 2016-2017 et 2017-2018 selon le dernier rapport Kapersky Security Network de l'entreprise de cybersécurité Kapersky Lab.

En 2019, le nombre d'attaques de rançonlogiciels devrait continuer à baisser mais elles seront plus ciblées. La vigilance est donc toujours de mise.

Cybermenaces 2019 tendance n°2 : le développement du spear phishing

Le phishing est désormais plus ciblé avec la technique du spear phishing. Plutôt que de s'attaquer à un grand nombre de victimes potentielles, les pirates visent une personne ou une entreprise particulière. Le pirate étudie la messagerie électronique et les réseaux sociaux de sa victime pour trouver des informations personnelles : nom de ses amis, de ses collègues, destination de ses dernières vacances…

Une fois le profil établi, il lui envoie un mail personnalisé ou un message sur les réseaux sociaux, en se faisant passer pour un associé, un ami, sa banque. Le but du pirate ? Inciter la personne à cliquer sur un lien malveillant ou à dévoiler des informations ses sensibles comme ses mots de passe, ses coordonnées bancaires ou son numéro de sécurité sociale.

Cybermenaces 2019 tendance n°3 : une hausse des attaques sur les données personnelles

Noms, adresses postales, numéros de cartes de crédit… les données personnelles d'environ 500 millions clients de la chaîne hôtelière Marriott ont été piratées. C'est ce qu'a annoncé le groupe américain en novembre. Le pirate avait accès à la base de données depuis quatre ans. Certains escrocs ne se contentent pas de dérober les données présentes dans les bases des entreprises, ils exigent ensuite une rançon pour ne pas divulguer sur le web ces informations.

Afin d'éviter d'entacher leur réputation et de déclarer la fuite à la Cnil, comme l'impose désormais le Règlement européen sur les données personnelles, certaines entreprises n'hésitent pas à payer. Les attaques devraient donc s'intensifier en 2019.

Cybermenaces 2019 tendance n°4 : l'authentification multifactorielle s'impose

La deuxième version de la directive européenne sur les services de paiement (DSP2) est entrée en vigueur en 2018. Un de ses objectifs ? Renforcer le niveau de sécurité des paiements en ligne avec une authentification forte combinant l'utilisation de deux éléments de trois catégories : quelque chose que l'on sait (mot de passe, code PIN), quelque chose que l'on possède (ordinateur, téléphone mobile), quelque chose que l'on est (empreinte digitale, rétine, voix). Cette authentification plus contraignante va s'imposer en 2019.

La responsabilité de chacun

Il est essentiel de former et sensibiliser ses salariés pour se protéger des menaces informatiques. D'autant que leur responsabilité peut être engagée en cas d'attaque.

Ainsi la charte informatique de l'entreprise peut interdire aux salariés la visite de certains sites ou encore le téléchargement de certains fichiers. En cas de non-respect de cette charte, la faute du salarié pourra être reconnue et aller jusqu'à son licenciement pour faute grave.

Les collaborateurs du cabinet se tiennent à votre disposition pour tout renseignement complémentaire.

Votre expert-comptable : Guillaume GAHIDE 03.27.62.18.11 / ggahide@acdl.fr