Que faire quand un salarié ne respecte pas les consignes de sécurité ?

Un enjeu de gouvernance pris en compte …

L'entreprise et l'administration d'aujourd'hui font face à de nombreux défis. Fortement dépendantes de leurs systèmes d'information, elles doivent ménager une place de choix à leur patrimoine informationnel numérique dans leur stratégie.

Développer et valoriser le patrimoine informationnel est aujourd'hui tant une nécessité qu'un atout commercial. Mais ce patrimoine attire également les convoitises des cybercriminels. Ceux-ci peuvent chercher à subtiliser les données de l'entreprise ou de l'administration pour les exploiter directement ou pour les revendre, ou à porter atteinte à leur intégrité pour compromettre les activités des entités.

Les salariés ont accès à Internet via leur outil de travail. Par ce biais, ils sont également exposés à des tiers malveillants, et ceux-ci peuvent les atteindre par leur messagerie professionnelle, leur messagerie personnelle ou encore par leurs comptes sur les réseaux sociaux.

Malgré les communications effectuées par les Ressources Humaines, malgré les recommandations de sécurité de la Direction Informatique, il arrive que certains collaborateurs n'aient pas conscience de leur rôle dans la protection du patrimoine informationnel de l'entité.

Par négligence, ces salariés permettent à des tiers de paralyser l'activité de leur entité. Par exemple, en cédant à des tentatives de *phishing*, ils permettent à des personnes malveillantes de s'introduire dans le réseau de l'entreprise ou de l'administration concernée et d'y subtiliser ou d'y détruire des informations sensibles. Le dernier baromètre du CESIN 2019[1] indique que le *phishing* est le mode d'attaque le plus fréquent, avec 73% des répondants victimes d'au moins une tentative.

Les moyens mis au point pour inciter le salarié à céder à la tentative d'hameçonnage sont nombreux et en perpétuelle évolution. Le plus souvent, les tiers malveillants utilisent les cas d'usages suivants :

1. Le salarié est tenté par le biais d'un bon cadeau, un billet pour un spectacle, un droit d'accès à un service, etc., qui aurait autrement été payant ;
2. L'usurpation d'identité : le tiers malveillant envoie un message en usurpant l'identité d'une personne connue, souvent un supérieur hiérarchique, pour tromper la confiance de la victime et l'inciter à céder aux demandes. On parle souvent dans ce cas de « *fraude au président* », qui ont lieu très régulièrement lieu aujourd'hui. Le dernier baromètre du CESIN précité indique que la fraude au président est le deuxième mode d'attaque le plus fréquent constatée dans les entités interrogées ;

Les conséquences sont souvent lourdes. Ces incidents ont un coût, tant en terme financier qu'en terme d'image. De tels incidents mettent à mal la confiance que les clients et les partenaires commerciaux accordaient à l'entité. Ils peuvent remettre en question la protection de leurs données, des informations stratégiques et confidentielles (secrets de fabrications, stratégies commerciales, etc.) échangées au cours des relations contractuelles. Les relations commerciales peuvent ainsi être sévèrement fragilisées.

[1] https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

Des actions en justice peuvent en découler, notamment si l'incident de sécurité a causé une atteinte aux droits de tiers. D'une manière générale, un incident peut avoir des conséquences multiples et complexes sur l'ensemble de l'entité et ses salariés.

Au-delà de la simple sensibilisation générale, il est judicieux d'élaborer une stratégie de communication interne visant à prévenir et contrer les incidents les plus probables. Les communications pourront comprendre des exemples précis de cas d'attaques cyber réussies, des exercices de mise en situation avec des tests de faux messages en provenance des hackers, etc.

Dans ce cadre, la meilleure pratique reste la sensibilisation régulière de l'ensemble des collaborateurs et la diffusion large de l'information. Cette sensibilisation aux pratiques frauduleuses et aux enjeux de la cybersécurité permettra de réduire le risque de survenue de ce type d'incident.

Toutefois, la sensibilisation ne suffit parfois pas. Comment sanctionner un salarié qui ne respecte par les principes de précaution et de sécurité prônés par son employeur ? Quels sont les possibilités qu'offre le droit français pour agir contre un salarié ?

… Au sein de la réglementation française :

Si le salarié a commis une faute, l'employeur peut prendre une mesure disciplinaire à son encontre, qui doit être proportionnée à la faute commise.

En premier lieu, il convient d'établir que le salarié a commis une faute. Est une faute « *tout agissement du salarié considéré comme fautif par l'employeur* » (article L.1331-1 du Code du travail). Par exemple, il s'agira de démontrer que le salarié, en ne respectant pas une consigne de sécurité qui lui a été communiquée, a commis une faute. Pour cela, il faudra prouver que les consignes de sécurité informatique ont effectivement été communiquées au salarié, par le biais de sensibilisations par la direction des ressources humaines, des systèmes d'information, ou encore par le biais d'une charte informatique.

A noter qu'un employeur peut sanctionner différemment deux salariés ayant commis la même faute, au regard notamment de l'ancienneté, du comportement de chacun ainsi que de leur fonction. En cas de contestation, il revient au juge d'estimer si la sanction disciplinaire était effectivement proportionnée.

Si l'employeur est libre du choix de la forme de la sanction, toutes les sanctions disciplinaires ne sont pas permises. Ainsi, il n'est pas autorisé de prononcer de sanction pécuniaire à l'encontre d'un salarié.

De plus, pour les structures d'au moins 20 salariés, l'employeur ne peut prononcer que des sanctions prévues au règlement intérieur. L'absence de règlement intérieur équivaut alors à priver l'employeur de pouvoirs en matière disciplinaire, à l'exception du licenciement. Rappelons que la charte informatique, pour avoir un caractère disciplinaire, doit être annexée au règlement intérieur. Cela suppose notamment qu'une information préalable, individuelle et collective, soit délivrée aux salariés.

Pour résumer, il convient l'importance d'avoir une charte informatique à jour et de sensibiliser régulièrement l'ensemble des collaborateurs, compte tenu des évolutions constantes de l'état de la menace.

Michel JUVIN

Garance MATHIAS

Avocat Associé – Fondateur MATHIAS Avocats