Sécuriser sa messagerie professionnelle : pourquoi et comment faire ?

La sécurité de vos emails. Une option ? Les attaques de phishing ou de spear phishing sont à l'origine de 93 % des violations de sécurité des réseaux.

Autre chiffre avancé également par Vade Secure, plus de 80 % des emails malveillants ont diffusé des ransomwares et des chevaux de Troie bancaires qui sont devenus les programmes malveillants les plus distribués. Il y a des chiffres qui parfois résument à eux seuls une situation, et ceux-ci traduisent bien le besoin urgent de sécurisation des mails, qu'elle passe par la technologie ou par la sensibilisation. Attaques de phishing, de spear phishing, ransomware, malwares, sont toutes en croissance explosive et touchent de façon indifférenciée toutes les activités économiques, militaires et civiles d'un État. Les impacts sont quant à eux alignés avec la nature des activités.

Des retours d'expérience menés ont pu dresser les risques par secteurs d'activité et si certains en doutaient, peu d'activités sont à l'abri. Les banques demeurent des cibles de choix notamment pour des attaques de spear phishing pouvant entraîner des vols d'informations stratégiques, des données à caractère personnel comme des informations bancaires, à commencer par le numéro de carte de crédit ou un encore le statut du client.

Le secteur de la vente au détail n'est pas épargné et ce à plusieurs titres. Fraude au président grâce à du spear phishing, vol d'informations en masse grâce à des actions de phishing plus classiques, ou encore de l'escroquerie à l'achat afin de voler de la marchandise et tout ceci grâce à des attaques passant par mail. Pour les secteurs des produits pharmaceutiques et de la technologie, où l'information numérique représente parfois des investissements colossaux, là encore le spear phishing, fait ici dans une pure logique d'espionnage industriel, peut avoir des conséquences particulièrement coûteuses. Les concurrents peuvent avoir accès à des informations confidentielles relatives à la propriété intellectuelle, qui résultent de nombreuses années de développement et de millions d'investissement.

Les industries de défense peuvent être également victimes d'espionnage industriel, pour le compte d'un membre du secteur privé ou d'autres États. Les entreprises de défense sont les cibles fréquentes de services de cyberguerre de puissances étrangères. Ces guerres certes silencieuses font pourtant des ravages. La santé enfin. Les établissements de soins de santé sont tenus de respecter des règles strictes. Ils sont exposés à de sévères sanctions financières et juridiques en cas de violations des données par un tiers. Au vu du caractère sensible des données médicales personnelles, toute fuite risque également de nuire à la réputation de l'établissement concerné. Comme l'ont récemment découvert de nombreuses caisses d'assurance maladie, la protection contre l'usurpation d'identité de dizaines de millions de preneurs d'assurance dont le nom, l'adresse et le numéro de sécurité sociale ont été piratés, peut coûter très cher.

Réduire les risques passe d'abord par de bonnes pratiques

Les cas explicités plus haut le démontrent. N'importe qui peut vous envoyer un email en se faisant passer pour un autre. Et malheureusement, ce n'est pas si difficile. Comme l'ANSSI, autorité de

référence et de contrôle en la matière, le rappelle souvent, quelques bonnes pratiques et réflexes sont nécessaires à faire adopter aux employés des entreprises.

- Vérifiez les noms et adresses email des expéditeurs afin d'éviter une attaque homoglyphe : une règle s'impose, celle de la méfiance : Partir du principe que l'expéditeur n'est pas celui qu'il prétend en vérifiant d'abord l'adresse email et voir si elle ne contient pas de piège (une lettre en plus, un « i » transformé en « l », nom de domaine légèrement amendé ou autre subterfuge.) Si le mail ne correspond pas aux habitudes de l'expéditeur habituel, si des liens sont présents, un coup de fil sera toujours préférable. L'expéditeur dont le message est urgent saura toujours vous trouver.

- Tourner votre souris 10 fois, avant de cliquer sur des pièces jointes : les pièces jointes sont des nids à virus et autres programmes malveillants. L'entreprise doit donc avoir des antivirus activés et bien évidemment à jour.

- Toute vérité n'est pas bonne à dire surtout quand elles concernent vos données personnelles : les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires de l'entreprise, etc.). En cas de doute, là encore, il est préférable de demander à son correspondant légitime de confirmer sa demande car il se peut que ce soit une tentative de phishing.

- Vérifier l'architecture des liens, et la langue employée / les fautes : en passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, c'est le moment d'être méfiant, et d'éviter de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur. Si la langue utilisée est malmenée, cela doit vous alerter. Mais néanmoins, les menaces évoluent et ce défaut des cybercriminels a tendance à se corriger.

- Paramétrer correctement les messageries professionnelles : sur le plan technique, il est important de mettre en place des mécanismes de protections. Qu'ils existent pour vous protéger d'une usurpation de votre domaine (vous recevez un email d'une personne se faisant passer pour l'un de vos collaborateurs), ou pour préserver la réputation de votre nom de domaine (afin de ne pas voir systématiquement nos emails dans le répertoire spam de votre destinataire) les protocoles DKIM et SPF sont à configurer sur votre nom de domaine.

- « L'humain reste humain », la sensibilisation ne fait pas tout : si l'entreprise a le devoir de sensibiliser ses employés à toutes ces bonnes pratiques, il importe de faire preuve de réalisme et de pragmatisme. Les solutions de messagerie professionnelles du marché - à commencer par la suite Office 365 particulièrement prisée des grandes entreprises - ont fortement revu à la hausse leurs exigences de sécurité. Mais malheureusement les solutions natives de ces solutions ne suffisent pas.

D'abord, c'est un problème statistique. Le nombre de mails reçus par un employé aujourd'hui est substantiel par rapport à son temps de travail. Bien que les solutions de sécurité existantes arrêtent une large part des menaces, le pourcentage de risques résiduels correspond à un nombre bien trop important de mails pour être écarté. En effet, si le pourcentage est faible, le chiffre ne l'est pas et la probabilité de cliquer sur un mail malveillant est quasiment avérée. L'humain reste l'humain.

Ensuite, c'est une question de menace qui évolue et qui malheureusement a des capacités de régénération trop forte pour être absorbée par des produits de sécurité classique. Le Gartner a d'ailleurs mis en garde sur le faux sentiment de sécurité que peuvent avoir les utilisateurs sur la solution Office 365, en recommandant de se doter de systèmes de protection spécialisés complémentaires. En effet, les entreprises restent non seulement responsables de la sécurité de leurs données, mais en plus, le barrage que constituent les solutions traditionnelles est de plus en

plus mince pour les cybercriminels.

L'intelligence artificielle au secours des nouvelles formes de menaces

La plupart des solutions du marché s'appuie sur des techniques de réputation des IP, de fingerprint ou encore de sandboxing pour détecter les menaces. Cela signifie qu'elles sont capables de bloquer principalement les attaques connues et que pour les nouvelles menaces, elles laissent passer les premières vagues avant de les identifier et trouver des patchs de sécurité. Elles sont aujourd'hui dépassées par l'évolution des techniques d'attaques qui sont de plus en plus sophistiquées et difficilement détectables : de faible volume, polymorphes ou encore très personnalisées. Et une seule attaque réussie peut faire de réels dégâts.

C'est la raison qui explique qu'aujourd'hui, l'entreprise se doit non seulement de sécuriser nativement sa messagerie mais de faire le choix de solutions complémentaires qui enrayent les menaces de type Zero day et à fortiori en cas de messagerie hébergée dans le Cloud. Heureusement l'intelligence artificielle a fait son entrée et les technologies de sécurité sont maintenant capables de combler les trous dans la raquette des mesures de sécurité déjà embarquées.

On ne parle pas là de la boule de cristal de madame Irma, mais bien de techniques qui permettent d'évaluer le niveau de dangerosité d'un email grâce à la détection de signaux faibles complémentaires issus de l'analyse de l'origine, du contenu, mais également du contexte de l'email. Des algorithmes prédictifs sont ainsi conçus grâce à l'analyse quotidienne de millions d'emails et permettent de concevoir des règles de détection des emails vérolés. Les entreprises qui ont fait le choix de ce type de solution de protection de leur messagerie ont été largement épargnées par les dernières vagues d'attaque.