Sélection du mois d'avril 2016

Le braquage numérique : un risque réel pour les PME

En dépit d'une sensibilisation plus importante concernant la violation de la sécurité et de la perte de données soulignée par la nouvelle étude Risk:Value du spécialiste de la gestion du risque et de la sécurité de l'information, NTT Com Security (Global Security Mag, février 2016) ainsi que des partenariats défensifs qui se nouent entre les pouvoirs publics et les entreprises privées autour de pôle cyberdéfense, les cyberattaques ne cessent d'augmenter. Les PME françaises y sont particulièrement exposées par rapport à la moyenne européenne. Or selon Stéphane Richard, PDG d'Orange (La Voix du Nord, 05/02/16), « Pour une entreprise, la question n'est plus de savoir si elle va se faire attaquer, mais quand » ajoutant que le vol de données est en passe de devenir « l'or du XXIème ». Le braquage numérique constitue un risque jugé sérieux pour les PME.

Un manque de prévention spécifiquement français

Il se révèle au travers d'une étude citée par l'Argus de l'Assurance, (20/01/16), et réalisée par le cabinet d'audit PWC qui a interrogé les entreprises françaises, composées à 99,8 % de TPE/PME, que seulement 5 % du panel est équipé d'une assurance cyber. Les principaux freins à la souscription demeurent notamment le sentiment de ne pas avoir besoin de protection, l'absence d'information et le manque de clarté des offres. Les entreprises françaises se sentent peu, ou pas, exposées à la cybercriminalité (83 % des dirigeants). « Une des raisons de cette prise de conscience déficiente tient dans la relégation des responsabilités cyber aux seules équipes techniques », analyse PWC alors que le facteur humain tient une large part dans la menace cyber. Un manque de prévention dommageable.

Sensibiliser ses collaborateurs aux vulnérabilités

La technique phare utilisée actuellement par les hackers est celle du ramsonware. Elle consiste à placer un virus aspirant ou bloquant toutes les données. Pour les récupérer, une rançon doit être payée, généralement en bitcoin. Au cœur de cette technique, le smartphone fait réellement figure de maillon faible. Le ransomware va être placé préférablement dans les applications que tout à chacun télécharge sur son mobile, mais il faut savoir qu'un SMS, une photo peuvent également être des points d'entrée pour un délinquant numérique. La connexion du smartphone au monde professionnel fait actuellement de celui-ci le vecteur prioritaire des attaques pour pénétrer le réseau d'une entreprise. Il faut bien se rendre compte que les extractions de données (qu'il s'agisse des contacts, des SMS, des identifiants, des codes personnels) ne sont que des réalités techniques et loin d'être insurmontables qui plus est. L'utilisation actuelle des smartphones manque de prudence et dénote un retard dans une prévention ciblée. Comme l'a souligné Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), « Nous avons encore affaire à beaucoup de naïveté et d'angélisme », (La Voix du Nord, 05/02/16), lors du FIC 2016 (Forum international de la cybersécurité. Concernant le ransonware, la seule parade réside dans la sauvegarde régulière des données. Récemment, un coiffeur de Glasgow a payé 1 000 € pour récupérer son fichier client, crypté par une intrusion informatique. En février 2016, un ransomware a paralysé le Hollywood Presbyterian Medical Center, un hôpital de Los Angeles. Pendant une dizaine de jours, l'établissement a refusé de payer la rançon de 15 000 euros, demandant à son personnel de prendre toutes ses notes sur papier. Une situation qui ne pouvait pas durer : les laboratoires et salles de scanners de l'établissement sont dépendants de cette connexion. Certains patients ont d'ailleurs dû être transférés dans les établissements des alentours. Finalement, totalement paralysé, le Hollywood

Presbyterian Medical Center a cédé. Il s'agit du quatrième établissement médical américain, victime ces derniers mois (L'Expansion, 18/02/16). En France, le cabinet d'avocat Hawadier à Saint-Raphaël (Var) a été victime en mai 2015 d'une attaque par ransomware. Un véritable séisme pour ce cabinet qui gère plus de 4.600 dossiers. "Nous avons perdu un mois et demi de travail, à essayer de les reconstituer, a indiqué Me Elric Hawadier au tribunal correctionnel de Draguignan. Les sauvegardes n'avaient pas fonctionné, et ce n'est que six mois plus tard que nous avons pu récupérer nos données. Sinon, c'était la mort du cabinet. C'était l'angoisse permanente de laisser passer un délai d'appel ou de forclusion. Les conséquences ont été très préjudiciables". (Var Matin, 12/01/16). L'enquête a finalement montré qu'elle avait été menée à distance, par la société qui avait assuré pendant dix ans la maintenance du système informatique du cabinet. Une société dont le contrat avait été rompu quelques mois auparavant. La gérante de la société Quadri-concept à La Seyne-sur-Mer, son directeur commercial, et leur ingénieurs réseaux, ont reconnu devant le tribunal être responsables de cette cyberattaque.

Les utilisateurs ne sont pas encore suffisamment méfiants à l'égard des courriers électroniques suspects. Le phishing reste le premier vecteur d'attaque par e-mail. Or, des solutions existent, en cas de doute sur un mail, il est possible de le faire vérifier sur le site Phishing-initiative.fr où en 20 minutes maximum, un expert dira s'il s'agit d'une page frauduleuse. Ce site qui fonctionne 24/24 et 7 jours sur 7, a permis à 20.000 internautes d'éviter d'être victimes de ces attaques (20 Minutes, 25/01/16). L'identité de l'envoyeur devrait être reconnue avant toute ouverture de pièces jointes et son adresse web vérifiée selon les experts participant aux Assises de la Sécurité 2015.

Un danger, plus sérieux, apparaît avec le spear phishing, un hameçonnage personnalisé de la victime. Les criminels procèdent en amont à un travail d'ingénierie sociale, cherchent et analysent toutes les infos sur la cible qui traînent sur le Web. Ce qui permet de lancer une attaque élaborée (chantage ou vol de données). Difficile en effet désormais d'accéder à un service en ligne sans créer de compte, s'identifier et donc dévoiler un peu de sa personne. Toutes ces informations sont plus diverses, plus complètes. Les posséder, c'est l'assurance d'avoir un moyen de pression sur la victime, voire de monnayer plus tard ce que l'on a subtilisé.

A l'heure de l'interface universelle, il faut désormais au contraire cloisonner au maximum, séparer les activités ludiques et privées du smartphone et celles liées aux informations professionnelles, soit en n'utilisant l'appareil que pour l'une ou l'autre de ces interfaces, soit en disposant de deux appareils, chacune affectés à leur secteur et de limiter très fortement de manière générale l'utilisation de ces appareils sur des informations sensibles. Certaines entreprises, notamment outre-Atlantique ont commencé à mettre en place au sein de leur organisation des politiques de sécurité IT très restrictives. Déjà en vigueur dans les grands groupes, ces règles arrivent maintenant dans les petites entreprises désormais prises pour cible. Dans une PME de moins de 50 personnes du secteur industriel, la direction enjoint ses salariés de ne pas utiliser de mots de passe, ni accéder à un fichier sans autorisation. Elle leur demande aussi de ne pas rechercher de notes de communication archivées sans y être autorisé. Pas question non plus de se servir de la messagerie pour des engagements externes à l'entreprise.