Phishing sur mobile : comment les administrations françaises peuvent donner l'exemple

Ces "qualités" partagées toutefois, qui sont essentielles pour garantir l'efficacité de toute grande organisation, les rendent aussi plus vulnérables aux attaques de phishing. Plus il y a d'employés, de terminaux, interactions et échanges d'informations, plus le risque est grand de rencontrer des incohérences et des vulnérabilités que des attaquants peuvent cibler et exploiter

La gravité de ce problème ne peut être sous-estimée. Une récente enquête initiée par le Government Business Council aux Etats Unis a révélé que pas moins de 47% des employés du secteur public ont rencontré une attaque de phishing dans le cadre de leurs activités professionnelles sur un terminal mobile.

Les données récoltées pour la France montrent que 51,3% des terminaux ont reçu au moins une attaque de phishing en 2019, tous secteur confondue. Pour empêcher ce chiffre d'augmenter, nous devons comprendre *pourquoi* les employés sont ciblés *en masse*.

L'attrait de la mobilité est une arme à double tranchant

Poussées par la nécessité, les évolutions culturelles et les nouveaux comportements de leurs employés, les administrations publiques se sont converties au monde 'cloud-first, mobile-first'. En rendant les informations accessibles à partir de n'importe quel terminal, les employés peuvent travailler à distance avec une plus grande souplesse en étant plus productifs.

Toutefois, les terminaux mobiles sont beaucoup plus difficiles à contrôler et à sécuriser que s'ils étaient connectés à un même réseau interne, spécialement si la moitié d'entre eux accèdent à leurs données via un réseau externe, comme l'a révélé une récente enquête du Government Business Council.

Ces résultats sont tous deux emblématiques d'une modification nécessaire de nos méthodes de travail, car les données sont désormais migrées dans le cloud, et les employés peuvent accéder aux informations à partir de différents types de terminaux, où qu'ils soient. En conséquence, les équipes de sécurité ont de plus en plus de mal à les protéger dans un environnement toujours plus disparate et vulnérable.

Pour les administrations publiques, le problème principal vient du décalage entre les politiques de sécurité définies en interne et la manière dont les employés les respectent. Si ces derniers travaillent à l'extérieur du réseau, il est quasi impossible de contrôler et gérer leur activité sans empiéter sur leur vie privée ou les mettre sous surveillance constante.
Toutefois, l'incapacité à y parvenir peut-être préjudiciable. Par exemple, si un employé travaille

depuis son téléphone portable et reçoit un SMS ou un message instantané de phishing, contenant un lien malveillant, il peut très facilement tomber dans le piège et cliquer dessus.

En fait, les utilisateurs ont trois fois plus de chances d'être victimes d'une attaque de phishing sur le petit écran d'un smartphone que sur un ordinateur. De même, il peut se connecter sur un 'hotspot' WiFi public non sécurisé dans un café, et exposer son terminal, et les informations professionnelles qu'il contient, aux attaquants à proximité.

Quelle protection choisir ?

Donc, que peuvent faire les administrations françaises pour protéger leurs employés à distance s'ils ne respectent pas les règles à la lettre?

La réponse, en théorie, est assez simple : elles doivent mettre en place une solution de protection contre les menaces mobiles qui garantit la sécurité du terminal même lorsque les utilisateurs visitent un site web malveillant, installent une application risquée ou se connecte à un réseau wifi piraté. Ceci nécessite de déplacer la sécurité sur le terminal lui-même et d'adopter une solution de sécurité qui protège contre les attaques de phishing qui ciblent les utilisateurs via une variété de canaux, qu'il s'agisse de SMS, d'applications de messagerie, d'emails, de jeux ou de réseaux sociaux.

Mais dans le même temps, la solution de sécurité doit être discrète et non intrusive, de sorte que les utilisateurs puissent continuer à travailler avec leur téléphone avec confiance et souplesse.
En contrôlant en continu la santé des terminaux qui accèdent à des informations sensibles de cette façon, le secteur public peut se protéger contre les attaques de phishing tout en profitant des avantages du monde 'mobile-first, cloud-first'.