acteurspublics.com

lundi 10 février 2020 14:24
1247 mots - 5 min

: ACTEURS PUBLICS VIP

Comment insuffler une culture de la sécurité

Les experts sont unanimes : l'Homme est le maillon faible de toute politique de cybersécurité. Différents dispositifs, ludiques ou ultraréalistes, permettent d'éveiller les consciences et d'inculquer les bons réflexes.

© Tierney – Adobestock.com

La communauté urbaine Grand Paris Seine & Oise (GPS&O) prend le risque cyber très au sérieux. La plus grande communauté urbaine de France avec quelque 405 000 habitants répartis dans 73 communes des Yvelines a été, dans un passé récent, victime de deux cyberattaques. La première remonte au 8 mars 2017, la seconde au 25 octobre dernier. Pour cette dernière, il s'agissait d'une attaque par ingénierie sociale. Muni d'un RIB fictif, un pirate a tenté de détourner une importante somme d'argent. Il a appelé la direction des finances de la collectivité en prenant l'identité d'un fournisseur sur une relance de factures.

“Cela montre combien les agents sont en première ligne, en déduit Jalal Boularbah, directeur « systèmes d'information et usages numériques » à GPS&O. Une grande partie des incidents de cybersécurité sont liés à une faille humaine.” Pour rappeler que la sécurité est l'affaire de tous, il a voulu faire évoluer les comportements en combinant des actions de communication, de sensibilisation et de formation.

Les formations anxiogènes ou institutionnelles donnant rarement de bons résultats, il a adopté une approche plus engageante, fondée sur des mises en situation. La communauté urbaine, qui emploie environ 1 000 agents, utilise depuis deux ans la plate-forme Sensiwave de Conscio Technologies, qui fait appel à des saynètes, des vidéos, des quizz.

Sensibilisation en douceur

“La personnalisation de l'outil et son caractère ludique permettent de sensibiliser en douceur, poursuit Jalal Boularbah. Chaque trimestre, nous diffusons des saynètes de deux minutes au maximum qui traitent d'un point particulier, en le resituant dans le contexte de la communauté urbaine. Ce focus est fait sur une thématique donnée comme le mot de passe, le phishing, le RGPD ou l'ingénierie sociale. En moyenne, nous obtenons de 25 à 30 % de participation.” La direction du système d'information et des usages numériques organise aussi des matinées dédiées à la protection des données, les “Jeudis-tech”. Il s'agit de voir, par exemple, comment sécuriser les fichiers pour prévenir les fuites.

En amont de ce parcours de sensibilisation à la cybersécurité, la communauté urbaine GPS&O a lancé une simulation de cyberattaque afin d'évaluer les réactions, et ce sans que les utilisateurs soient prévenus. Cette campagne a permis de cartographier les comportements et de savoir quel pourcentage d'utili-

sateurs s'étaient laissé piéger, compromettant la protection des données personnelles.

“Nous sommes dans la sensibilisation, pas dans le jugement, poursuit Jalal Boularbah. Je ne veux pas jouer le rôle du « Docteur No ». La sécurité absolue, c'est la mort de la donnée, de la collaboration et de l'innovation. Il faut avoir une approche d'équilibriste. Les agents n'ont aucune restriction sur leur poste de travail. Mon objectif est que l'utilisation de l'outil informatique soit aussi simple que l'utilisation d'un terminal personnel avec, bien sûr, derrière, les exigences de sécurité.”

La simulation de cyberattaque est aussi utilisée par la plate-forme Avant de cliquer, qui vise à prévenir l'hameçonnage, une des cybermenaces les plus répandues, 90 % des cyberattaques ayant pour origine un courriel frauduleux. Selon Stéphane Tabia, son cofondateur, la sensibilisation se fait en 3 parties. Pour évaluer le niveau de risque, la plate-forme envoie, comme dans le cas de GPS&O, de faux e-mails infectés aux agents, sans information préalable. “C'est une étape optionnelle, explique Stéphane Tabia. Certaines collectivités préfèrent communiquer en amont. D'autres concentreront les efforts de formation sur les 15 à 20 % des agents qui auront cliqué sur le lien ou la pièce jointe.”

Mises en situation et modules d' e-learning

Cette formation se présente sous forme de contenus en e-learning, avec des modules de 35 minutes, découpés en capsules d'une à deux minutes sous forme de vidéos, avec ou sans le son, ou en mode texte. Le principe de l'hameçonnage y est abordé dans une approche de vulgarisation. D'après Stéphane Tabia, la formation est bien suivie car elle intéresse les personnes à titre professionnel comme personnel car, relève-t-il, “elles sont aussi confrontées aux risques de phishing dans leur vie privée.”

Les mises en situation peuvent ensuite être envoyées automatiquement tout au long de l'année comme autant de piqûres de rappel. Différents types de mails apparaissent dans les messageries, dans un ordre aléatoire. Le courriel peut comprendre un lien demandant à l'utilisateur de mettre à jour Outlook sinon il perd tous ses contacts. Un autre mail peut intégrer une pièce jointe, une invitation à télécharger un fichier ou à saisir ses identifiants dans un formulaire. “Le message peut sembler provenir de la DSI elle-même, explique Stéphane Tabia. Si l'agent tombe dans le piège, il lui est proposé de revoir ce qu'il aurait dû faire avec le module d'e-learning correspondant.” La campagne peut ainsi durer de six mois à un an. La plate-forme remonte différents statiques par utilisateur, service ou entité. Elle va se concentrer sur les utilisateurs moins vigilants, qui recevront davantage de leurres, sachant que 90 % des clics fautifs proviennent de 10 à 15 % d'utilisateurs.

Former les experts comme les élus ou les agents

Il n'y a pas de profil type, cela concerne tout le monde y compris les élus ou… les collaborateurs du service informatique. “Les jeunes, et notamment les stagiaires, ont tendance à beaucoup cliquer, constate Stéphane Tabia. En revanche, ils apprennent plus vite. Le but n'est pas d'être dans la stigmatisation ou la sanction, mais bien dans la prévention.”

Confrontés à une pénurie de spécialistes de la sécurité informatique (lire encadré), les acteurs doivent non seulement sensibiliser les agents, mais aussi former leurs experts cyber. Institut de formation qui a formé plus de 15 000 personnes à la cybersécurité depuis 2015, Orsys vient, à cet effet, de sélectionner la plate-forme CyberRange d'Airbus CyberSecurity.

Cette plate-forme permet de faire des entraînements dans un environnement ultraréaliste. Deux équipes, l'une en rouge, l'autre en bleu, symbolisant les défenseurs et les attaquants, s'affrontent. “En modélisant le système d'information d'une organisation, la plate-forme permet virtuellement de tester sa résilience”, estime Giuseppe d'Arco, directeur des grands projets chez Orsys.

Le “bug bounty” pour pallier la pénurie de compétences

Selon Guillaume Vassault-Houlière, P.-D.G. de Yes We Hack, il y aurait 3 millions de postes non pourvus dans la cybersécurité dans le monde. Cette pénurie de compétences serait encore plus aiguë pour les acteurs publics souffrant d'un manque d'attractivité. Pour contourner le problème, Yes We Hack fédère une communauté de plus de 10 000 hackers présents dans 110 pays. Selon le principe du bug bounty, ces experts en sécurité gagnent des récompenses lorsqu'ils font remonter des failles découvertes dans un produit ou un service.

“Les organisations faisaient jusqu'alors un audit de vulnérabilité par an, avance Guillaume Vassault-Houlière. Cela les rassurait psychologiquement, mais aujourd'hui, la sécurité opérationnelle doit être testée en continu.” La start-up française a notamment pour références la métropole de Rennes, Aéroports de Paris, la Caisse des dépôts et consignations, la direction interministérielle du numérique de l'État (Dinum) et le commandement de la cyberdéfense (ComCyber) du ministère des Armées.

https://www.acteurspublics.fr/upload/media/default/0001/27/35d452a11f72c1c66624a85c7e06d7911d3ec3e6.jpeg

https://www.acteurspublics.fr/media/cache/default_news_big/upload/media/default/0001/27/35d452a11f72c1c66624a85c7e06d7911d3ec3e6.jpeg

par Acteurspublics