Abo **Armer les entreprises**

Les employés au cœur de la cybersécurité des PME

Une campagne de cyberattaques éducatives de l'EPFL a ciblé pendant deux mois des entreprises de l'arc lémanique. Un quart des employés ont été piégés.

Mathias Délétroz

Publié: 09.02.2023, 21h23

Dans le cadre du programme Trust4SMEs, une campagne d'envergure de prévention en matière de cybersécurité a été menée pour la première fois en Suisse romande.

Florian Cella

«Quand on a reçu le faux e-mail de phishing *(ndlr: une technique dont se servent les pirates informatiques pour soutirer des renseignements)*, quelqu'un

l'a directement signalé sur le groupe WhatsApp de l'entreprise, on ne s'est pas fait avoir.» Cette saine réaction, entendue ce jeudi matin à l'EPFL, n'a toutefois pas été la règle lors de la campagne de phishing éducative menée ces deux derniers mois par la Trust Valley (pôle de compétences en matière de cybersécurité) en collaboration avec 25 PME de la région lémanique.

Alain Mowat, expert en cybersécurité, a présenté les résultats d'une série de cyberattaques fictives devant un auditoire de près de 200 employés et directeurs de ces entreprises. Ouverture de courriels contenant un lien piégé: 681 sur 2562. Mots de passe récoltés sur des faux sites web imitant des services comme LinkedIn ou le webmail de Microsoft: 70, dont plus de la moitié étaient beaucoup trop faibles.

Certaines personnes dans la salle poussent des exclamations de surprise. Et pour cause: quelques minutes plus tôt, quand le «hacker éthique» leur a demandé qui savait détecter un e-mail frauduleux, presque toute la salle a levé la main. La sensibilisation a peut-être joué un rôle.

> **«Un employé bien formé peut être précieux pour la sécurité de l'entreprise.»**
>
> Alain Mowat, expert en cybersécurité pour SCRT SA

Cet événement a marqué la fin de la première année du programme Trust4SMEs, soutenu par le Canton de Vaud, la Confédération, l'EPFL et plus d'une trentaine d'entreprises privées. Pendant un an, chaque PME participante a été formée à la cybersécurité et a bénéficié d'une subvention de 50'000 francs. Le but: protéger l'économie régionale dans un contexte mondial de hausse des cyberattaques. Selon le rapport sur la cybersécurité de Check Point, les cyberattaques auraient augmenté de 38% dans le monde en 2022 ↗ par rapport à 2021. Et de 61% en Suisse.

L'importance de la prévention

Pendant plus de deux heures, Alain Mowat et son acolyte, l'expert en cybersécurité Mahandry Rambinintsoa, ont alterné entre démonstration de piratage en direct, astuces pour protéger son entreprise à son échelle et statistiques. Car «le piratage demande de comprendre la technologie et l'humain», explique Alain Mowat. Mais il tient à nuancer nos failles: «On entend souvent dire que l'être humain est le maillon faible dans la cybersécurité mais, dans beaucoup de cas, un employé bien formé peut être précieux pour la sécurité de l'entreprise.»

Pour cela, le nerf de la guerre tient en un mot: communiquer. Et ne pas hési-

Pour cela, le nerf de la guerre tient en un mot: communiquer. Et ne pas hésiter à demander de l'aide. «Dans les attaques bien faites, il y aura toujours quelqu'un qui se fera avoir. Ce n'est pas dramatique, ça peut arriver à tout le monde, mais il faut le signaler au service informatique», insiste Alain Mowat.

Les mots de passe, porte d'entrée principale des pirates

Et si l'on tombe dans le piège d'un lien malveillant, voire que l'on entre son mot de passe dans un faux formulaire, ne jamais utiliser deux fois le même sésame peut limiter la casse. Il faut aussi qu'il soit fort et évite des schémas répétitifs: «Lausanne2023! est trop faible, tout le monde met une date et un point d'exclamation à la fin», sourit l'expert.

L'idéal serait d'utiliser une phrase plutôt qu'un mot, avec des termes personnels. Mais comment retenir tout cela? Le gestionnaire de mots de passe est une solution, que compte d'ailleurs appliquer cette comptable active dans la finance et croisée à la sortie: «Je ne sais pas si j'ai été piégée, car je reçois énormément d'e-mails. Mais actuellement, j'emploie le même mot de passe à plein d'endroits, je vais changer ça.» Et si vous craignez d'avoir déjà été piraté, un petit contrôle sur le site *haveibeenpwned.com* ↗ peut vous éclairer.

La Trust Valley va reconduire le programme pilote de sensibilisation en 2023. Des guides vidéo et textuels seront aussi mis gratuitement à la disposition des PME en mars et en août.

Vous avez trouvé une erreur? Merci de nous la signaler.

1 commentaire