



ÉTUDE DE CAS

Un MSP voit les appels liés à l'hameçonnage diminuer de 20 %

Profil

- Site Web : www.tuor.ca
- Fondée : 2003
- Employés : 18
- Domaines de spécialité : cloud, support informatique, mise en œuvre, sécurité

Défi

- Les attaques par phishing et les escroqueries par social engineering devenant de plus en plus sophistiquées, Tuor devait offrir à ses clients une protection plus complète ainsi qu'une formation en matière de sécurité.

Solution



Barracuda

Email Protection™

Résultats

- Le MSP prévoit une croissance de 20 % cette année et s'attend à ce que le nombre de ses clients bénéficiant d'un plan de services gérés augmente de 70 % à 80-90 % au cours de l'année prochaine.
- Le nombre d'appels au centre d'assistance client a baissé de 20 % depuis la mise en place de la formation de sensibilisation à la sécurité gérée.
- L'utilisation d'un modèle d'abonnement est un élément crucial de la réussite du MSP.





Basé à Toronto, Tuor Networks est un fournisseur de services informatiques managés (MSP) qui dessert des clients partout au Canada. L'entreprise propose une gamme complète de solutions d'infrastructure informatique, de cloud et de services informatiques managés externalisés aux petites, moyennes et grandes entreprises de divers secteurs d'activité.

Les clients ont besoin d'aide pour se protéger contre les attaques par hameçonnage

Les clients de Tuor Networks subissaient des attaques par hameçonnage sophistiquées, un problème qui exigeait l'intervention du MSP et qui s'avérait chronophage pour les deux parties. Le MSP a pu relever ce défi en déployant un service de sécurité des e-mails offrant Barracuda Email Protection, qui comprend le chiffrement des e-mails, le filtrage anti-spam, la sauvegarde cloud et l'archivage. Cela a permis de réduire considérablement le nombre d'e-mail malveillants reçus par ses clients.

Cependant, afin de fournir une protection de sécurité des e-mails suffisamment complète pour contrecarrer les attaques de social engineering utilisant des comptes de messagerie professionnels compromis, il a dû ajouter des couches supplémentaires de sécurité. Étant donné que de nombreuses attaques sophistiquées ne présentent pas les caractéristiques des attaques traditionnelles, en raison de l'absence de fichiers ou de pièces jointes malveillants, elles peuvent être difficiles à détecter sans couches technologiques supplémentaires.

L'un des responsables financiers de notre client a reçu un email semblant provenir du PDG. Cet e-mail se présentait en ces termes : « Je vais être absent du bureau pendant un certain temps et j'ai besoin que vous transfériez immédiatement 100 000 \$ sur mon compte bancaire », explique Albert Trinh, Vice-Président Exécutif de Tuor Networks. Si la cible mord à l'hameçon, elle contourne toutes les technologies de sécurité.

L'IA et la formation en matière d'hameçonnage offrent une protection supplémentaire

Pour lutter contre ces cyberattaques plus sophistiquées, Tuor s'est à nouveau tourné vers Barracuda pour obtenir de l'aide, en ajoutant la protection de Barracuda contre l'usurpation d'identité et la fraude au nom de domaine (Impersonation and Domain Fraud Protection) à sa pile de sécurité. « Cette solution intègre l'intelligence artificielle (IA), qui peut apprendre les modèles de communication des utilisateurs et repérer les anomalies que les humains pourraient manquer », explique Albert Trinh. Contrairement à d'autres solutions de sécurité qui doivent rattraper leur retard à mesure que les menaces externes évoluent, un système basé sur l'IA comme Impersonation and Domain Fraud Protection se développera et s'adaptera aux nouvelles menaces au fur et à mesure qu'elles émergent.

Plus récemment, le MSP a ajouté une autre couche essentielle à son offre de sécurité : une formation de sensibilisation à la sécurité. « Nous utilisons la formation de sensibilisation à la sécurité gérée de Barracuda pour envoyer de faux e-mails d'hameçonnage à nos clients dans



« Nous utilisons la formation de sensibilisation à la sécurité managée de Barracuda pour envoyer de faux e-mails d'hameçonnage à nos clients dans le cadre de campagnes de sécurité permanentes. Si un client tombe dans le piège, nous en sommes immédiatement avertis et nous pouvons en profiter pour former l'employé afin qu'il soit mieux sensibilisé à l'avenir. »

le cadre de campagnes de sécurité permanentes », déclare Albert Trinh. « Si un client tombe dans le piège, nous en sommes immédiatement avertis et nous pouvons en profiter pour former l'employé afin qu'il soit mieux sensibilisé à l'avenir. »

Des avantages pour les entreprises en période de besoin

D'après les données de son outil PSA, Albert Trinh indique que l'inscription des clients au service de formation de sensibilisation à la sécurité gmanagée et leur participation à la formation permettent généralement de réduire jusqu'à 20 % les appels d'assistance liés à l'hameçonnage. « En outre, les services de Barracuda étant tous proposés sous forme d'abonnement, il s'agit d'un module facile à ajouter pour notre clientèle de PME », dit-il. « Actuellement, 70 % de nos clients bénéficient d'un programme de services gérés, et ce pourcentage devrait atteindre entre 80 % et 90 % au cours de l'année à venir. »

Le passage à un modèle commercial basé sur l'abonnement ne profite pas seulement aux clients de Tuor, mais aussi au MSP. « Sans un pourcentage aussi élevé de clients bénéficiant d'un plan de services gérés, nous aurions dû licencier du personnel au cours des premiers mois de la pandémie de coronavirus », explique-t-il. « Même si nous avons perdu des revenus avec certains clients qui ont dû fermer, d'autres clients ont prospéré et ont ajouté des services informatiques supplémentaires, ce qui a non seulement compensé les pertes, mais a conduit à une croissance prévue de 20 % pour cette année. Le fait de travailler avec des fournisseurs comme Barracuda, qui proposent les bons types de produits et tiennent compte de nos recommandations, joue un rôle essentiel dans notre réussite. »

À propos de Barracuda

Barracuda est une entreprise de cybersécurité leader sur son marché, offrant une protection complète face aux menaces complexes. Notre plateforme fournit une protection des e-mails, des données, des applications et des réseaux, avec des solutions innovantes ainsi qu'un service managé XDR. Des centaines de milliers d'organisations et de fournisseurs de services managés (MSP) du monde entier nous font confiance pour les protéger et les accompagner, avec des solutions faciles à acquérir, déployer et utiliser. Pour plus d'informations, visitez fr.barracuda.com.