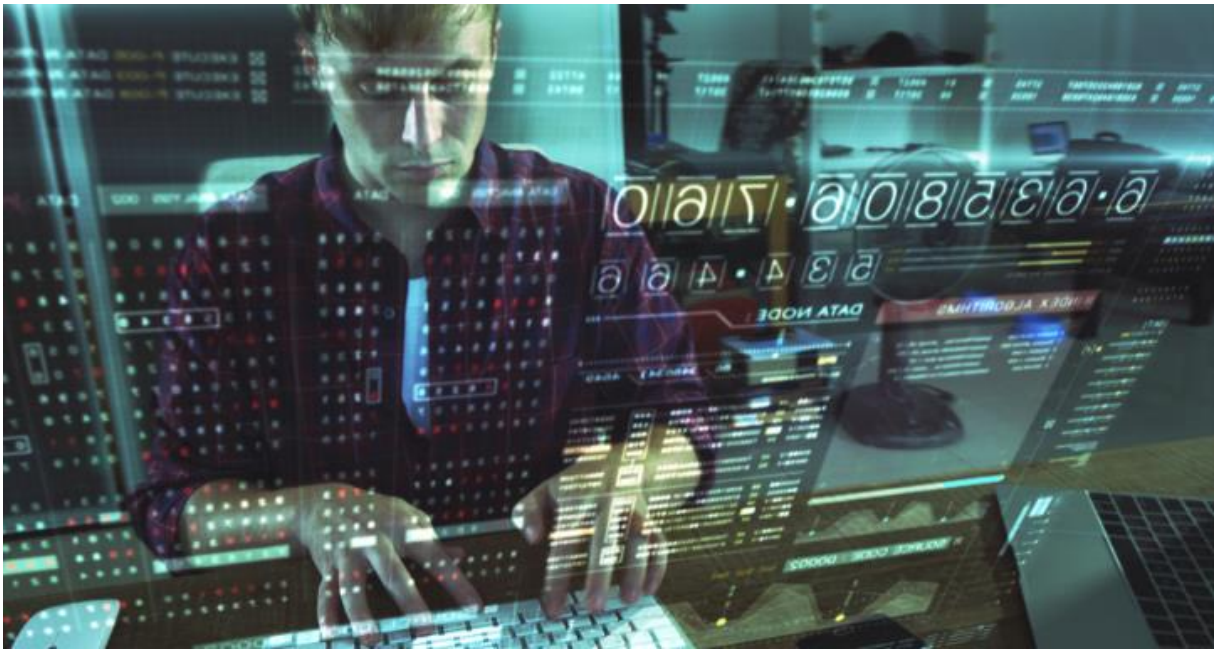
LeJournalduNet

Cyber attaques : n'oubliez pas la relation client !

Chronique de Arnaud Labyre publié le 20 octobre 2022 – Mis à jour à 08:27



Si l'été 2022 a été marqué par la hausse des températures, il a également été le théâtre d'une autre hausse impressionnante : celle des attaques informatiques et en particulier des attaques dites par ransomware ou "rançongiciels". Avec plus de 400 attaques (déclarées) de ce type en juillet et août à travers le monde, les entreprises ont dû faire face à de nombreux défis pour réparer les dégâts occasionnés et reprendre une activité normale. Mais si la réponse technologique est cruciale, il y a un autre volet qui est souvent délaissé, celui de la relation client.

Et pourtant, sans restaurer la confiance dans l'entreprise, aucune chance de récupérer pleinement d'une cyberattaque !

Restaurer la confiance, une question de survie

Les clients sont de plus en plus sensibles à l'impact d'une violation de données et à la façon dont une entreprise gère la réponse. Et le coût lié à une cyberattaque est directement lié à la capacité de l'entreprise de limiter la perte de ses clients, or il n'est de secret pour personne que la confiance est un élément fondamental du modèle économique de toute organisation prospère. Et si votre modèle est mature et que vous avez tissé des relations personnelles avec vos clients, la confiance est encore plus importante.

Alors, pourquoi les entreprises ne sont-elles pas plus nombreuses à en faire une priorité lors du processus de réponse aux incidents ? La réponse est trop souvent que les équipes

informatiques chargées de gérer un incident ne se sentent pas responsables de la promotion et de la préservation de la confiance ou de la réputation. La plupart des plans d'intervention en cas d'incident sont centrés, à juste titre, sur l'objectif de résoudre le problème et de remettre le système touché en état de marche avec le moins de perturbations possible. Mais cette approche ne tient pas compte de la nécessité de s'assurer que l'organisation continue de prospérer dans son ensemble. Il en résulte une certaine déconnexion entre les efforts fournis pour répondre à l'incident et la perception des clients sur la compétence affichée de l'entreprise. Et elle occulte un autre facteur : ce sont de plus en plus souvent les données clients qui sont impactées, données souvent sensibles qui incluent leur identité, leurs moyens de paiement, etc. Les clients sont donc personnellement impliqués et ne désirent pas apprendre l'étendue des dégâts par voie de presse.

Alors, comment maintenir les relations avec les clients pendant que vous vous efforcez d'atténuer l'impact d'un incident ? La réponse réside dans de bonnes pratiques de communication qui commencent avant même que les choses ne tournent mal.

Construisez un capital confiance en amont

Lorsqu'une importante violation de données survient, vous avez besoin de la bonne volonté de tous pour traverser la tempête. Il est toujours intéressant de voir le degré d'indulgence dont bénéficie une entreprise lorsque ses clients sont déjà prédisposés à lui faire confiance. Investissez donc le temps et les ressources nécessaires pour bâtir votre capital confiance avant d'en avoir besoin.
Cela passe par une amélioration constante et continue de votre relation client et de l'expérience client. Un client qui se sent valorisé et écouté aura plus tendance à se sentir concerné et impliqué quand vous êtes touché par une cyberattaque et à vouloir vous soutenir qu'un client qui vous considère comme une commodité remplaçable.
Mais attention, ce capital confiance est un fusil à un coup et il faudra redoubler d'effort pour le reconstituer post-incident.

Soyez multitâches

Après une cyberattaque, de nombreuses entreprises commettent l'erreur de se concentrer uniquement sur les détails techniques de la correction de l'incident, sans tenir compte de la santé et du bien-être sous-jacents de l'entreprise. N'oubliez pas que l'objectif est de continuer à soutenir la croissance de l'entreprise. Il vous faudra donc, en parallèle, rétablir la santé technique de votre entreprise mais également consacrer des ressources et de l'énergie à la maintenir à flot.
Lorsqu'un incident s'est produit, communiquez avec toutes vos parties prenantes et en particulier vos clients. Soyez transparents sur l'étendue et l'impact de l'attaque en question et sur les mesures que vous avez prise pour corriger et pour éviter qu'un tel incident puisse se produire à nouveau. Cela ne diminuera pas vos efforts sur le plan technique, mais contribuera à la résilience globale de votre organisation.

Concentrez-vous sur votre audience, pas sur l'orateur

Une bonne communication engendre la confiance. C'est un truisme qui reste vrai en cas de violation de données. Plutôt que de vous contenter de cocher les cases et d'envoyer des informations aux parties prenantes que vous êtes légalement tenu d'informer, considérez également cette situation comme une occasion de renforcer vos relations avec vos clients.

En vous concentrant sur ce que vos clients ont besoin d'entendre, plutôt que sur ce que vous voulez dire, vous pouvez transformer une communication légale insipide et sans saveur en une communication empathique donnant le sentiment que vous pensez d'abord et avant tout à vos clients. Ces derniers apprécieront la transparence et vous aurez plus de chances de préserver ces précieuses relations à long terme.

Bien sûr, comme dans toute situation de crise, tout ceci doit être anticipé. La communication vers les clients doit être régulière en amont de l'incident afin de garder une certaine fluidité dans les échanges. Et il est également important de réfléchir aux différents canaux de communication possibles car il faut prévoir que certains des canaux classiques aient pu être compromis (serveur email impacté par exemple). Tous ces éléments doivent naturellement faire partie du plan de continuité et de reprise d'activité de l'entreprise.

C'est à ce prix que l'objectif de sortie de crise sera atteint par une entreprise victime d'une cyberattaque et plus particulièrement de violations de données qui touchent directement les clients concernés. Penser que la relation client arrivera en deuxième rideau après avoir répondu à l'urgence technique est une erreur qui a coûté très cher aux entreprises l'ayant commise. Il faut considérer l'incident dans sa globalité et garder à l'esprit que sans confiance client, il n'y a pas de relations commerciales durables.

Arnaud Labyre, Responsable de la sécurité des systèmes informatiques chez **Eloquant**