Les banques confient leurs donneés sensibles à CPP Group, qui les protège grâce à l'aide de Forcepoint

CPP Group Plc est une entreprise mondiale de produits et de services spécialisée dans le secteur des services financiers et des assurances. Elle s'appuie sur Forcepoint pour la prévention des pertes de données, tout en relevant le double défi de répondre aux nouvelles exigences de mise en conformité sur les marchés mondiaux et de passer au cloud.

CPP Group a beaucoup de données à protéger – aussi bien les données de ses clients directs générées par ses activités d'assistance commerciale que les données ultra-sensibles que les banques et les sociétés de cartes de crédit lui confient pour les protéger dans le cadre de ses services de protection des cartes et de prévention de la fraude. L'entreprise a besoin d'un cadre de protection des données flexible, capable de sauvegarder des données décentralisées et distribuées dans le cloud dans plusieurs pays.

PROFIL CLIENT :
CPP développe et fournit des produits d'assurance et de protection du crédit destinés aux consommateurs.

SECTEUR :
Services financiers

PAYS D'ORIGINE :
Royaume-Uni

PRODUIT(S) :
› Forcepoint Web Security Cloud
› Forcepoint Data Loss Prevention

Fondée au Royaume-Uni en 1980, CPP Group Plc réalise aujourd'hui environ 65 % de son chiffre d'affaires en Inde, principalement grâce à ses activités de protection des cartes de paiement, d'extension de garantie et d'assurance de téléphones portables. Le recentrage géographique de ses activités commerciales pose de nouveaux défis à l'équipe de sécurité informatique de CPP.

Les services de protection des cartes et d'assurance de téléphones de CPP sont particulièrement sensibles aux risques de sécurité. Ces activités consistent à protéger les informations financières sensibles des personnes pour le compte des émetteurs de cartes de paiement tiers, comme les banques et les sociétés de cartes de crédit. En tant qu'entreprise basée au Royaume-Uni, CPP doit se conformer au règlement général de l'Union européenne sur la protection des données (RGPD) lors du traitement de ces données. Mais l'entreprise doit également se conformer à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), aux directives ISO 27001 et aux normes nationales de protection des données dans les différents pays où elle opère.

Par exemple, l'Inde a récemment promulgué des lois qui exigent que les données financières, comme les informations de transactions figurant sur les cartes de paiement, soient stockées localement par les sociétés de services financiers opérant sur son territoire. D'autres pays dans lesquels CPP poursuit ses activités, notamment la Turquie, sont en train de créer des règles similaires pour protéger les données financières.

Relever les défis posés par les nouvelles règles gouvernant la résidence des données en Inde

« Cela a mis la pression sur CPP pour sécuriser ces données localement, tout en permettant leur transfert sécurisé en cas de besoin entre son siège britannique et d'autres bureaux internationaux, » explique Patrick Viner, directeur des opérations informatiques de CPP.

Jusqu'à tout récemment, l'entreprise conservait l'ensemble des données de cartes dans son centre de données britannique, et toutes ses bases de données étaient soumises à son système de politiques britannique. Mais aujourd'hui, ces données doivent être sécurisées dans un environnement Amazon Web Services (AWS), ainsi qu'au niveau local au Royaume-Uni, en Inde et dans d'autres endroits du monde, bien que les politiques régulant les bases de données soient toujours maintenues et définies au Royaume-Uni.

Le défi consiste à maintenir un flux de travail fluide tout en s'accommodant « d'une politique de sécurité des données plus complexe, à mesure que de plus en plus de pays commencent à insister sur la résidence des données à l'intérieur de leur territoire », a déclaré M. Viner. « Nous sommes en plein milieu d'un projet important, la mise au point d'une nouvelle plate-forme accueillant un modèle permettant de stocker toutes les données dans les pays où la société exploite des services de cartes de paiement. »

Transférer les normes de sécurité sur site vers le cloud

La société CPP Plc est un client de longue date de Forcepoint. Elle utilise des appareils Web Security sur site pour sécuriser son trafic web via des VPN et des proxys dans son centre de données du Royaume-Uni. Mais cette approche de l'acheminement du trafic commençait à causer des retards dans la transmission des informations et une perte de productivité, car une majeure partie des activités quotidiennes de CPP se déroulaient hors du Royaume-Uni, en particulier en Inde.

L'entreprise a voulu compenser cette perte de productivité en basculant ses opérations informatiques vers le cloud, tout en sécurisant les données, protégeant ainsi ses clients et assurant la conformité et la continuité des activités. Pour ce faire, CPP a fait équipe avec Forcepoint.

Défis

L'acheminement du trafic via le centre de données du Royaume-Uni afin de le sécuriser a commencé à causer des retards et une perte de productivité.

Pour opérer dans plusieurs pays, il fallait se conformer à de multiples normes de protection des données.

Approche

Passer à Forcepoint Web Security Cloud pour améliorer le flux de trafic tout en maintenant la sécurité.

Déployer Forcepoint Data Loss Prevention pour accroître la visibilité sur les mouvements des données et se conformer aux réglementations complexes.

« Tout d'abord, nous sommes passés à une architecture hybride, dans laquelle nous avons installé des clients de sécurité web dans quelques-uns de nos pays d'opération », a déclaré M. Viner. « Nous avons ensuite décidé de mettre hors service notre centre de données du Royaume-Uni et de passer à un environnement VPC (cloud privé virtuel). À ce stade, j'ai pris la décision de supprimer complètement les appareils physiques et de basculer entièrement dans le cloud, et c'est l'orientation que nous suivons actuellement pour toutes nos opérations. »

Forcepoint DLP met en évidence les comportements qui mettent les données en danger

Lors d'un essai de la solution DLP (Data Loss Prevention) de Forcepoint, l'équipe de sécurité de CPP a découvert qu'il était possible que des collègues et des partenaires commerciaux en Inde se livrent à des pratiques à risque, par exemple l'envoi de feuilles de calcul contenant des données clients sans supervision – ce qui signifie que ces données sensibles pourraient accidentellement ou intentionnellement aboutir dans de mauvaises mains. L'équipe de sécurité de CPP a aussi remarqué qu'aucune mesure n'empêchait l'envoi de fichiers de clients-prospects vers des sites web non sécurisés.

Forcepoint DLP a aidé CPP à mettre ces comportements potentiellement dangereux en évidence tout en évitant la perte de productivité causée par une redirection du trafic des données et par la mise en place de points de contrôle de sécurité, qui prennent beaucoup de temps et interrompent le flux de travail.

Et le mieux de tout, c'est sans doute que M. Viner a déclaré que son équipe a pu ajuster sa politique DLP en fonction de ce qu'elle apprend des utilisateurs eux-mêmes. La solide bibliothèque de politiques prêtes à l'emploi de Forcepoint DLP comprend des politiques prédéfinies conformes aux réglementations régionales et sectorielles, comme RGPD et PCI-DSS. D'autres politiques prédéfinies couramment utilisées sont conçues pour se conformer aux réglementations relatives aux informations de santé protégées (ISP), comme la loi sur la portabilité et la responsabilité des assurances maladie (HIPAA) aux États-Unis, et les réglementations financières du Comité de Bâle concernant le contrôle bancaire dans l'UE.

> « Avec l'aide de Forcepoint, nous avons trouvé le juste équilibre entre sécurité et productivité. »
>
> **PATRICK VINER,** RESPONSABLE DES OPÉRATIONS INFORMATIQUES, CPP GROUP

Grâce à la mise en place de politiques DLP appropriées, CPP a pu procéder à quelques ajustements mineurs pour réduire les faux positifs et satisfaire à toutes les exigences de conformité, le tout sans nuire à la productivité des employés, a déclaré M. Viner.

« Vous pouvez configurer la politique quand elle est trop restrictive, et quand les utilisateurs ne peuvent pas être aussi productifs. Mais si vous laissez trop de liberté sans pouvoir surveiller et alerter, vous vous exposez à des risques de sécurité, » a-t-il déclaré. « Avec l'aide de Forcepoint, nous avons trouvé le juste équilibre entre sécurité et productivité. »

Résultats

Identifier et stopper la circulation à risque des données tout en trouvant le juste équilibre entre sécurité et productivité.