Danske Bank investit dans des logiciels vidéos pour détecter la fraude et combattre le blanchiment d'argent

Depuis que Danske Bank, basée à Copenhague, a commencé à utiliser les systèmes de vidéosurveillance March Networks® en 2007, les risques auxquels le secteur bancaire est confronté ont considérablement changé. ➤

ETUDE DE CAS : DANSKE BANK

EN 2012, selon Thomas Johansen, directeur de la sécurité physique et du groupe risque de la banque, Danske Bank a enregistré 36 attaques rien qu'au Danemark. En 2018, alors que les consommateurs effectuaient davantage de transactions bancaires en ligne et que le nombre de succursales diminuait, seuls trois attaques de banque ont été enregistrés. Cependant, pendant la même période, la criminalité liée aux guichets automatiques a considérablement augmenté — à tel point que, selon les sources, les pertes brutes sur les cartes de crédit émises au Danemark s'élevaient à plus de 60 millions de dollars en 2018.

Aujourd'hui, la banque utilise son système de vidéosurveillance autant pour lutter contre la fraude et le blanchiment que pour la sécurité physique, selon Johansen. Le logiciel March Networks Searchlight™ for Banking, en particulier, est devenu un outil essentiel pour la protection des actifs de la banque.

Le logiciel Searchlight, qui intègre la vidéosurveillance aux données de transaction des guichets automatiques de Danske Bank, alerte les enquêteurs des fraudes sur les transactions concernant des retraits juste en dessous de la limite journalière, et sur les retraits importants sur les comptes nouvellement activés. Les rapports quotidiens listent les numéros de carte bancaire, que les enquêteurs des fraudes peuvent utiliser pour identifier les cartes perdues ou volées.

Environ 500 employés de Danske Bank ont accès aux vidéos en direct et enregistrées de March Networks. Ce sont notamment les employés des agences, les services de lutte contre la fraude et le blanchiment d'argent, le personnel gérant les guichets automatiques, les agents de sécurité, le personnel de santé et de prévention des risques et les réceptionnistes.

Les rapports permettent également aux enquêteurs de se connecter facilement aux vidéos enregistrées pour voir la personne effectuant la transaction. Par exemple, si le propriétaire de la carte est une femme, mais si c'est un homme qui utilise la carte dans la séquence vidéo, c'est une indication supplémentaire que la transaction pourrait être frauduleuse. Les enquêteurs peuvent ensuite suspendre le compte, contacter le propriétaire de la carte bancaire et utiliser les preuves vidéo enregistrées pour construire leur dossier. ➤

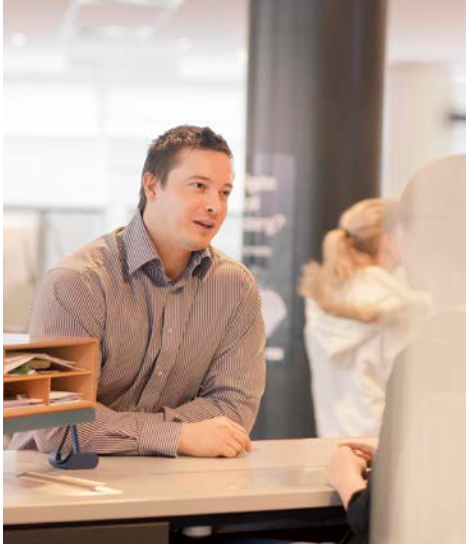
Le logiciel Searchlight alerte les enquêteurs des fraudes de Danske Bank sur les transactions concernant des retraits juste en dessous de la limite journalière, et des retraits importants sur les comptes nouvellement activés.

Au total, plus de 50 opérateurs de Danske Bank utilisent quotidiennement le logiciel pour détecter et décourager les activités frauduleuses. Danske Bank prévoit également d'utiliser ultérieurement Searchlight pour détecter les cas de blanchiment d'argent, en configurant le logiciel pour signaler les transactions indiquant une activité suspecte, telles que les dépôts et transferts de grande valeur multiples.

Dans la région nordique, Danske Bank exploite 102 succursales de banque de détail au Danemark, 32 en Norvège et 35 en Suède. Rien qu'au Danemark, elle exploite environ 500 guichets automatiques. Globalement, la banque enregistre les vidéos d'environ 4 000 caméras et compte plus de 500 enregistreurs vidéo March Networks, dont les 8732 NVR hybrides dans ses succursales et sièges sociaux, et les 8804 ou 8508 NVR hybrides dans ses guichets automatiques.

En outre, Danske Bank est présente à Kuala Lumpur, en Allemagne, en Pologne, en Lettonie, en Lituanie, en Inde et au Royaume-Uni, où elle fournit des services bancaires aux sociétés nordiques, ou possède des centres technologiques et des opérations de services administratifs, qui sont également équipés en systèmes de vidéosurveillance March Networks.

Johansen estime qu'environ 500 employés de Danske Bank ont accès aux vidéos en direct et enregistrées de March Networks. Ce sont notamment les employés des agences, les services de lutte contre la fraude et le blanchiment d'argent, le personnel gérant les guichets automatiques, les agents de sécurité, le personnel de santé et de prévention des risques et les réceptionnistes. Même les employés de cuisine et les serveurs utilisent le système pour surveiller les salles de réunion du siège de la banque à Copenhague, afin de savoir quand servir le prochain plat et gérer les réunions suivantes. ➤



Pour permettre cet accès étendu à la vidéo, les administrateurs système utilisent le logiciel March Networks Command ™ Enterprise pour limiter l'accès aux caméras en fonction de la mission ou du service de chaque employé. Cela garantit que chaque utilisateur ne voit que la vidéo dont il a besoin pour faire son travail, et répond aux exigences essentielles en matière de sécurité et de Réglement Général sur la Protection des Données (RGPD) pour la banque.

Alors que la vidéosurveillance se multiplie dans les villes, les services de police utilisent de plus en plus la vaste collection de vidéos archivées enregistrées par les banques, les commerces, les écoles et autres organisations. Pas d'exception, Danske Bank doit régulièrement transmettre des vidéos pour les enquêtes de police sur les vols et autres crimes, selon Johansen.

Lors d'une attaque terroriste près d'une succursale de la Danske Bank en 2015, par exemple, Johansen a été personnellement impliqué dans la transmission de séquences vidéo à la police.

«Heureusement, dans la plupart des cas, je peux trouver la vidéo nécessaire en quelques minutes et la livrer à la police dans un dossier contenant la visionneuse de Command Client. Cela nous a beaucoup aidés car il y a trois ou quatre ans, nous devions transmettre la vidéo sur CD ou clé USB, ce qui prenait beaucoup plus de temps. »

La fonctionnalité de recherche intelligente de March Networks permet aux utilisateurs de rechercher rapidement un mouvement dans une zone spécifique de la vidéo archivée en générant une liste de tous les événements enregistrés détectés dans cette zone. Les fonctionnalités de recherche additionnelles de March Networks, telles que les histogrammes de mouvement, les indicateurs vidéo et les recherches visuelles, aident également les utilisateurs à trouver les preuves vidéo précises recherchées.

Johansen est satisfait d'aider les forces de l'ordre dans leurs enquêtes, mais il espère trouver une solution permettant de réduire la charge imposée au personnel de Danske Bank en offrant à la police un accès sécurisé et limité à la vidéo de certaines caméras pendant une période donnée.

À l'heure actuelle, la société de surveillance des alarmes de Danske Bank dispose d'un accès 24h/24 et 7j/7 au système March Networks et peut récupérer la vidéo de toutes les agences à distance pour vérifier la cause de l'activation d'une alarme. Cela permet d'envoyer immédiatement la police si nécessaire, tout en évitant les fausses alarmes.

Le secteur bancaire a considérablement changé depuis 2007, lorsque Danske Bank a choisi pour la première fois March Networks comme partenaire de vidéosurveillance. La technologie de March Networks a également évolué, offrant des performances toujours meilleures ainsi que des fonctionnalités de veille stratégique basées sur la vidéo, dont les clients comme Danske Bank ont besoin pour protéger leurs actifs. ◆

Le défi

Danske Bank, une institution financière basée à Copenhague, compte plus de 200 succursales dans 10 pays. Les risques auxquels elle fait face ont considérablement évolué du fait de la forte augmentation des pertes liées à la fraude aux guichets automatiques. Il semblait évident qu'un logiciel capable de détecter les transactions suspectes et d'enregistrer des preuves vidéo claires pourrait jouer un rôle important pour aider la banque à protéger ses actifs.

La solution

Danske Bank a étendu les capacités de sa solution vidéo March Networks avec le logiciel Searchlight for Banking. Le logiciel intelligent combine les données de transaction aux guichets automatiques avec une vidéosurveillance dans des tableaux de bord de synthèse personnalisables, qui mettent en évidence les transactions suspectes pouvant indiquer un vol de carte bancaire ou du blanchiment d'argent.

Le résultat

Les enquêteurs des fraudes sont désormais alertés des transactions impliquant des dépôts suspects, des retraits juste en dessous de la limite journalière, et des retraits importants sur les comptes nouvellement activés. Ils peuvent ensuite utiliser les données et le logiciel Searchlight for Banking pour mener des enquêtes plus poussées et fournir des preuves aux services de police. La banque envisage d'étendre ses capacités Searchlight en introduisant l'analyse vidéo, ce qui aidera à détecter les cas de retrait d'argent illicite et à combattre le blanchiment d'argent.

Amérique du Nord 1 800 563 5564
Amérique du Sud ..... +5255 5259 9511
Europe ..... +39 0362 17935
Asie ..... +65 6818 0963
Australie et Nouvelle Zélande ..... +61 1300 089 419
Moyen-Orient et Afrique 971 4 399 5525

marchnetworks.com

MARCH networks