MARKET INSIGHT #4

Services de sécurité pour DAB

EN BREF

Les attaques contre les banques prennent de plus en plus souvent la forme d'attaques logiques et de cyberattaques.

De telles attaques à partir du système bancaire, nouvelle méthode d'accès illicite aux DAB, devraient se multiplier à l'avenir.

Cette nouvelle menace nécessite une solution centralisée, commune à toutes les banques. À l'avenir, le service de sécurité dédié aux DAB de SIX fera office de point central vers lequel convergeront les alertes en cas d'attaques contre des DAB et qui offrira également des consignes pour contrer ce type d'attaque.

DAB: évolution des méthodes d'attaque

Les attaques spectaculaires contre des distributeurs automatiques de billets font régulièrement les gros titres. En réalité, le nombre d'attaques physiques faisant appel à la force ont récemment diminué en Suisse, au profit de méthodes plus «rusées», les attaques dites logiques. Ainsi, alors que SIX recensait, en 2019, 43 attaques physiques en Suisse, ce chiffre avait chuté à 19 en 2020, enregistrant un recul de 56 %.

Au cours de la même période, le nombre d'attaques logiques progressait de 86 %. Il est intéressant de noter que le type d'attaque logique privilégié par les criminels a évolué. Le nombre d'attaques de skimming (clonage de carte bancaire), procédé par lequel une manipulation technique du lecteur de carte du distributeur automatique de billets permet de lire les données des cartes de crédit et bancaires, diminue, une tendance qui résulte en Suisse notamment de l'introduction par SIX du système de géoblocage. Le nombre d'attaques par boîtes noires en revanche augmente rapidement, non seulement en Suisse mais aussi à l'échelle internationale. Ces attaques consistent à implanter dans les distributeurs de billets un petit ordinateur contenant un logiciel malveillant et permettant de lancer des attaques logiques. L'Association européenne pour les transactions sécurisées (European Association for Secure Transactions, EAST) a enregistré au cours du premier semestre 2020 une augmentation de 269 % des attaques par boîtes noires.

À cela s'ajoute une autre méthode d'attaque de plus en plus fréquente: les cyberattaques ciblant les réseaux de DAB, par lesquelles les hackers accèdent aux réseaux informatiques des banques, à partir desquels ils lancent ensuite l'attaque.

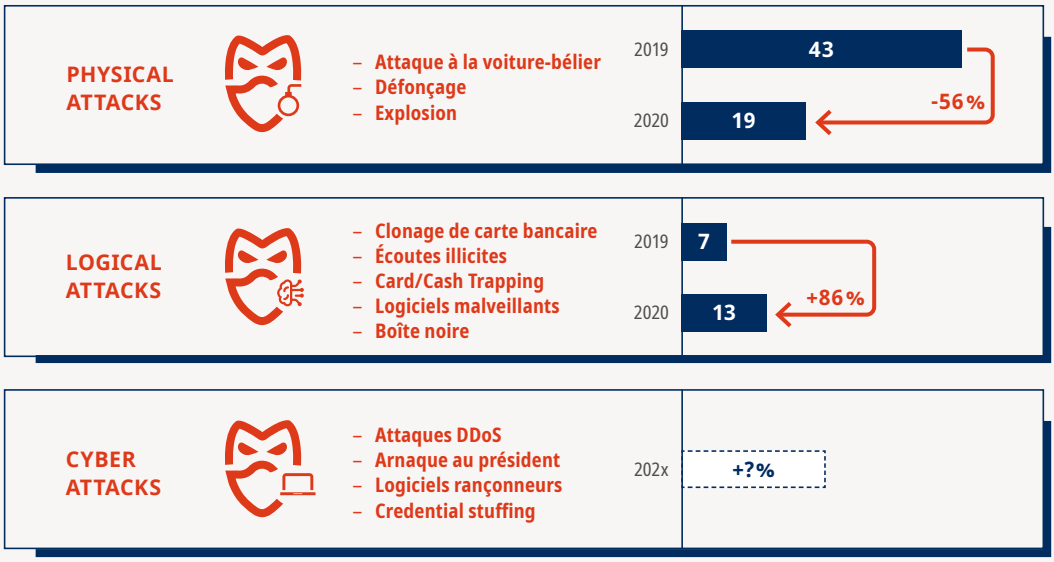

Illustration: évolution des méthodes d'attaques contre les DAB en Suisse. Source: SIX.

Le défi de la cybersécurité

La cybersécurité est un défi mondial, comme en témoigne la vague mondiale de cyberattaques qui déferle depuis mars 2020 sur les organismes gouvernementaux, les entreprises de télécommunications et les entreprises exploitant des matières premières et dans le cadre de laquelle s'inscrit l'attaque qui, en décembre 2020, a frappé les ordinateurs du ministère du commerce et des finances américain. Aucun secteur n'est aussi violemment attaqué que le secteur financier. «La cybercriminalité organisée tente de prendre en otage les établissements financiers et de prendre le contrôle de la transformation numérique», constate VMware Carbon Black, fournisseur de cloud, dans son rapport sur la sécurité «Modern Bank Heists 2020». C'est ainsi qu'au premier trimestre 2020, les cyberattaques dirigées contre les banques ont augmenté de 238 %.

Il peut paraître à première vue rassurant que le nombre de cyberattaques en Suisse demeure très faible par rapport à d'autres pays, ainsi que l'indique le Cyber Security Report 2020 publié par SIX. Il faut cependant noter à cet égard que le signalement des cyberattaques à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), qui est rattachée au Centre national pour la cybersécurité (NCSC), repose sur une base (pour l'instant) volontaire.

Il n'en reste pas moins que les cyberattaques contre les systèmes bancaires sont une menace qui doit être prise au sérieux. Une menace qui concerne de plus en plus souvent également les distributeurs automatiques de billets.

Menaces pesant à l'avenir sur les DAB

Les hackers se concentrent pour l'instant sur les attaques par deni de service distribuée (Distributed Denial of Service attack, DDoS), qui consistent à soumettre un nombre de demandes excédant les capacités de traitement, rendant le système cible indisponible et le mettant ainsi hors service. À ces attaques s'ajoutent les escroqueries telles que l'arnaque au président, le «credential stuffing» (abus systématique des données d'accès) ainsi que les logiciels rançonneurs, qui chiffrent les données et empêchent leur accès. Il est inévitable qu'avec le temps, les hackers ne se contenteront plus d'accéder aux réseaux bancaires afin d'en chiffrer ou voler les données et utiliseront ces méthodes pour organiser des attaques de grande envergure contre les réseaux DAB. Ils pourraient par exemple utiliser leurs logiciels malveillants pour déclencher des distributions de billets et récupérer l'argent sur place. Une fois mis en œuvre avec succès, ce type d'opération se répandra rapidement à l'échelle mondiale. Interconnectés au sein de réseaux internationaux, les hackers échangent en effet savoir-faire et données et joignent leurs forces pour optimiser leurs méthodes d'attaque.

Les banques suisses doivent faire face à la menace que constituent les attaques logiques et les cyberattaques. Tous les acteurs du secteur des DAB doivent agir de manière concertée dans un souci d'efficacité, afin de mettre en place des systèmes d'alerte précoce et développer des mesures de défense coordonnées.

État des lieux de la sécurité des DAB en Suisse

La situation actuelle en matière de sécurité des DAB requiert une action concertée de tous les acteurs du secteur des DAB. Tous les exploitants d'infrastructures de DAB sont confrontés aux mêmes risques et menaces. Une vue d'ensemble de toutes les attaques manque toutefois. Des dizaines de solutions sont développées en parallèle. Au lieu d'unir leurs forces, les banques surveillent simultanément les mêmes distributeurs. Les enseignements tirés des attaques perpétrées se font également de manière cloisonnée au sein des différents établissements financiers. La perte d'importance de l'argent liquide et par conséquent des DAB entraîne la disparition de précieuses connaissances sur les distributeurs automatiques de billets, les emplois vacants dans ce secteur n'étant pas renouvelés.

Il manque une communication centralisée entre les acteurs du secteur des DAB, mais aussi une infrastructure permettant de détecter rapidement et globalement les vagues d'attaques et les méthodes utilisées, de comprendre leur déroulement, d'émettre à temps des avertissements précoces et de mettre en œuvre des contre-mesures efficaces.

Made in Switzerland: le nouveau service de sécurité dédié aux DAB

Les banques suisses, en coopération avec SIX, s'intéressent depuis 2018 déjà aux tendances actuelles et à venir en matière de menaces. Des ateliers interbancaires ont été organisés et les incidents de sécurité et attaques ont été analysés. La nécessité de créer un service de sécurité centralisé dédié aux DAB fait l'unanimité. Sa mission sera:

- de fournir une vue d'ensemble complète des attaques;
- de détecter les risques de manière ciblée et d'adopter les mesures correspondantes;
- de mettre à disposition des rapports de grande qualité;
- d'offrir une plateforme centralisée fournissant des données et des informations homogènes;
- d'établir un point de convergence central pour toutes les banques suisses;
- de créer une chaîne d'information et d'alerte institutionnalisée.

Sur la base de ces considérations, SIX a commencé à mettre au point des services de sécurité dédiés aux DAB. Cette nouvelle offre de services comportera la surveillance centralisée des événements, messages et alertes relatifs aux DAB des banques participantes, l'analyse des informations relatives aux menaces qui pèsent sur les distributeurs automatiques provenant de MELANI, d'EAST et d'autres sources publiques et l'intégration des avertissements émis par les constructeurs de distributeurs automatiques de billets.

Le cadre centralisé de sécurité dédié aux DAB de SIX sera étendu et reposera sur trois piliers:

THREAT INTELLIGENCE & SECURITY ADVISORY

surveillance centralisée des notifications à l'échelle mondiale relatives aux nouvelles procédures et menaces frappant les Bancomats et envoi régulier d'informations aux banques participantes.

SECURITY & EVENT ANALYSIS

analyse centralisée des potentiels de risque pour les Bancomats en Suisse.

ALARMING & RAPID RESPONSE

alertes ponctuelles et informations continues ainsi que mise à disposition d'actions recommandées pour les banques participantes.

EN SAVOIR PLUS

SIX BBS SA
Hardturmstrasse 201
Case postale
8021 Zurich
T +41 58 399 4012
cash@six-group.com