LA CYBERSÉCURITÉ DANS LES BANQUES DE DEMAIN

SÉCURISER LE RÉSEAU DE SERVICES NUMÉRIQUES

CHRONIQUE

AURIGA
the banking e-volution

THE # NEXTGENBANK®

www.aurigaspa.com

Alors que de multiples entreprises ont été victimes de cybercriminels depuis le début de la crise sanitaire, le secteur bancaire était lui aussi particulièrement exposé, et notamment les transactions à distance que les hackers cherchent à exploiter.

Avec les services numériques qui ont été largement adoptés, assurer la sécurité bancaire est devenu un élément essentiel. Adopter de nouveaux processus pour sécuriser et assurer une protection préventive des clients sur tous les canaux est de mise.

Il est donc important de voir la banque et la cybersécurité sous leurs différents aspects. L'écosystème des DAB est particulièrement vulnérable en raison de sa complexité et du fait qu'il fonctionne souvent sur des systèmes d'exploitation obsolètes et non adaptés. Les DAB sont constitués de matériel et de logiciels hétérogènes, souvent difficiles à mettre à jour, tant du point de vue des systèmes que des coûts.

De plus, les DAB doivent rester accessibles aux clients 24/7: le temps d'indisponibilité doit être limité, créant ainsi un impact sur les tests et mises à jour. En effet, compte tenu de l'équilibre à trouver entre disponibilité et mises à jour, on a tendance à repousser ces dernières. En conséquence, les améliorations apportées aux réseaux de DAB sont parfois laissées pour compte et les banques ont du mal à obtenir une vue d'ensemble de leur vulnérabilité globale.

De ce fait, la gestion et la maintenance de ces équipements sont souvent fragmentées. En outre, les systèmes et le matériel sont légitimement accessibles à un trop grand nombre de personnes au sein du personnel, ce qui augmente le risque de cyberattaques. Des mises à jour, souvent très coûteuses à déployer, sont alors nécessaires. Et même lorsque les mises à jour proposées par les fournisseurs sont disponibles, les hackers ont souvent déjà trouvé un moyen de les contourner.

La réponse à tous ces problèmes est le déploiement des solutions sur mesure pour réduire les risques de cyberattaques.

LES CYBERATTAQUES EN HAUSSE

Avant d'appliquer une stratégie ciblée pour protéger les DAB des cybermenaces, il faut avant tout identifier les principales attaques dont les réseaux de DAB sont victimes.

Au cours de la dernière décennie, les cyberattaques logiques ont connu une progression continue, en raison des récompenses élevées et de la discrétion de l'attaque sur plusieurs DAB à la fois. On distingue différents types d'attaques logiques, qui évoluent constamment et se font de plus en plus sophistiquées.

L'attaque dite de l'homme du milieu (HDM) est une autre tendance en vogue. Il s'agit d'intercepter une opération sur un DAB. Par exemple, lorsqu'un client lance une transaction, elle est transmise à un centre d'autorisation qui vérifie s'il s'agit d'une demande valide. Les hackers essayeront d'intercepter les messages donnant l'accès à l'autorisation de l'opération pour ensuite prendre la main sur la transaction.

Une autre technique qui se développe en 2021 est l'attaque par boîte noire. Il s'agit d'une attaque physique, qui ne passe pas par un logiciel malveillant ou l'informatique, mais par un dispositif matériel externe. Connecté au distributeur, ce dispositif peut émettre des commandes générant la sortie d'espèces.

Le fait que la plupart des DAB sont facilement accessibles contribue à l'augmentation des attaques par boîte noire. C'est une technique de fraude moins coûteuse et plus simple que d'autres, telles que la duplication de cartes ou skimming. Cela dit, même les personnes malveillantes peu expérimentés peuvent facilement se procurer l'équipement nécessaire à la réalisation d'une attaque de ce type.

Si la plupart des attaques par boîte noire ciblent des DAB autres que ceux des banques, les DAB d'agences bancaires sont tout aussi vulnérables.

Une autre technique assez similaire est le jackpotting, qui consiste à utiliser un logiciel malveillant pour retirer

de l'argent au distributeur. Très facile à mettre en oeuvre, le jackpotting ne cesse de se développer depuis plusieurs années.

Les hackers déploient beaucoup d'efforts pour développer des moyens innovants d'attaquer la couche XFS. Les DAB sont le maillon faible de l'infrastructure bancaire, dans laquelle les cybercriminels peuvent s'infiltrer facilement et exploiter les données sensibles des clients, comme les numéros des cartes bancaires ou codes pin.

Là encore, c'est la vulnérabilité des systèmes obsolètes des DAB qui a contribué à l'essor mondial du jackpotting. De nombreux automates utilisent d'anciennes versions de Windows, ce qui permet d'infiltrer les couches logicielles et d'exploiter le matériel pour déclencher la distribution de billets.

LES NOUVEAUX DISPOSITIFS DE LIBRE-SERVICE CIBLÉS

Les distributeurs automatiques ne sont pas la seule cible. En effet, avec la généralisation du télétravail, les collaborateurs des banques n'ont accès à leurs systèmes qu'à distance, ce qui représente aussi des faiblesses pouvant être exploitées par les cybercriminels. Or, cela soulève de nombreuses lacunes en termes de sécurité qui nécessitent la mise en place de mesures et de meilleures pratiques relatives à la cybersécurité des ordinateurs des employés.

Par exemple, les dispositifs de libre-service assisté, appartenant à une banque et dont celle-ci assure la sécurité, seront à l'avenir l'interface avec les clients. Et pour gagner la confiance de ces derniers, les automates doivent être suffisamment sécurisés. L'aspect sécurité pourrait devenir un facteur de différenciation important par rapport à d'autres canaux, tels que les services en ligne ou mobiles, que le client est également tenu de protéger.

En termes de risques, la fraude bancaire resterait évidemment l'un des facteurs clés d'une cyber-attaque, mais une attaque ciblée constituerait une menace encore plus dommageable pour la fiabilité et la sécurité de

l'agence bancaire. Cela entraînerait une violation des données des clients, une interruption de la continuité des activités, une atteinte à la réputation de la banque et une perte de confiance des clients dans le service même.

Comme les DAB, les dispositifs de libre-service assisté sont physiquement accessibles et dépendent des communications à distance et de l'interconnexion avec l'infrastructure informatique, héritant ainsi de certains de ses risques et vulnérabilités. Il est donc nécessaire de mettre en place une stratégie de cybersécurité OT efficace. Une approche complète et robuste de la cyberprotection est indispensable, qui doit être accompagnée d'une supervision proactive de l'appareil, en termes de disponibilité du service et d'état de la sécurité, et d'un accès en temps réel pour investiguer et remédier à tout incident de sécurité potentiel.

Cette année, les banques devront s'intéresser de plus près à la cybersécurité et aux solutions y afférentes et veiller activement à ce que les données personnelles de leurs clients et leurs systèmes soient protégés.

L'IA ET LE MACHINE LEARNING AU SERVICE DE LA SÉCURITÉ BANCAIRE

L'intelligence artificielle (IA) et le machine learning (ML) jouent un rôle essentiel dans la cybersécurité. En effet, les outils de sécurité qui analysent des millions de cyberincidents se basent sur ces technologies pour identifier les menaces potentielles, telles que le compte d'un collaborateur qui clique sur un lien de phishing par exemple. Dans ce contexte, l'un des principaux avantages du machine learning vient de sa capacité de détecter et de traiter les éventuelles menaces de manière quasi immédiate, évitant ainsi tout dysfonctionnement de l'activité de la banque.

Quant à l'IA, elle permet d'automatiser certaines fonctions de protection, afin de garantir la sécurité du réseau, sans que les collaborateurs humains se voient contraints d'accomplir la tâche impossible de tout surveiller en même temps. Toutefois, bien que cette technologie présente de nombreux avantages, elle ne peut pas se substituer totalement au travail des équipes IT. Comme tout autre logiciel sur le réseau, il ne suffit pas de l'installer et de le négliger: il faut l'évaluer régulièrement car ces technologies ne sont pas là pour apporter des solutions à tous les problèmes.

DES SOLUTIONS QUI ONT FAIT LEURS PREUVES EN MATIÈRE DE SÉCURITÉ DES AUTOMATES

Lookwise Device Manager (LDM) d'Auriga permet aux banques de surveiller l'état de sécurité de leur réseau à partir d'une seule interface graphique, sans devoir gérer plusieurs solutions indépendantes.

Cette approche centralisée permet également de gérer tous les dispositifs et l'infrastructure à partir d'un seul pôle et d'exécuter des actions à distance pour déployer rapidement de nouvelles mesures de défense, telles que la segmentation du réseau et de nouveaux systèmes pare-feu.

Les différentes couches de protection requises comprennent la protection de l'intégrité des fichiers, l'établissement d'une liste blanche des applications, le cryptage intégral du disque et la protection de l'équipement. Ces mesures, appliquées séparément ou en synergie, ont un effet dissuasif sur les pirates informatiques potentiels et permettent à la banque de détecter et corriger toute faille avant qu'elle ne devienne un problème systémique plus vaste.

Rosvanna D'Amico, Product Engineer chez Auriga, explique:

> *"LDM est la solution de sécurité intégrée multifournisseur qui propose le niveau de protection le plus avancé du marché pour les dispositifs en libre-service, permettant de surveiller le système d'exploitation ou le statut XFS et les événements de sécurité pertinents."*

La solution dispose également d'un module de chargement de clé à distance (RKL) qui est intégré aux autres couches et qui fournit différents modules permettant de contrôler à les automates à distance, facilitant ainsi les opérations, les enquêtes de sécurité et la maintenance.

> *"Le gestionnaire LDM ajoute une couche de contrôle supplémentaire afin que les équipes opérationnelles puissent gérer le processus de chargement de clé à distance et exécuter des actions ciblées pour enquêter ou réagir à des attaques logiques et physiques de nouvelle génération basées sur des logiciels malveillants"*, explique Rosvanna D'Amico.

Ainsi, nous disposons d'un moyen central et efficace pour gérer la sécurité des points d'accès individuels des banques. Le gestionnaire LDM assure la prévention de tous types d'attaques en bloquant l'intrusion et les tentatives de contamination des DAB par des logiciels malveillants.

En pratique, cela signifie qu'après une tentative d'attaque, la banque peut prendre des mesures pour l'empêcher de se propager dans le réseau de DAB en fermant la zone affectée, plutôt que l'ensemble du réseau.

Assurer une sécurité optimale pour protéger chaque poste de travail d'une organisation est un devoir essentiel. Les postes de travail sécurisés sont la base des réseaux sécurisés. Il suffit qu'un seul poste de travail soit piraté pour que l'ensemble du réseau soit compromis. Toute solution de sécurité doit comporter: antivirus, sauvegardes, pare-feu, télé-maintenance et surveillance. LDM est une solution complète qui simplifie le processus de sécurité et de surveillance des postes de travail, en utilisant le concept de liste blanche pour contrôler l'accès aux ressources du système.

In fine, si les banques n'investissent pas dans les technologies appropriées, elles risquent de compromettre leur sécurité, de perdre des données clients ou leur argent. Les répercussions sur la réputation de la banque sont tout simplement trop importantes pour être envisagées. Il est temps d'agir.

AURIGA
the banking e-volution

18 rue Pasquier
75008 Paris - France
paris@aurigaspa.com
www.aurigaspa.com