LE DAB

LE MAILLON FAIBLE DE LA SÉCURITÉ DES BANQUES ?

CHRONIQUE

THE # NEXTGENBANK®

AURIGA
the banking e-volution

www.aurigaspa.com

Si les cyberattaques ciblant les entreprises ont été fortement médiatisées ces derniers mois, en raison de la recrudescence des attaques pendant la période de confinement, le secteur bancaire est lui aussi loin d'être épargné par cette menace. Alors que les cyberattaques visant les services bancaires à distance sont le plus souvent évoquées, celles visant les distributeurs automatiques de billets (DAB) sont quant à elles moins connues du grand public. Cela peut d'ailleurs paraitre surprenant au vu de leur nombre en constante accélération : l'enquête "ATMIA Global Fraud and Security Survey 2019" dévoile en effet que 58% des personnes interrogées déployant des DAB font état d'une augmentation des fraudes que ce soit par voie logicielle ou matérielle.

Riche en données personnelles (numéros de compte, codes PIN, etc.) et en argent liquide, l'infrastructure des DAB se révèle être un point d'accès privilégié des cybercriminels, mais à contrario elle reste fréquemment peu sécurisée par les banques qui investissent peu dans ce canal qu'il considère bien souvent comme un centre de coût vieillissant. Pourtant, c'est justement en raison de ce qu'il contient que les banques devraient tout mettre en oeuvre pour transformer ce dispositif critique en maillon fort de l'infrastructure de la sécurité bancaire.

DES TECHNOLOGIES DÉPASSÉES EMPÊCHANT UNE SÉCURITÉ MAXIMALE

Le malware Ploutous, utilisant la technique du jackpotting, identifié pour la première fois lors d'une cyberattaque au Mexique en 2013 est l'une des attaques les plus importantes recensées. Depuis, ce sont plus de 400 millions d'euros qui ont ainsi été dérobés. D'autres techniques, telles que le clonage de cartes sont également très répandues, notamment en raison de leur efficacité, puisqu'elles causent d'importantes pertes à de nombreuses banques dans le monde.

Les raisons qui font que les DAB sont si vulnérables sont multiples. Tout d'abord, ils traitent des informations sensibles qui se trouvent dans des environnements

souvent sans surveillance ou mal surveillés, et sans grande protection informatique. Mais surtout, les réseaux de DAB sont composés de matériels et de logiciels hétérogènes, aujourd'hui considérés comme obsolètes. Le manque de politique de mise à jour et l'utilisation de systèmes d'exploitation vieillissants rendent ces environnements d'autant plus vulnérables. Nombre d'entre eux dépendent encore du système d'exploitation Windows 7, or celui-ci n'est plus mis à jour par Microsoft, n'apportant plus de protection contre les nouvelles menaces. Et pour couronner le tout, environ 40 % des DAB dans le monde utiliseraient encore Windows XP, système d'exploitation plus ancien que Windows 7 dont le suivi n'est plus assuré depuis 2014.

Le deuxième point faible du DAB est sa couche XFS. Cette couche est l'interface standard permettant aux applications multi-constructeurs de fonctionner sur l'ensemble des automates. La couche XFS utilise des API standards pour communiquer avec les applications de libre-service ; mais en l'absence de processus d'authentification automatique, l'interface peut être rapidement piratée afin d'accéder aux composants de la machine : distributeur de billets, lecteur de carte et clavier numérique.

ADOPTER UNE SOLUTION DE SÉCURITÉ CENTRALISÉE

Il apparait clairement que les programmes génériques de protection des terminaux, conçus pour protéger des ordinateurs de bureau ou des portables personnels, ne sont pas suffisants pour sécuriser les données et l'argent présents dans un DAB. Les banques ont besoin de stratégies de sécurité ciblées pour ces dispositifs critiques, qui obéissent à des contraintes bien spécifiques.

Contrairement à des appareils mobiles, il n'est pas possible de déconnecter un DAB pendant un certain temps puis de le redémarrer. Ce sont des appareils sensibles, qui doivent être disponibles en permanence ; ils requièrent donc une

approche différente. De plus, les hackers ne cessent d'innover : ils ont mis au point de nouvelles attaques locales ciblées, qui sont moins risquées et bien plus rentables que les traditionnelles attaques matérielles. Le déploiement de solutions de sécurité efficaces permettant de protéger, surveiller et contrôler les environnements des DAB de manière adéquate est devenu une nécessité pour le monde bancaire.

Les banques doivent désormais adopter une solution de sécurité centralisée qui protège, surveille en temps réel et contrôle les réseaux et les. Cette solution doit offrir une plateforme unique grâce à laquelle les banques pourront prévenir les tentatives d'attaques de logiciels malveillants ou autres activités frauduleuses sur des distributeurs infectés. En agissant à distance, les banques peuvent exécuter des actions adéquates pour se protéger en cas de menaces via des techniques telles que le chiffrement de disque ou le blocage d'exécution de scripts non autorisés. En préventif, ce type de solution effectue également une surveillance proactive, en générant des alertes sur les fraudes possibles et en activant des actions de sécurité spécifiques en fonction de l'événement déclencheur ; vérifie l'intégrité des fichiers et des dossiers pour empêcher leur usurpation ; bloque l'accès non autorisé aux ressources des terminaux en libre-service.

Enfin, l'essor du cloud et des services dématérialisés pose un second défi aux banques en termes de cybersécurité. Si le cloud offre de nombreux bénéfices à ces institutions, tels que l'amélioration de la sécurité des données et de la fiabilité des systèmes, tout en bénéficiant d'une puissance de calcul considérablement accrue, il s'agit aussi d'investir des ressources face à des scénarios de menaces en constante évolution, dans un monde où la cybersécurité doit devenir une priorité absolue. Dans un second temps, il sera nécessaire pour les banques de garder une longueur d'avance en anticipant les nouvelles méthodes d'attaques afin que des solutions innovantes puissent être mises en place à temps pour minimiser ces risques en constante évolution.

CHRONIQUE

THE # NEXTGENBANK®

AURIGA
the banking e-volution

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