E-book consacré au secteur financier

Protéger le secteur financier contre les attaques ciblant Salesforce

Blocage d'une voie d'attaque méconnue dans le CRM de Salesforce

WITH secure

Sommaire

Introduction

Les données jouent désormais un rôle plus que central. Si une entreprise n'est pas en mesure de stocker, gérer et accéder à ses données en toute confiance, elle ne peut opérer normalement. Le secteur financier est particulièrement concerné, avec des millions de transactions quotidiennes qui soutiennent notre économie.

Le stockage cloud progresse rapidement et s'impose comme la clé d'une stratégie efficace de gestion des données. La migration des données vers le cloud présente en effet de nombreux avantages : accessibilité, convivialité et meilleure rentabilité. Grâce au cloud, les grandes entreprises peuvent accéder à leurs actifs depuis n'importe quel endroit, et synchroniser leur activité au niveau mondial. Plus récemment, le cloud a permis aux entreprises de rendre possible le travail à distance.

D'après le cabinet d'analystes Gartner, les dépenses en services de cloud public atteindront 482 milliards de dollars en 2022, et le cloud représentera plus de 45 % de toutes les dépenses informatiques professionnelles d'ici 2026.

Toutefois, les entreprises qui investissent dans le cloud doivent être conscientes que cette technologie présente aussi des risques : les infrastructures cloud constituent une cible de choix pour les cybercriminels. Selon le DBIR (Data Breach Investigation Report) de Verizon pour 2021, environ 90 % des violations de données ciblent des actifs cloud externes.

Alors que de nombreux secteurs tardent à sécuriser leur cloud, les services financiers, eux, sont à la pointe de la gestion sécurisée des données.

Le secteur financier s'est montré très tôt convaincu par la flexibilité et de l'efficacité offertes par la migration cloud. Les institutions financières se trouvent souvent à un stade avancé de leur transition cloud, et disposent de stratégies de sécurité plus avancées que les entreprises d'autres secteurs.

Les menaces et contraintes propres au secteur financier

Malgré les progrès réalisés en matière de sécurité cloud, le secteur financier reste une cible de choix pour les pirates informatiques, attirés par l'appât du gain. Depuis la naissance même du concept de finance, les banques et autres organismes financiers constituent une cible préférentielle et, aujourd'hui encore, ils sont la cible d'un assaut d'attaques quotidien.

Le secteur n'est pas seulement menacé par des groupes criminels en quête de profit : il est également ciblé par des acteurs étatiques cherchant à frapper en plein cœur d'autres économies, et à perturber des infrastructures financières tout entières. Et ce n'est pas tout : les entités financières doivent aussi faire face aux attaques internes menées par des employés malveillants, qui tentent d'accéder à des comptes clients ou de commettre des délits d'initiés.

Les entreprises financières sont tenues de satisfaire aux exigences de confidentialité et de protection des données parmi les plus strictes de tous les secteurs. Elles doivent se plier à des contrôles réglementaires spécifiques tels que la norme PCI DSS (sécurité des données des cartes de paiement) et à des règlements plus généraux comme le RGPD (Règlement Général sur la Protection des Données de l'Union Européenne) qui s'applique à toutes les entreprises traitant les données personnelles de citoyens de l'UE.

Les réglementations financières continuent d'évoluer en fonction des nouvelles technologies et des nouvelles menaces. Les services financiers sont donc contraints d'être particulièrement attentifs à leur propre sécurité. Ils sont confrontés à un véritable exercice d'équilibriste, dans lequel la sécurité ne peut se faire au détriment de l'efficacité du cloud, et inversement.

Le rôle essentiel de Salesforce pour le secteur financier

Salesforce s'est imposé comme l'un des outils incontournables dans les stratégies cloud de nombreuses organisations. Plus de 150 000 entreprises s'appuient sur cette plateforme de données cloud pour s'engager auprès de leurs clients. Grâce à sa fonctionnalité d'intégration omni-canal et à son adaptabilité, Salesforce peut répondre à un très large éventail de besoins stratégiques.

Cette plateforme est particulièrement omniprésente dans le secteur financier. La majorité des grandes banques mondiales, ainsi que de nombreux autres organismes financiers de toutes tailles et missions, en dépendent actuellement.

Les sociétés de gestion de patrimoine, quant à elles, utilisent Salesforce pour capturer l'ensemble des données concernant un client et élaborer des plans financiers sur mesure en fonction de sa situation et de ses besoins.

Avec Salesforce, les clients peuvent eux-mêmes télécharger des fichiers rapidement et facilement : les entreprises peuvent ainsi gérer plus efficacement la relation client. Par exemple, les compagnies d'assurance utilisent Salesforce pour permettre aux clients de télécharger des documents sensibles permettant de vérifier leur identité ou de lancer une réclamation. Une telle fonctionnalité est désormais essentielle : elle crée un processus beaucoup plus efficace que les anciennes méthodes par envoi postal.

Cependant, cette fonctionnalité est de plus en plus utilisée de manière abusive par les pirates informatiques. Salesforce permet à des tiers, tels que des partenaires et des clients, d'uploader des documents directement sur la plateforme, mais Salesforce lui-même ne dispose pas de fonctionnalité native permettant d'analyser ces fichiers à la recherche de menaces potentielles. À moins que l'entreprise n'ait mis en place une sécurité adéquate, les cybercriminels peuvent utiliser Salesforce pour transmettre des fichiers malveillants directement dans l'infrastructure cloud de l'entreprise.

Comment la plateforme Salesforce peut-elle être exploitée par les pirates informatiques ?

Sans mesure de sécurité supplémentaire, les fonctionnalités de partage et d'engagement de Salesforce peuvent être utilisées par des pirates informatiques pour toute une série d'activités malveillantes.

Ils peuvent, comme nous l'avons évoqué, télécharger des fichiers malveillants sur la plateforme : en opérant ainsi, ils contournent les couches de sécurité traditionnellement mises en place pour empêcher les malwares d'atteindre le réseau. Les ransomwares constituent l'un des principaux dangers, car les variants les plus évolués peuvent commencer à se propager quelques secondes seulement après leur exécution dans le réseau cible. Une telle épidémie peut rapidement paralyser l'entreprise concernée, car les données et les systèmes vitaux sont chiffrés et verrouillés. Selon les estimations, les coûts de récupération post-ransomware ont plus que doublé en 2021, pour atteindre environ 2 millions de dollars par incident en moyenne.

Outre les ransomwares, d'autres menaces sont présentes : le keylogging (enregistrement des touches du clavier), l'exfiltration de données, et la création de portes dérobées pour les serveurs de commande et de contrôle. Les hackers les plus aguerris peuvent aussi utiliser des malwares 0-day.

L'utilisateur peut, par exemple, télécharger un document malveillant sans le savoir, ou bien son compte peut avoir été corrompu. Par exemple, un PDF contenant un scan de passeport à des fins de vérification peut avoir été secrètement infecté par un code malveillant.

Les outils de communication (portails web communautaires, outil Chatter) peuvent également être exploités dans le cadre d'attaques de phishing : les pirates informatiques y publient des liens malveillants qui, autrement, seraient interceptés par les passerelles de messagerie sécurisées.

Les plateformes de type Salesforce sont aussi, de plus en plus, visées par des attaques de la supply chain. Les fonctions de partage de fichiers avec des systèmes externes permettent à plusieurs organisations de collaborer plus facilement, mais ces fonctions fournissent aux hackers des raccourcis, pour passer d'un réseau professionnel à un autre.

Sur le même principe, les cybercriminels peuvent utiliser Salesforce pour cibler les clients d'une entreprise. Les utilisateurs peuvent involontairement cliquer sur des liens malveillants ou sur des fichiers infectés via les fonctions de chat, permettant ainsi aux pirates informatiques d'infecter leurs appareils ou d'obtenir leurs identifiants. Il peut s'agir d'attaques d'initiés malveillants ou de comptes professionnels piratés. Quel qu'en soit son origine, ce genre d'incident porte toujours gravement atteinte à l'organisation qui en est victime.

Ces vecteurs d'attaque concernent toutes les plateformes cloud offrant des niveaux similaires de partage de documents et de communication. Toutefois, la quasi-omniprésence de Salesforce en fait l'une des cibles préférées des hackers.

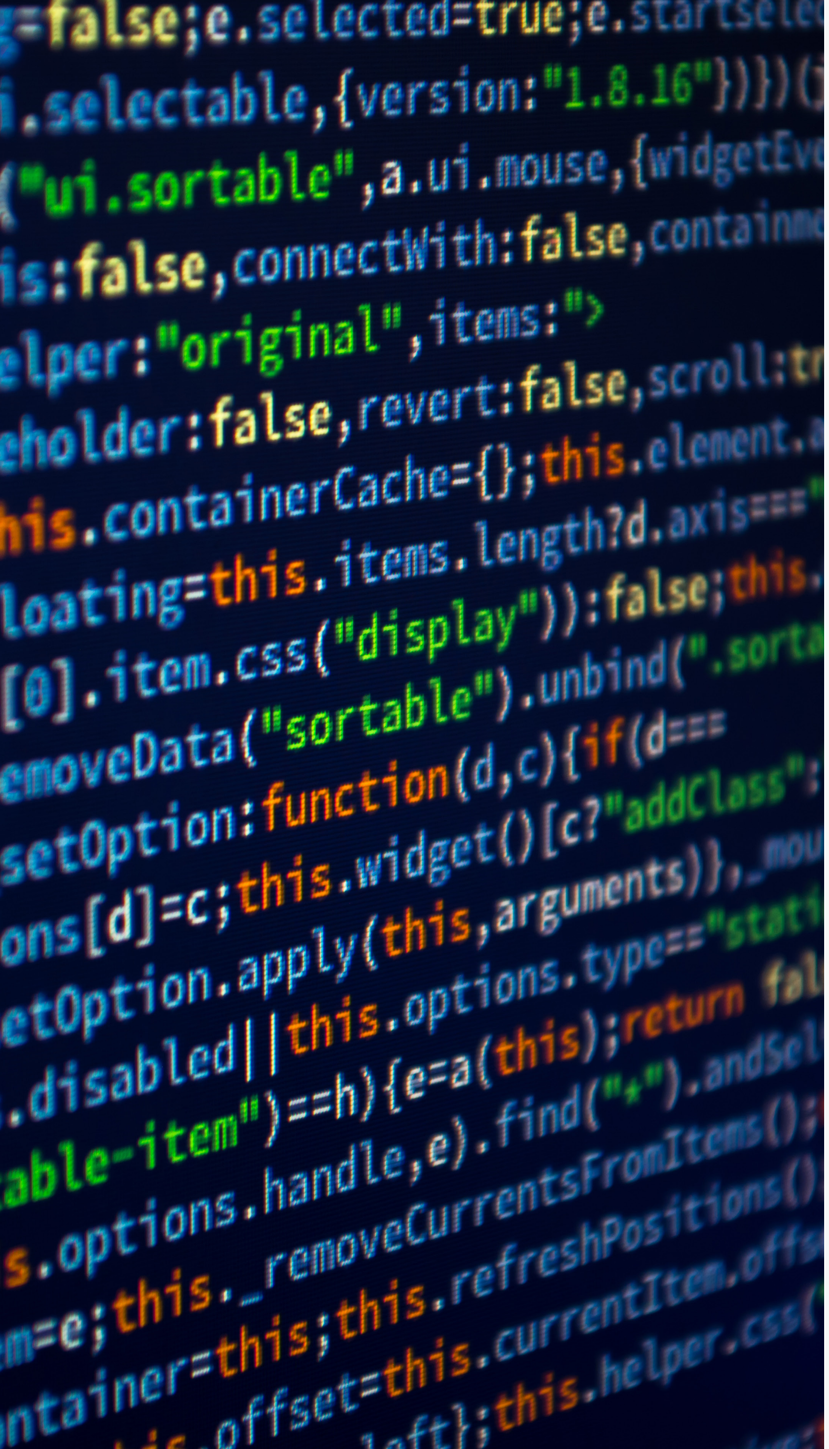
Salesforce n'en demeure pas moins un atout essentiel en matière de stratégie numérique pour les entreprises. Comment les organisations financières peuvent-elles, dès lors, minimiser les risques ?

L'étude de cas suivante avec BEC Financial Technologies montre comment WithSecure peut contrer ce type de menaces.

Étude de cas : WithSecure Cloud Protection for Salesforce protège les données des clients dans le cloud.

Avec environ 1 500 employés, BEC Financial Technologies, basé à Roskilde, fournit des solutions informatiques à des banques danoises telles que Nykredit, Arbejdernes Landsbank et Spar Nord. Les solutions informatiques de BEC permettent de gérer 2,1 millions de clients bancaires actifs et 6,3 millions de comptes bancaires actifs, pour plus de 25 banques. La cybersécurité joue donc là un rôle essentiel.

WITH secure



Sécuriser le cloud

BEC et les institutions financières de BEC ont implémenté la plateforme Salesforce afin de permettre aux banques de renforcer leur relation avec leurs clients.

La plateforme traite de grandes quantités de données, notamment des informations sensibles sur les finances personnelles des clients. Ces données transitent entre les banques et leurs clients. Il est donc crucial pour BEC de protéger ces données tout en les préservant de tout code malveillant.

Beaucoup d'utilisateurs pensent que Salesforce prend en charge toute la sécurité des données. Certains aspects de la sécurité restent pourtant du ressort des entreprises qui l'utilisent. C'est le cas, notamment, lorsque les fichiers sont téléchargés. Il nous appartient de scanner tout ce qui entre et sort du système, explique Tonny Rabjerg, Program Director chez BEC.

Implémentation simple et rapide

BEC a examiné trois fournisseurs de solutions de sécurité informatique avant de choisir WithSecure Cloud Protection for Salesforce.

Nous avons choisi WithSecure car c'est un fournisseur sérieux, capable de répondre à tous nos besoins de conformité. WithSecure a par ailleurs été recommandé par Salesforce, car son logiciel peut être implémenté facilement et rapidement. Il s'agit presque d'une solution prête à l'emploi », explique Tonny Rabjerg.

Notre collaboration avec WithSecure a été de qualité, tout au long du processus. Il n'est pas rare que je sois impliqué dans des projets d'implémentation lorsque des dysfonctionnements surviennent, mais cette fois-ci, tout s'est déroulé sans accroc, ajoute-t-il.

WithSecure Cloud Protection for Salesforce analyse tous les e-mails et documents reçus et envoyés, en temps réel, par exemple, lorsqu'un conseiller bancaire envoie un contrat à un client. Le logiciel analyse les données en temps réel. Pour autant, Tonny Rabjerg n'a observé aucun ralentissement ou perte d'efficacité.

Les conseillers bancaires ne remarquent pas l'exécution de l'analyse avancée pendant leur travail. Notre sécurité informatique ne constitue pas une source de problèmes et c'est un véritable atout., dit-il.

Une sécurité informatique évolutive

La solution de sécurité de Salesforce ne nécessite pas de mises à jour majeures, comme cela était le cas des solutions non-cloud. Pour BEC, il s'agit d'un immense progrès.

Avec WithSecure Cloud Protection for Salesforce, le système est automatiquement mis à jour sans affecter les opérations, et sans que BEC n'ait aucune action manuelle à effectuer.

Présentation du modèle de responsabilité partagée

Cette étude de cas illustre le modèle de responsabilité partagée, un cadre de sécurisation du cloud défini par plusieurs grands acteurs du secteur, comme Amazon et Microsoft.

Les fournisseurs de services cloud sont responsables de la protection des données qu'ils stockent et gèrent, comme le soulignent des règlements comme le RGPD. Pour autant, les entreprises qui utilisent ces services cloud pour stocker des données critiques ont également un rôle à jouer.

L'entreprise qui utilise une plateforme cloud est responsable de l'intégrité et de la sécurité de tous les contenus qui y résident. L'organisation qui utilise des services cloud SaaS tels que Salesforce, Microsoft 365 et Google Workspace doit s'assurer qu'elle est en capacité de sécuriser tous les actifs transférés vers le cloud. Dans le cas d'entreprises en contact avec la clientèle, tous les contenus téléchargés par des clients sont également concernés.

Les organisations du secteur financier ne sont toujours pas conscientes des risques associés à l'entrée de contenus malveillants sur les plateformes CRM cloud. Elles ne connaissent pas non plus systématiquement leur responsabilité dans la minimisation de cette menace. Même les grandes organisations financières dotées de stratégies de sécurité bien établies sont vulnérables face aux attaques qui exploitent leur CRM pour contourner d'autres couches de sécurité.

Cette étude de cas démontre comment le concept de responsabilité partagée permet d'assurer la protection de toutes les parties, sans impacter les opérations commerciales.

WithSecure Cloud Protection for Salesforce est le seul outil de sécurisation des contenus conçu en coopération avec Salesforce : il permet aux organisations de supprimer cette voie d'attaque, pour minimiser les risques et ne conserver que les atouts du cloud.

À Propos de WithSecure™

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnement cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H
secure