proofpoint.

Gestion des menaces internes dans le secteur des services financiers

Protégez vos données sensibles et votre réputation

proofpoint.com/fr

Introduction

Les sociétés de services financiers sont généralement parmi les premières à adopter de nouveaux outils de cybersécurité. Malgré cet investissement, le secteur essuie à lui seul près d'un quart des compromissions de sécurité, et plus de la moitié de ces incidents sont imputables à des utilisateurs internes.

Dans le cadre de leurs fonctions, les travailleurs de ce secteur stratégique ont non seulement accès à des flux monétaires numériques, mais aussi à des données clients sensibles. Cela fait d'eux des facteurs de risque inhérents à l'entreprise et des cibles très lucratives pour les cybercriminels.

Si certains de ces collaborateurs sont foncièrement malintentionnés, la plupart sont tout simplement négligents. D'autres encore sont victimes de pirates externes qui exploitent leurs vulnérabilités pour accéder à des données, systèmes et ressources sensibles. Rien d'étonnant dès lors à ce que les menaces internes soient si difficiles à endiguer.

Cet ebook se penche sur la gestion des menaces internes dans le secteur des services financiers. S'appuyant sur des cas concrets dans les domaines des assurances, des banques et de la gestion du patrimoine, il passe en revue les difficultés que pose la prise en charge de ces menaces. Vous découvrirez également comment Proofpoint peut vous aider à identifier, analyser et corriger ces incidents d'origine interne, et ce de manière rapide et efficace.

24 % des compromissions de sécurité touchent des institutions financières. Et plus de la moitié des attaques ciblant ces établissements émanent d'utilisateurs internes[1].

[1] Data Breach Investigations Report 2017 (Rapport d'enquête 2017 sur les compromissions de données), Verizon.

SECTION 1

Les menaces internes dans le secteur dynamique actuel des services financiers

Depuis 2018, les menaces internes touchant le secteur des services financiers ont augmenté de 20,3 %[2].

S'il est obligatoire pour toute entreprise de protéger ses informations confidentielles (données clients, données métier ou encore éléments de propriété intellectuelle), l'enjeu est d'autant plus crucial pour les banques, les établissements de crédit, les sociétés de gestion d'investissements et les compagnies d'assurances.

À l'instar d'autres secteurs, celui de la finance doit faire face à la dispersion croissante des effectifs et à la multiplication des applications cloud, des tendances convergentes qui rendent la gestion des menaces internes encore plus ardue.

Qui plus est, les entreprises partagent aujourd'hui leur infrastructure informatique avec un grand nombre d'utilisateurs, des sous-traitants aux collaborateurs distants, en passant par les partenaires et les prestataires de services. Définir ce qu'est un « utilisateur interne » n'est dès lors pas si simple.

Et malheureusement, définir ce qu'est une « menace » n'est pas beaucoup plus évident. Gérer les menaces internes ne se limite donc pas à éliminer les utilisateurs malintentionnés. Il s'agit également de pouvoir identifier et gérer les menaces émanant d'utilisateurs négligents ou ayant été victimes d'une compromission.

[2] 2020 Cost of Insider Threats Global Report (Rapport 2020 sur le coût des menaces internes à l'échelle mondiale), Ponemon Institute.

SECTION 2

Les tenants et aboutissants des risques internes

Les risques internes doivent être l'une des priorités des entreprises qui utilisent les technologies numériques. C'est particulièrement vrai pour les sociétés de services financiers.

Mais par où et par quoi commencer ? La première étape de tout programme de gestion des menaces soutenu par des technologies est de bien cerner les *tenants et aboutissants* des risques internes :

- Qui sont les personnes à risque ?
- Que faut-il protéger ?

Qui sont les personnes à risque ?

Pour pouvoir gérer les risques internes, vous devez d'abord dresser la liste des utilisateurs représentant la plus grande menace. Si cette liste est différente pour chaque entreprise, quelques profils communs d'utilisateurs à risque se détachent :

Prestataires externes – Les chaînes logistiques et de services dynamiques et désagrégées sont monnaie courante dans le secteur des services financiers. Il n'est donc pas rare que les sous-traitants, les prestataires de services, les consultants et les partenaires aient accès à la même infrastructure informatique que les collaborateurs internes. Dès lors, n'importe lequel d'entre eux est potentiellement vecteur de risque.

Utilisateurs à privilèges – Certains collaborateurs doivent pouvoir accéder à des infrastructures ou des données protégées. En voici quelques exemples :

- Administrateurs informatiques
- Agents des centres d'assistance
- Associés des centres d'appels
- Administrateurs financiers

Collaborateurs à haut risque – Certains utilisateurs peuvent être considérés à haut risque par les RH pour les motifs suivants :

- Comportement
- Changement de fonction
- Problèmes de performances ou disciplinaires
- Risque de démission

Collaborateurs concernés par des fusions et acquisitions – Le secteur des services financiers est en perpétuel changement. Fusions, acquisitions et cessions font partie de la vie de tous les jours. De ce fait, la base d'utilisateurs autorisés d'une entreprise peut rapidement passer du simple au double, et inversement. Ces changements créent des tensions au sein de l'entreprise et peuvent conduire à des compromissions de données.

Collaborateurs distants – C'est un fait, la tendance mondiale est au télétravail. Or, le fait de travailler en dehors de périmètres réseau protégés augmente le risque de compromissions internes.

Les utilisateurs malintentionnés et les autres…

Le concept de « menace interne » est souvent associé à des utilisateurs malintentionnés, dont les motivations peuvent être d'ordre financier ou politique ou relever de la vengeance personnelle. Pourtant, les utilisateurs négligents ou victimes d'une usurpation d'identité (« utilisateurs compromis ») sont bien plus souvent à l'origine de compromissions internes.

Le terme « utilisateurs négligents » désigne les personnes qui agissent en marge des procédures approuvées. En dévoilant involontairement votre infrastructure et vos données, elles augmentent le risque de compromission.

Le terme « utilisateurs compromis » désigne quant à lui les personnes agissant sous l'influence de cybercriminels extérieurs à l'entreprise : certaines sont incitées, au moyen de techniques d'ingénierie sociale, à envoyer des données ; d'autres perdent tout simplement le contrôle de leur compte.

Qu'ils relèvent de l'une ou de l'autre catégorie, ces utilisateurs sont la plus grande menace interne.

Utilisateurs internes négligents

Utilisateurs internes malintentionnés

Utilisateurs internes compromis

Que faut-il protéger ?

Comme la plupart des entreprises, les sociétés de services financiers doivent pouvoir compter sur une protection optimale de leurs transactions numériques. Toutefois, cette protection dépend également de l'intégrité de l'infrastructure informatique orientée clients et collaborateurs. Voici quelques-unes de leurs principales préoccupations :

Protection des données sensibles – Les sociétés de services financiers gèrent un grand nombre de données à caractères privé, telles que des informations bancaires ou des données médicales personnelles. Compte tenu de leur valeur aux yeux des fraudeurs, ces données sont la cible de nombreuses attaques.

Conformité – Le secteur des services financiers est soumis à d'innombrables réglementations et obligations de conformité, qui dictent aux sociétés comment protéger leurs données et l'intégrité de leurs processus. Les failles de conformité et de sécurité peuvent s'avérer particulièrement coûteuses.

Fraude financière – Les sociétés de services financiers effectuent de nombreuses transactions et gèrent d'importants volumes de capitaux. Les fraudeurs piègent les collaborateurs et se servent ensuite des accès internes usurpés pour dérober de l'argent de différentes manières.

Perturbation des activités – Les sociétés de services financiers s'appuient sur des infrastructures informatiques pour gérer les services orientés clients et collaborateurs. Si un cybercriminel obtient des accès internes, il peut s'en servir pour perturber ou endommager vos systèmes. Entre perte de revenus, d'opportunités commerciales et de confiance, les répercussions de ces interruptions de service sont multiples.

Protection des informations propriétaires – Nombre de sociétés d'investissement s'appuient sur des informations propriétaires ou sur des algorithmes de trading pour assurer leur compétitivité. Le succès de leurs services dépend de leur capacité à sécuriser ces données.

Atteinte à la réputation – Les services financiers forgent leur réputation en misant sur la confiance, que ce soit des clients, des partenaires commerciaux ou des régulateurs. Lors d'une compromission de sécurité, en particulier si elle est le fait d'utilisateurs internes, cette confiance est mise à mal et la réputation est entachée.

SECTION 3

Le rôle des technologies de gestion des menaces internes

Les solutions de gestion des menaces internes (ITM) permettent aux équipes de sécurité de mieux contrôler ce vecteur de risque unique.

Alliant des fonctionnalités de prévention des fuites de données et d'analyse du comportement des utilisateurs, elles limitent les risques via trois méthodes clés :

Identification des risques liés aux utilisateurs

Les solutions ITM permettent une détection rapide des éventuelles failles de sécurité. Les outils les plus performants permettent même de faire la différence entre les faux positifs et les activités internes nécessitant un suivi. Pour ce faire, ils analysent, en contexte, les mouvements de données et les activités des utilisateurs, en particulier de ceux les plus à risque.

Protection contre les fuites de données

Qu'il s'agisse d'algorithmes exclusifs, de secrets commerciaux, d'informations personnelles ou autres, la plupart des institutions financières ont des données à protéger. Et il est impensable que ces données puissent tomber entre n'importe quelles mains. La capacité à identifier et à bloquer rapidement les fuites de données est une fonction centrale de toute solution ITM moderne.

Réponse accélérée aux incidents

Le coût d'une menace interne est fonction du délai de résolution. Les systèmes ITM modernes permettent de diviser par 10 les temps de réponse aux incidents. Ainsi, certaines tâches qui auraient habituellement pris des jours, voire des semaines, peuvent être bouclées en quelques minutes à peine. En accélérant les investigations, vous réduisez le délai moyen de résolution.

SECTION 4 – La solution Proofpoint ITM en action

Cas clients

Société internationale de courtage en assurance – Visibilité accrue sur les activités des collaborateurs dispersés

Le défi

Une société internationale de courtage en assurance souhaitait protéger les données relatives aux sinistres de ses clients.

Pour ce faire, l'équipe de sécurité en place avait besoin d'une meilleure visibilité sur les éventuelles compromissions de données d'origine interne. Bien que l'entreprise soit en mesure de contrôler ses effectifs largement dispersés au moyen d'une application cloud, l'analyse et l'interprétation des journaux d'activités générés par cette application étaient bien trop fastidieuses et chronophages. De plus, la législation de plus en plus stricte ne faisait que renforcer les préoccupations concernant la protection des données recueillies et gérées via cet application.

La solution

Pour pouvoir préserver en tout temps la confidentialité de ses données, surtout sur les endpoints distants, la société de courtage devait installer un outil de gestion des menaces internes. Elle souhaitait en outre bénéficier d'une meilleure visibilité sur les interactions des utilisateurs avec les données et sur leurs activités au niveau des endpoints. Enfin, il lui fallait une solution capable d'identifier de manière proactive les comportements à haut risque, d'envoyer des alertes de conformité et de faciliter les audits de conformité.

Le résultat

Grâce à sa solution ITM, la société bénéficie désormais des avantages suivants :

- Détection des mouvements risqués de dossiers de sinistre, que ce soit au départ d'applications et d'endpoints ou au niveau des serveurs.
- Sensibilisation des utilisateurs et signalement en temps réel des comportements non conformes aux règles.
- Mise en corrélation de preuves irréfutables et détaillées (qui a fait quoi, quand, où, pourquoi et comment) à chaque investigation d'alerte. Des captures d'écran de l'activité au niveau des endpoints fournissent des informations contextuelles sur les événements survenus avant, pendant et après un incident. Ces informations contextuelles permettent de déterminer si l'incident résulte d'une négligence, d'un acte malveillant ou d'une compromission externe.
- Sauvegarde d'une piste d'audit détaillée des activités des collaborateurs et des tiers, afin de satisfaire aux obligations de conformité financière.

Société indépendante de gestion du patrimoine – Protection des actifs et de la confiance des clients

Le défi

Les sociétés indépendantes de gestion du patrimoine sont chargées de protéger les informations sensibles et personnelles de leurs clients. Leur réussite repose sur la confiance.

Gérer des données clients privées est le quotidien de cette société. Les utilisateurs internes ne se limitent pas aux gestionnaires de fonds, aux administrateurs et aux autres collaborateurs, mais incluent également des sous-traitants tiers. Entre cybercriminalité, cyberespionnage commandité par des entreprises et des États et fraude monétaire, la société était constamment la cible de menaces.

La solution

La société avait besoin d'un système de sécurité robuste capable de la protéger contre les risques de cybercriminalité et de fraude monétaire. L'équipe de sécurité devait, quant à elle, pouvoir contrôler plus facilement les activités potentiellement dangereuses à tous les échelons de l'entreprise, tiers et utilisateurs dispersés compris.

Le résultat

Ce qu'a apporté la solution ITM :

- Simplification des règles d'utilisation acceptable et de conformité.
- Détection automatique et en temps réel des mouvements risqués de données sensibles et confidentielles.
- Rationalisation des investigations d'incidents grâce à la mise en corrélation, en temps réel, de tous les mouvements de données et de l'activité des utilisateurs. Les captures d'écran de l'activité au niveau des endpoints apportent des preuves irréfutables des actes commis.
- Sauvegarde d'une piste d'audit détaillée des activités des utilisateurs, afin de satisfaire aux obligations de conformité financière.

Banque régionale – Protection contre les menaces internes émanant des centres d'appels

Le défi

Face à la généralisation du télétravail, une banque régionale souhaitait garantir la sécurité de ses centres d'appels.

Les collaborateurs de cette institution accédaient à des données de membres du personnel à chaque appel. De son côté, l'équipe de sécurité devait pouvoir continuer à contrôler les activités internes et à intervenir en cas d'incident, même si les collaborateurs travaillaient de chez eux. La banque s'inquiétait principalement des collaborateurs à haut risque, c'est-à-dire ceux ayant accès à des données personnelles de valeur susceptibles d'être volées, exfiltrées ou altérées. Elle souhaitait également pouvoir identifier, collecter et partager des données d'investigation numérique lors de ses interventions sur incident.

La solution

L'équipe de sécurité recherchait une solution capable de détecter les comportements anormaux en temps réel. Celle-ci devait toutefois optimiser la collecte et la surveillance des données dans un contexte de télétravail, sans nuire à la productivité et à la qualité du service client.

Le résultat

La solution ITM a permis au centre d'appels d'endiguer la menace interne, notamment grâce aux mesures suivantes :

- Renforcement de la résilience des utilisateurs. La solution ITM a sensibilisé les utilisateurs à la sécurité en s'appuyant sur des cas concrets de menaces internes. Elle a également aidé la banque à clarifier ses règles en matière de données d'entreprise.
- Déploiement, au niveau des endpoints, de collecteurs légers et exécutés en mode utilisateur. Cette méthode a permis de préserver la productivité des utilisateurs en évitant de ralentir leurs terminaux.
- Détection en temps réel des mouvements de données et des comportements à risque.
- Collaboration avec les différents départements : RH, juridique, conformité et informatique. Ceux-ci se sont concertés pour définir les modalités de collecte des données relatives aux utilisateurs et aux fichiers, les besoins en matière de détection comportementale et les workflows de réponse aux incidents.
- Accélération des investigations. En plus de fournir des renseignements contextuels sur les utilisateurs, la solution ITM simplifie la collecte de preuves et facilite la collaboration entre les équipes.

Conclusions et recommandations

Proofpoint : un partenaire de confiance, des solutions ITM performantes

Tous les jours, vos équipes informatiques et de sécurité travaillent d'arrache-pied pour identifier, détecter et neutraliser les cybermenaces. La solution Proofpoint Insider Threat Management (ITM) peut leur venir en aide. En effet, elle vous protège des fuites de données, des perturbations d'activité et des autres dommages pouvant être causés, volontairement ou non, par vos collaborateurs.

Notre solution primée a déjà aidé plus de 1 200 entreprises de premier plan dans plus de 100 pays :

- Réduisez le délai moyen de détection des menaces internes susceptibles de mettre à mal vos données sensibles et confidentielles.
- Réduisez la fréquence, la gravité et le coût des compromissions grâce à un délai d'intervention plus rapide.
- Améliorez la productivité de vos équipes de sécurité en réduisant les coûts. Proofpoint vous permet en effet de rassembler différentes technologies (telles que les analyses basées sur les utilisateurs et les outils DLP pour endpoints) au sein d'une seule et même plate-forme ITM.

Voici comment nous vous aidons :

- Nous réalisons avec vous une validation de concept (PoC) pour vous aider à mieux visualiser votre programme ITM.
- Nous vous aidons à concevoir et élaborer votre programme de gestion des menaces internes. Nous fractionnons votre projet en une série de tâches faciles à gérer que nous hiérarchisons en fonction des comportements à risque. La validation de concept (PoC) vous permet de mieux visualiser votre programme ITM et nos services ITM Jump Start vous garantissent un délai de rentabilité très court.
- Enfin, nous renforçons la résilience de vos utilisateurs grâce au programme Proofpoint Security Awareness Training.

Notre objectif est identique au vôtre : protéger les ressources les plus précieuses et les personnes qui les gèrent.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

0512-002-01-01 10/21