SAFEND DPS POUR LES INSTITUTIONS FINANCIÈRES

Livre Blanc

safend
a SuperCom company

QUAND LES CHANCES SONT ÉLEVÉES, NE SOYEZ PAS UNE CIBLE

Identifiées comme le pivot de l'économie mondiale et comme le secteur du marché le plus ciblé, les institutions financières d'aujourd'hui sont confrontées aux menaces les plus technologiquement avancées sur leurs données suivant leur sensibilité, leur utilisation et leur sécurité.
Introduites pour protéger les informations sensibles, ces menaces ont engendré des réglementations et des normes strictes comme la régulation Européenne GDPR qui apporte également des exigences supplémentaires aux sociétés financières et à leur personnel.
Lorsqu'on examine les solutions de protection des données, il est essentiel de définir qui vise à savoir quoi, et aussi de comprendre l'impact qu'une attaque réussie peut avoir sur une institution financière et ses organismes associés.

Récents faits et chiffres

Les institutions financières sont une cible très recherchée par les criminels qui cherchent à obtenir des récompenses financières:

- Cabinet d'Avocats Preet Bharara New York, 2015: le plus grand vol de données sur les clients d'une institution financière américaine dans l'histoire, le vol d'informations personnelles de plus de 100 millions de personnes
- Service Canadien du renseignement de Sécurité (SCRS): La cybercriminalité coûte à l'économie mondiale environ 445 milliards de dollars par année. Les dommages causés aux activités liées au vol de propriété intellectuelle dépassent 160 milliards de dollars
- Financial Fraud Action UK (FFA Royaume-Uni): La fraude financière au premier trimestre et au deuxième trimestre 2016 a augmenté d'un quart pour s'établir à 399,5 millions de livres sterling. Les pertes résultant des cartes de paiement, des opérations à distance et des chèques ont totalisé 755 millions de livres sterling en 2015, soit une augmentation de 26% par rapport à 2014
- Agence Bloomberg News, USA: En 2015, les commerçants boursiers américains et les hackers ukrainiens ont collaboré pour générer des bénéfices illégaux de 100 millions de dollars en volant des communiqués de presse avant qu'ils ne soient publiés publiquement
- Presse City A.M, Royaume-Uni: Les fraudeurs ont frappé les Britanniques avec une escroquerie financière toutes les 15 secondes

Qu'est-ce qu'une information financière sensible?

- Les informations des clients
  - Les informations personnelles, y compris: Nom, numéro d'identification et adresse électronique
  - La situation familiale et les renseignements sur les membres de la famille
  - Les numéros bancaires, de cartes de crédit et IBAN
  - Les activités financières passées, présentes et futures
- Les informations des institutions
  - Toutes les données, y compris les fichiers, les noms d'utilisateur, les mots de passe, l'accès au cloud et à d'autres systèmes de stockage
  - Les activités passées, présentes et futuresLes informations sur le personnel
  - Les informations sur le personnel

Quelles sont les principales menaces liées aux postes clients?

- Les accès non autorisés aux données protégées et non protégées
- La fourniture innocente d'informations par manque de connaissance ou par négligence
- Les extorsions ou le transfert forcé d'informations sensibles
- La fuite accidentelle ou intentionnelle des données via les terminaux: ports et périphériques de stockage USB, enregistreurs de clés, BOYD et autres périphériques externes tels que CD, DVD et imprimantes
- L'introduction de virus, de chevaux de Troie ou de vers via des terminaux comme les clés USB, les keyloggers ou via Internet
- Le trafic et l'utilisation externe de données sensibles volées

Quelles sont les répercussions possibles ?

- Le non-respect des réglementations et normes telles que GDPR, SOX, HIPAA, PCI…
- Le contrôle malveillant des informations sensibles d'une institution, des réseaux de données et des informations sur les clients
- Le trafic, la vente et la réutilisation d'informations volées / modifiées pour gain financier criminel
- Des dommages irréparables de l'intégrité, de l'image, du cours de l'action et des finances de l'institution
- Des dommages irréparables de la chaîne d'approvisionnement d'une institution pour ses clients
- La perte irréparable de la confiance et de la fidélité de la clientèle, entraînant des pertes financières supplémentaires
- La perte de temps et d'argent pour gérer les attaques réussies
- Les amendes et les sanctions (GDPR)

L'ARGENT ATTIRE LES CONVOITISES

Offrant de grandes tentations, les institutions financières peuvent attirer les pirates, les groupes organisés et même les collaborateurs à la recherche d'argent ou d'informations ayant de la valeur.

Quels sont les défis en matière de protection des données?

Souvent en plein essor, les technologies de vol de données posent de plus en plus de défis aux fournisseurs de solutions de protection des données dans leurs efforts pour demeurer en avance. Cela comprend le respect des normes, le contrôle de l'accès aux fichiers et aux dossiers de données sensibles, le chiffrement des données et la façon dont les informations sont sauvegardées et téléchargées. Les autres exigences sont la sécurisation des dispositifs externes ainsi que la mise en place d'alertes et d'analyses en continu.

Etre à jour avec les normes telles que la régulation GDPR

- Comprendre et respecter les normes locales et internationales
- Comprendre et respecter aussi les normes dans les pays où vous faites ou voulez faire des affaires

Où les données sensibles sont-elles les plus exposées à la menace?

- Sur les postes clients tels que les ordinateurs, les ordinateurs portables et les appareils mobiles
- Sur les supports externes tels que les clés de stockage USB, les disques durs externes ou les CD/DVD
- Lors des transferts de données

Savoir où les données sensibles sont à tout moment

- Pour définir une forte politique des autorisations d'accès
- Pour empêcher les bonnes personnes de faire de mauvaises choses
- Pour empêcher les mauvaises personnes de faire de mauvaises choses

Comment éviter l'utilisation de données volées

- Définir quelles sont les informations accessibles et par qui
- Chiffrer les informations sensibles
- Chiffrer les données des ordinateurs portables et des périphériques externes de stockage

Plus de faits et de chiffres

- Vista Research: 70% des fuites de données proviennent de l'entreprise
- Forrester: 52% des grandes entreprises nord-américaines ont perdu des données confidentielles via des supports amovibles comme les clés USB
- IDC: plus de 60% de données confidentielles résident sur les postes clients
- Ponemon Institute: plus de 16 000 ordinateurs portables sont perdus chaque semaine dans les aéroports par des hommes et des femmes en transit aux Etats-Unis, en Europe et aux Emirats Arabes Unis

COMMENT SAFEND DPS PROTÈGE VOS DONNÉES

Les Dilemmes de la Protection des Données

- Trouver une solution qui fonctionne et qui ne perturbe pas les activités quotidiennes
- Trouver une solution efficace et granulaire
- Répondre aux exigences de conformité telles que le GDPR
- Surmonter les problèmes d'intégration
- Définir simplement les profils, les politiques de sécurité et les exceptions

Un fonctionnement silencieux sans perturber les activités quotidiennes

La solution Safend DPS Data Protection pour les institutions financières est basée sur les modules Protector et Encryptor qui équilibrent la productivité et la performance sans interférer avec les activités quotidiennes.
Lors de l'installation de Safend DPS sur un réseau, une analyse précise des exigences en matière de protection des données est évaluée. Cela permet de créer des stratégies et leurs exceptions, de créer des profils et d'ajouter des autorisations utilisateur / machine concernant l'utilisation des ports et des médias de stockage externes.

En tant que suite granulaire, qui surveille et contrôle les flux d'informations sur les postes clients de votre établissement, Safend DPS applique des politiques d'autorisations et d'exceptions car il protège, chiffre, inspecte et génère des rapports sur l'utilisation des ports et des périphériques.
Par exemple, Protector peut bloquer l'utilisation de tous les périphériques externes tout en autorisant la copie des fichiers Excel sur un modèle de clé USB spécifique.

Rentabilité et adaptabilité

L'intégration de Safend DPS dans le réseau de données de votre organisation contribue à réduire les coûts associés aux fuites de données via les postes clients non protégés. Safend DPS a actuellement la capacité de prendre en charge plus de 250 000 terminaux via un seul environnement.

Compréhension des exigences de conformité

Safend DPS Protector propose déjà une solution pour répondre à la norme GDPR de l'UE et, en tant que solution personnalisable, elle peut être modifiée pour s'adapter à tous les cas de figure. Safend DPS peut également répondre à d'autres exigences de conformité majeures telles que SOX, HIPAA, PCI, FISMA ou d'autres normes spécifiques.

Surmonter les problèmes d'intégration

Safend DPS est conçu pour une installation complète et peut être installé par les experts certifiés Safend ou par l'administrateur système de votre société. En fonction des besoins de la solution, l'ensemble du processus d'intégration est simple et ne prend que très peu de temps.

Les profils, les politiques et les exceptions de Safend DPS

Avant l'installation du serveur, Safend DPS peut identifier l'utilisation des connexions USB, FireWire, PCMCIA, PCI, stockage interne et WiFi dans votre établissement. L'utilisation de ces informations fournit aux administrateurs les connaissances dont ils ont besoin pour créer des politiques, des autorisations et des exceptions préventives à l'échelle de l'entreprise. Cela peut inclure le blocage de tous les périphériques externes, puis l'attribution d'exceptions à différents utilisateurs / périphériques ou que des informations spécifiques puissent uniquement être téléchargées sur un périphérique externe.

Safend DPS propose les options suivantes:

- Bloquer / permettre le transfert de données
- Bloquer le transfert de données et recueillir des informations
- Bloquer le transfert de données sans recueillir d'informations
- Permettre le transfert de données et recueillir des informations
- Permettre le transfert de données sans recueillir d'informations

Un serveur et un agent de protection des données

Construit en tant que suite de modules de protection des données, Safend DPS protège vos informations en les contrôlant, les chiffrant, les surveillant et les mettant à jour au cours de leur cycle de vie.

Les modules Safend Data Protection Suite

- Protector: contrôle des ports (physiques et sans fil) des postes clients, contrôle et chiffrement des médias de stockage
- Encryptor: chiffrement transparent des données sur les ordinateurs portables et les PC
- Auditor: détection immédiate des risques sur les ports / périphériques WiFi connectés aux postes du réseau

Protector, contrôle des points ports et des périphériques

Solution souple et intuitive, dotée de puissantes fonctionnalités de chiffrement des fichiers basées sur des règles, Protector évite les échanges de données inappropriées avec les smartphones, les appareils photo numériques ou les cartes mémoires. Protector permet la création de stratégies de sécurité hautement granulaires et personnalisables qui détectent, autorisent ou restreignent automatiquement les transferts de fichiers en fonction des autorisations de chaque utilisateur et du type, du modèle et du numéro de série des périphériques utilisés.

Encryptor, chiffrement complet des données

Solution de chiffrement complète, spécialement pour les informations financières, Encryptor bloque l'accès inapproprié ou le transfert d'informations. Comme il sécurise les données des postes clients, Encryptor avertit immédiatement l'administration de tous les incidents de fuite de données intentionnels ou non. Avec toujours une longueur d'avance sur les technologies de piratage de données existantes et nouvelles, Encryptor protège les données au repos et peut couvrir jusqu'à 250 000 postes à partir d'un seul serveur.

Auditor, détection immédiate des risques

Ayant la capacité de fonctionner sur jusqu'à 60.000 ordinateurs, Auditor fonctionne avec ou sans le serveur DPS et permet de connaitre l'utilisation des ports USB, FireWire, PCMCIA, PCI, des stockages internes et des connexions WiFi des postes connectés sur votre réseau. Auditor recherche les informations sur vos postes selon l'architecture Microsoft Active Directory, la plage IP ou le nom de l'ordinateur et peut s'intégrer simplement à Safend Protector.

SAFEND DPS, PROTÉGER VOTRE PÉRIMÈTRE FINANCIER

En comprenant les défis de sécurité et en introduisant des solutions éprouvées, Safend DPS protège les données de vos postes clients en les surveillant et les protégeant et vous informe si elles sont utilisées et par qui.
Safend DPS est très stable, s'adapte à tous les environnements et, une fois intégré à votre réseau, il s'exécute automatiquement sans interrompre les activités quotidiennes.
Conçu comme une solution robuste pour le contrôle des ports et des périphériques, équipé également d'un mécanisme anti-sabotage, Safend DPS intègre même des règles prédéfinies de mise en conformité telles que GDPR, PCI, HIPAA et SOX.
Safend est déjà utilisé comme une solution de protection des données par de grandes institutions financières qui l'ont intégrée dans leur réseau pour protéger leurs informations sensibles.