jamf

LIVRE BLANC

Guide cybersécurité

Les données des entreprises et des utilisateurs peuvent être la cible d'attaques à tout moment. Ce guide créé par Jamf, expert en gestion des produits Apple, vous explique comment protéger votre organisation des cyberattaques les plus courantes.

Pour en savoir plus sur les fonctionnalités de sécurité de Jamf Pro et bénéficier de conseils, rendez-vous sur :
www.jamf/com/security

Pourquoi la cybersécurité est-elle si importante ?

Les données des entreprises et des utilisateurs sont ciblées par des menaces dont le nombre et la sévérité ne cessent de croître ; c'est pourquoi leur sécurité devient un enjeu crucial. En matière de cybersécurité, la protection des entreprises dépend en premier lieu de la qualité des logiciels. Les failles de sécurité peuvent mettre en danger la confidentialité des utilisateurs, les données sensibles des entreprises, l'expérience utilisateur et bien d'autres éléments. Quel que soit leur type, les cyberattaques continuent à exploiter les failles tant que celles-ci n'ont pas été corrigées. Cela implique d'investir du temps et de l'argent pour corriger un problème de sécurité qui aurait pu être évité. Les services informatiques doivent mettre un point d'honneur à s'assurer que les appareils et les données de l'entreprise comme des employés sont protégés par chiffrement et conformes aux normes de sécurité et de confidentialité.

Prendre des mesures efficaces pour assurer la sécurité de l'entreprise

La vaste majorité des cyberattaques peuvent être comparées à un voleur qui vérifie si vous avez fermé la porte à clé. Un plan de sécurité simple vous aidera à réduire les risques. Suivez les conseils donnés dans ce guide pour :

- Rassurer les clients, qui sauront que votre entreprise prend des mesures pour sécuriser son infrastructure technologique et ses données contre les cyberattaques
- Attirer de nouveaux clients qui préfèrent travailler avec des entreprises prenant la cybersécurité au sérieux
- Postuler à des appels d'offres gouvernementaux nécessitant des certifications en matière de cybersécurité
- Établir une relation de confiance avec un fournisseur de services informatiques

Se protéger contre les attaques les plus courantes

Votre plan de sécurité doit vous protéger contre les menaces les plus courantes sur Internet, plus particulièrement les attaques conçues à partir d'outils communs et nécessitant des compétences basiques. Votre objectif est d'empêcher :

- le hacking, qui exploite les vulnérabilités connues des appareils connectés à Internet en s'appuyant sur des outils et des techniques simples d'accès
- le phishing, qui dupe l'utilisateur et l'incite à installer ou à exécuter une application malveillante par le biais d'un e-mail ou d'une autre méthode
- la découverte de mots de passe, qui effectue des tentatives de connexion manuelles ou automatisées pour accéder à un système depuis Internet

Profiter de l'aide de Jamf

Jamf souhaite aider toutes les entreprises, qu'elles suivent scrupuleusement ou non les bonnes pratiques en matière de sécurité. Jamf Pro et Jamf Connect sont dotés de fonctionnalités intégrées qui permettront à la plupart des entreprises, sinon toutes, d'appliquer les bonnes pratiques de sécurité.

Si vous êtes débutant en matière de sécurité avec Apple et souhaitez simplement en découvrir les bases, veuillez lire notre e-book **La sécurité des appareils Apple**.

Bonne pratiquz n°1 : le pare-feu

Assurez-vous que seuls les services réseau sûrs et essentiels puissent être accessibles depuis Internet.

Les opérations suivantes doivent être effectuées de manière régulière :

- Modifier les mots de passe et opter pour des mots de passe complexes et difficiles à deviner
- Interdire l'accès à l'interface administrative depuis Internet, à moins que celle-ci soit protégée par l'un des éléments suivants :
  - Un deuxième facteur d'authentification, par exemple un code à usage unique
  - Une liste blanche d'IP qui limite l'accès à un petit nombre d'appareils de confiance
- Bloquer par défaut les connexions entrantes non authentifiées
- Vérifier que les règles de connexions entrantes du pare-feu sont certifiées et consignées par une personne autorisée
- Supprimer ou désactiver rapidement les autorisations du pare-feu
- Utiliser un pare-feu hôte sur les appareils connectés à des réseaux non sécurisés, par exemple des réseaux Wi-Fi d'aéroports

Adopter les bonnes pratiques de l'utilisation du pare-feu avec Jamf

Nous nous occupons de tout. L'entité de sécurité et de confidentialité de Jamf Pro possède des réglages permettant d'appliquer ces bonnes pratiques dans un profil de configuration Jamf Pro, que vous pouvez envoyer vers tous les Mac gérés :

- Activer le pare-feu
- Bloquer toutes les connexions entrantes, parmi lesquelles le partage de fichiers, le partage d'écrans, le protocole «Bonjour» dans les messages et le partage de musique avec iTunes
- Contrôler les connexions entrantes avec le menu des réglages de connexion pour des apps spécifiques : pour être autorisée, l'app doit fournir son nom, son ID de paquet et ses réglages de connexion
- Activer le mode incognito : ignorer les tentatives d'accès à l'ordinateur depuis le réseau des applications de test utilisant le protocole ICMP, comme Ping
- Configurer les appareils gérés pour qu'ils se connectent automatiquement à un VPN lorsque cela est possible, pour un accès au réseau plus sécurisé

De plus, Jamf Connect propose un approvisionnement simple des utilisateurs à partir d'un service d'identité cloud intégré à un processus d'approvisionnement Apple et associé à une authentification à plusieurs facteurs.

Pour plus de détails et d'informations techniques concernant le pare-feu applicatif et sa configuration avec Jamf Pro, veuillez consulter les ressources destinées aux développeurs qui suivent :

Référence du profil de configuration de développeur Apple ; Entité de pare-feu

Base de connaissances Apple – OS X : À propos du pare-feu applicatif

Guide de l'administrateur Jamf Pro ; Profils de configuration d'ordinateur

jamf | CONNECT

Pour plus d'informations sur Jamf Connect, consultez la ressource ci-dessous :

https://www.jamf.com/fr/ressources/documentation-des-produits/jamf-connect-transformer-lapprovisionnement-et-la-gestion-des-identites/

Bonne pratique n°2 : une configuration sécurisée

Assurez-vous que seuls les services réseau sûrs et essentiels puissent être accessibles depuis Internet

Bonnes pratiques de l'utilisation des ordinateurs et appareils connectés au réseau

Nous recommandons aux entreprises de régulièrement :

- Supprimer et désactiver les comptes utilisateurs qui ne sont plus utilisés
- Remplacer les mots de passe de comptes définis par défaut ou simples à deviner
- Supprimer ou désactiver les logiciels qui ne sont plus utilisés
- Désactiver l'activation automatique des fonctionnalités qui permettent d'exécuter des fichiers sans l'accord de l'utilisateur
- Authentifier les utilisateurs avant de les autoriser à accéder à des données sensibles via Internet

Adopter les bonnes pratiques de l'utilisation des ordinateurs et appareils connectés au réseau avec Jamf

Jamf Pro peut aider les administrateurs à mettre en place ces bonnes pratiques via des profils de configuration, des règles et des scripts pour désactiver, reporter ou corriger des processus. Par exemple :

- Pour s'assurer qu'un compte utilisateur invité est désactivé de manière permanente, un administrateur Jamf peut déployer un profil de configuration avec une entité obligeant la fenêtre d'ouverture de session sur tous les appareils gérés.
- Avec les groupes intelligents, les administrateurs peuvent révoquer l'autorisation de certains types d'utilisateurs avec une entité scripté. Jamf Nation, la plus grande communauté en ligne d'administrateurs Apple et d'utilisateurs de Jamf, est remplie d'informations, d'exemples de scripts et de solutions de dépannage proposées par les utilisateurs.
- Les rapports automatisés fournissent aux administrateurs des informations sur les comptes utilisateur locaux, si nécessaire, et les réglages de l'enrôlement par l'utilisateur peuvent être configurés dans la gestion globale ou de manière rétroactive avec l'entité de comptes de gestion.
- Les administrateurs peuvent désactiver le Bluetooth et limiter des apps ou révoquer leur autorisation.
- Lors de la configuration des réglages d'enrôlement, un administrateur Jamf peut activer une fonction de mots de passe aléatoires ou d'utilisation de mots de passe complexes via l'option d'enrôlement par l'utilisateur.

Pour en savoir plus sur l'administration des mots de passe de compte avec Jamf Pro, veuillez consulter ces ressources techniques :

Guide de l'administrateur Jamf Pro ; Administrer le compte de gestion

Guide de l'administrateur Jamf Pro ; Administrer les comptes locaux

Guide de l'administrateur Jamf Pro ; Réglages de l'enrôlement par l'utilisateur

Bonnes pratiques de l'authentification par mot de passe

Cette bonne pratique vise à vous protéger contre la découverte des mots de passe en appliquant au moins l'une des méthodes suivantes :

- Verrouiller le compte après un certain nombre de tentatives
- Limiter le nombre de tentatives dans un certain laps de temps
- Imposer des exigences de longueur et de complexité du mot de passe
- Appliquer une règle de mot de passe expliquant clairement aux utilisateurs comment créer un mot de passe fiable et sécurisé

Adopter les bonnes pratiques de l'authentification par mot de passe avec Jamf

Jamf Pro offre la possibilité de définir toutes ces préférences dans un profil de configuration. Les administrateurs Jamf Pro peuvent également créer des blacklist de mots de passe regroupant les mots de passe courants et simples à deviner. Avec Jamf Connect et Jamf Pro, les utilisateurs peuvent tirer parti de l'authentification unique et de l'authentification à plusieurs facteurs pour renforcer encore la sécurité des mots de passe.

Les comptes locaux associés à NoMAD et les comptes mobiles utilisant Active Directory ont de la chance : Jamf Connect fonctionne parfaitement avec NoMAD, pour une expérience encore plus sécurisée.

Pour plus d'informations sur la compatibilité de NoMAD et Jamf Connect, veuillez consulter cette infographie explicative : **https://www.jamf.com/resources/infographics/understanding-macos-catalina-and-jamf-connect/**

Bonne pratique n°3 : le contrôle des accès utilisateur

Les entreprises doivent s'assurer que les comptes utilisateur sont exclusivement attribués à des personnes autorisées, et que les applications, ordinateurs et réseaux sont accessibles uniquement par les utilisateurs qui en ont réellement besoin.

Les entreprises doivent donc :

- Mettre en place un processus de création et de validation des comptes utilisateur
- Authentifier les utilisateurs avant de leur donner accès aux applications ou aux appareils
- Supprimer ou désactiver les comptes utilisateur lorsqu'ils ne sont plus utilisés
- Utiliser les comptes d'administration uniquement pour la réalisation d'activités administratives
- Supprimer ou désactiver les privilèges d'accès spécifiques lorsqu'ils ne sont plus nécessaires

Adopter les bonnes pratiques du contrôle des accès avec Jamf

Les restrictions des Préférences système dans les profils de configuration, les entités de restriction et la suppression de l'accès administrateur lorsqu'il n'est plus nécessaire suffiront à régler ces problèmes. De plus, une bonne gestion de l'option **Self Service** garantira qu'aucun utilisateur ne pourra accéder à des espaces ou des apps qui ne sont pas nécessaires à son travail.

Pour supprimer des utilisateurs et des comptes, les administrateurs peuvent déployer une règle simple permettant de supprimer des accès, des comptes ou des utilisateurs.

Bonne pratique n°4 : la protection contre les logiciels malveillants

Les entreprises doivent veiller à empêcher l'exécution de programmes malveillants et logiciels non approuvés, qui pourraient provoquer des dégâts ou accéder à des données sensibles.

Bonnes pratiques pour se protéger contre les logiciels malveillants

- Veiller à ce que les antivirus et autres logiciels de sécurité soient bien à jour en mettant en place un processus de vérification automatique ou manuel quotidien
- Configurer le logiciel de manière à scanner les fichiers et les pages web automatiquement, dès leur ouverture
- Configurer le logiciel pour qu'il empêche les connexions à des sites web malveillants
- Autoriser uniquement l'installation de logiciels approuvés sur les appareils
- Exécuter le code d'origine inconnue dans un sandbox pour l'empêcher d'accéder à d'autres ressources sans autorisation explicite de la part de l'utilisateur

Adopter les bonnes pratiques pour se protéger contre les logiciels malveillants avec Jamf

Les fonctionnalités de sécurité de Jamf sont natives. En déployant vos logiciels via une règle et en mettant automatiquement à jour tous vos logiciels, vous êtes assuré que vos antivirus et autres logiciels de sécurité sont toujours à jour. Si le logiciel antivirus de votre entreprise ne permet pas de scanner les fichiers à l'ouverture, vous pouvez y remédier avec un script ou une règle Jamf. Bien entendu, tous les appareils macOS sont dotés de l'application **Xprotect** par défaut.

En outre, grâce aux profils de configuration de Jamf Pro, les administrateurs peuvent paramétrer des entités de sécurité et de confidentialité via les réglages de Gatekeeper, déployer des entités de transparence des certificats, restreindre les apps disponibles à une liste blanche spécifique, etc.

En plus du sandbox intégré d'Apple, qui empêche les apps de partager leurs caractéristiques, les serveurs de Jamf Cloud disposent eux aussi de leur propre sandbox pour plus de sécurité. Enfin, les administrateurs peuvent ajouter des fonctionnalités de sécurité supplémentaires pour protéger l'entreprise contre les logiciels malveillants via un profil de configuration de contrôle des règles de confidentialité.

Bonne pratique n°5 : la gestion des correctifs

Cette bonne pratique garantit que les appareils et les logiciels ne sont pas vulnérables aux problèmes de sécurité connus ayant fait l'objet d'un correctif.

Les logiciels doivent être :

- Toujours à jour
- Sous licence et pris en charge
- Supprimés des appareils lorsque leur prise en charge n'est plus assurée
- Corrigés dans les 14 jours suivant la sortie d'une mise à jour

Adopter les bonnes pratiques de gestion des correctifs avec Jamf

Les administrateurs peuvent utiliser la fonction de gestion des correctifs de Jamf Pro pour contrôler les appareils gérés et leur appliquer les correctifs. La fonction de gestion des correctifs applique automatiquement les correctifs aux appareils gérés après que l'administrateur a importé un paquet, l'a associé à une version de correctif et a créé une règle de correctif.

Le serveur de correctifs de Jamf pourra fournir les correctifs de certains logiciels. Les clients pourront aussi choisir d'intégrer une source de correctifs externe, gérée par des tiers ou par eux-mêmes. Les informations sur les logiciels indiquent les versions d'OS prises en charge.

Les administrateurs pourront facilement désinstaller les logiciels en configurant une règle pour désinstaller ou supprimer l'appareil du dossier Mac App Store.

Conclusion

Jamf facilite la mise en œuvre et le respect des meilleures pratiques en matière de cybersécurité. Contactez-nous dès aujourd'hui pour savoir comment votre organisation peut se protéger contre les cyberattaques..

jamf

www.jamf.com

Découvrez ces fonctionnalités de sécurité par vous-même en profitant d'un **essai gratuit**.