BONNE PRATIQUE :

RUA

Règles d'utilisation acceptable

En tant que professionnel de la cybersécurité, vous vous concentrez spontanément sur les contrôles de sécurité qui protègent activement votre infrastructure et vos données tout en atténuant le risque posé par les menaces et les attaques. Mais la sécurité de votre organisation repose également sur d'autres éléments essentiels. Les règles d'utilisation acceptable (RUA) en sont un excellent exemple.

jamf

Ce que sont les RUA

Une règle d'utilisation acceptable (RUA) est un ensemble de principes définis par la direction d'une organisation. Elle détermine comment les appareils, les données, les services et les ressources doivent être traités par leurs utilisateurs. Les RUA limitent explicitement ce qui est autorisé et ce qui ne l'est pas.

Pourquoi elles sont indispensables

Les RUA sont nécessaires pour plusieurs raisons. Principalement, ces lignes directrices mises en œuvre dans tous les secteurs et dans le monde entier :

- Définissent les comportements attendus des utilisateurs finaux
- Demandent la confirmation que les utilisateurs connaissent, comprennent et acceptent les règles
- Encadrent l'utilisation du matériel, des logiciels, des réseaux et des sites web
- S'alignent sur les cadres de sécurité de l'information pour la protection des données.

Dans de nombreuses organisations, les utilisateurs doivent signer une RUA afin de réduire le risque de responsabilité juridique**. Les salariés sont informés de leurs droits et devoirs vis-à-vis des ressources de l'organisation, mais aussi des conséquences auxquelles ils s'exposent en cas de non-respect des règles.**

Découvrez :

1. Ce qu'est une règle d'utilisation acceptable
2. Leur rôle clé dans votre posture de sécurité
3. Quelles bonnes pratiques permettent d'aligner la RUA sur votre stratégie de gestion des données et de renforcer votre plan de défense en profondeur.

Bonnes pratiques de création et de mise en œuvre des RUA

1 **Évaluation.** Évaluez la situation de départ de votre organisation. Réfléchissez à la manière dont les utilisateurs doivent interagir avec les ressources ainsi qu'aux liens entre leur rôle et leurs droits d'accès. Ensuite, demandez-vous si les pratiques sont en phase avec les besoins de l'entreprise.

2 **Identification.** Il se peut que votre RUA s'applique à d'autres appareils que ceux de l'organisation. Il est important d'identifier précisément les équipements et utilisateurs concernés par votre règle. Devez-vous inclure les appareils en BYOD et ceux qui sont inscrits par les utilisateurs ? Munis de ces informations, les administrateurs informatiques peuvent mettre en place la configuration adéquate pour autoriser ou refuser l'accès au réseau sécurisé en s'appuyant sur les données de gestion d'inventaire.

3 **Alignement.** Les RUA doivent s'aligner sur un cadre de sécurité de l'information tel que les critères du Center for Information Security (CIS). Quand des contrôles administratifs se superposent à des contrôles de sécurité, les RUA deviennent bien plus qu'un document autonome. Elles sont alors un rouage d'une stratégie holistique qui vous rapproche d'une défense en profondeur reposant sur plusieurs couches de sécurité.

4 **Réutilisation.** Vous n'avez pas besoin de partir d'une page blanche. Explorez et utilisez les ressources disponibles pour élaborer une RUA adaptée aux besoins de votre organisation. Vous trouverez notamment des formulations ciblant des exigences spécifiques, ou de modèles plus larges développés par des organisations fiables et compétentes en sécurité de l'information. Pensez par exemple au répertoire de modèles de règles de sécurité du SANS Institute, ou au modèle règles d'utilisation acceptable des technologies de l'information du CIS.

5 **Mise en application.** Toute activité jugée nuisible, enfreignant les lois locales, nationales, fédérales ou régionales, ayant un impact négatif sur les autres utilisateurs ou susceptible de causer des dommages (intentionnels ou non) doit être abordée dans votre RUA. N'oubliez pas de préciser la juridiction dans laquelle elle s'applique. Cela peut alléger la charge juridique si un incident nécessite une action en justice. En identifiant spécifiquement les personnes couvertes par la RUA et la région où elle s'applique, les organisations qui opèrent dans plusieurs endroits peuvent s'adapter aux différents degrés de responsabilité juridique propres à chacun.

Nous nous tenons à votre disposition. Découvrez comment sécuriser votre lieu de travail avec Jamf Trusted Access.