



RSX112

Sécurité des réseaux

Stéphane LARCHER

A high-angle, low-key photograph showing the lower legs and feet of several people walking across a light-colored, paved surface. The scene is backlit, creating long, dark, and elongated shadows that stretch across the ground. The shadows are sharp and clearly define the shapes of the legs and feet. The overall mood is one of movement and anonymity.

Le shadow IT

Le shadow IT

Définition

« Le Shadow IT, également connu sous le nom d'informatique clandestine ou informatique de l'ombre, fait référence à l'utilisation de technologies, de logiciels, de services ou d'applications informatiques en dehors du contrôle et de la connaissance des départements informatiques officiels d'une organisation »

Le shadow IT

utilisation de solutions technologiques

non autorisées

non conformes aux politiques de
l'entreprise

pour répondre à leurs besoins

Ses formes

services de
stockage
cloud
personnels

Messagerie
instantanée

de logiciels de
collaboration
en ligne

d'applications
mobiles non
approuvées
par
l'organisation



Ses formes

bénéficier de
fonctionnalités
spécifiques

de solutions
plus conviviales

contourner les
processus
bureaucratiques



Pourquoi ?

flexibilité
accrue

productivité
accrue

Pourquoi ?

Besoins spécifiques non satisfaits

Les employés peuvent rechercher des solutions technologiques qui répondent à des besoins particuliers ou qui offrent des fonctionnalités spécifiques qui ne sont pas disponibles dans les systèmes officiels de l'organisation

Ils peuvent trouver des applications ou des services en ligne qui facilitent leur travail ou améliorent leur productivité

Complexité des processus et des politiques

Si les processus de demande d'accès aux technologies officielles sont perçus comme complexes, bureaucratiques ou lents, les employés peuvent être tentés d'utiliser des solutions non autorisées pour contourner ces obstacles et accomplir rapidement leurs tâches



Pourquoi ?

Convivialité et facilité d'utilisation

Les services ou applications non officiels peuvent offrir une interface conviviale, une expérience utilisateur intuitive ou des fonctionnalités attrayantes qui attirent les employés

Ils peuvent préférer utiliser ces solutions plus conviviales par rapport aux systèmes approuvés qui peuvent être perçus comme moins conviviaux



Pourquoi ?

Rapidité et agilité

Le Shadow IT peut être motivé par la nécessité de répondre rapidement aux demandes et aux exigences opérationnelles

Les employés peuvent utiliser des outils ou des services en ligne pour obtenir des résultats plus rapidement sans attendre les processus officiels de validation et de déploiement des technologies



Pourquoi ?

Manque de formation ou de sensibilisation

Si les employés ne sont pas pleinement informés des politiques et des procédures informatiques de l'organisation, ils peuvent recourir au Shadow IT par méconnaissance ou par manque de sensibilisation aux risques associés



Pourquoi ?

Culture de l'innovation et de l'expérimentation

Certains employés peuvent être motivés par un désir
d'explorer de nouvelles technologies

d'expérimenter des applications ou des services innovants
pour améliorer leur travail ou leur efficacité

Les conséquences

Perte de
contrôle des
données
sensibles

Violation des
politiques de
sécurité

Non-
conformité
réglementaire

Exposition
aux
cyberattaques

Inefficacité
des processus

Les bonnes pratiques

Politiques et procédures claires	Élaborez des politiques et des procédures informatiques claires qui définissent les technologies autorisées, les processus d'approbation des nouvelles solutions technologiques, les mesures de sécurité et les conséquences en cas de non-respect des politiques
Sensibilisation et formation	Sensibilisez les employés aux risques associés au Shadow IT et aux politiques en place. Organisez des sessions de formation pour expliquer les procédures, les bonnes pratiques et les alternatives sécurisées disponibles.
Communication ouverte	Favorisez un environnement de communication ouverte où les employés se sentent à l'aise pour signaler les problèmes et partager leurs besoins en matière de technologies. Encouragez la collaboration entre les départements informatiques et les utilisateurs finaux.

Les bonnes pratiques

Évaluation des besoins des employés

Identifiez les raisons qui poussent les employés à utiliser des solutions non autorisées

Évaluez les lacunes des systèmes informatiques existants et collaborez avec les employés pour identifier des solutions alternatives sécurisées et conformes à leurs besoins

Gestion des fournisseurs

Établissez des relations avec des fournisseurs de confiance et des partenaires technologiques pour répondre aux besoins spécifiques des employés

Collaborez avec les fournisseurs pour intégrer leurs solutions dans l'écosystème technologique de l'organisation de manière sécurisée et conforme

Surveillance et gestion technologique

Utilisez des outils de surveillance et de gestion technologique pour détecter et suivre l'utilisation du Shadow IT au sein de l'organisation

Identifiez les applications, services ou logiciels non autorisés et prenez des mesures appropriées pour remédier à la situation

Les bonnes pratiques

Partage des meilleures pratiques

Établissez un forum ou une plateforme où les employés peuvent partager leurs expériences et leurs meilleures pratiques en matière de technologies

Encouragez la collaboration entre les équipes pour identifier et promouvoir les solutions technologiques efficaces et sécurisées.

Évolution des politiques et des procédures

Tenez compte des évolutions technologiques et des besoins changeants des employés

Révissez régulièrement les politiques et les procédures informatiques pour les adapter aux nouveaux défis et opportunités.

Les parades

Solutions de découverte et d'inventaire

Utilisez des outils de découverte et d'inventaire des actifs informatiques pour identifier et suivre les applications, les services et les logiciels utilisés au sein de l'organisation

Ces solutions permettent de cartographier l'environnement technologique et de détecter les éléments non autorisés

Solutions de surveillance et de gestion des utilisateurs

Misez sur des outils de surveillance des utilisateurs pour détecter les activités suspectes ou non autorisées liées au Shadow IT

Ces solutions fournissent des rapports sur les comportements des utilisateurs, les applications utilisées et les violations éventuelles des politiques informatiques.

Solutions de gestion des accès

Adoptez des solutions de gestion des accès et des identités (IAM) pour gérer de manière centralisée les autorisations et les accès aux systèmes et aux applications

Ces solutions permettent de contrôler les droits d'accès des utilisateurs et de limiter l'utilisation de solutions non autorisées.

Les parades

Solutions de sécurité des données

Mettez en place des solutions de sécurité des données telles que le chiffrement, la prévention des pertes de données (DLP) et la protection des informations sensibles

Cela aidera à minimiser les risques de fuite ou de compromission des données, même en cas d'utilisation de solutions non autorisées.

Collaboration entre départements informatiques et utilisateurs finaux

Encouragez la collaboration et le dialogue entre les départements informatiques et les utilisateurs finaux

Organisez des réunions régulières pour comprendre les besoins des employés et trouver des solutions technologiques alternatives qui répondent à leurs exigences tout en respectant les politiques et les normes de sécurité de l'organisation.

Formation et sensibilisation

Offrez une formation continue sur les politiques et les procédures informatiques de l'organisation, ainsi que sur les risques associés au Shadow IT

Sensibilisez les employés aux bonnes pratiques en matière de sécurité informatique et aux alternatives approuvées disponibles pour répondre à leurs besoins.

Les parades

Gouvernance et conformité

Mettez en place un cadre de gouvernance solide pour établir des politiques claires, des processus de validation des technologies et des mécanismes de suivi de conformité

Assurez-vous que les employés comprennent les exigences de conformité réglementaire et les implications associées au non-respect des politiques.

Évaluation continue des technologies

Effectuez régulièrement des évaluations et des analyses des technologies utilisées au sein de l'organisation

Identifiez les solutions non autorisées et évaluez si elles peuvent être remplacées par des alternatives sécurisées et conformes.