SHADOW IT
LE DANGER
CACHE

@aneol

Le phénomène du shadow IT, également connu sous les termes d'informatique de l'ombre ou rogue IT, se réfère à l'utilisation non autorisée par la direction informatique de logiciels, de services et d'applications au sein d'une organisation.

@aneol

Les différentes formes de Shadow IT

Applications et logiciels non autorisés

Services de stockage en ligne non approuvés

Messagerie instantanée et communications non officielles

Matériel informatique personnel

Outils de développement non officiels

@aneol

Le Shadow IT en quelques chiffres

32%[1]

des incidents de sécurité rencontrés par une entreprise sont causés par le Shadow IT en 2021

42%[2]

des employés utilisent des comptes de messagerie non approuvés par les équipes informatiques en 2020

58%[3]

des employés ne sont pas entièrement satisfaits des outils proposés par leur entreprise

1 Source : Baromètre de la cybersécurité des entreprises, CESIN, Janvier 2022

2 Source : Online services used by employees not approved by information technology team as of 2020, Statista, April 2020

3 Source : Report Workplace trends & insights report : Building a hybrid future that works for everyone, APPSPACE | BEEZY, 2022

@aneol

Comment se manifeste le Shadow IT ?

Imaginons que vous ayez mis en place une suite logicielle spécifique pour gérer vos projets. Celle-ci doit être utilisée par l'ensemble de vos collaborateurs.

Cependant, l'un de vos salariés trouve cette solution trop compliquée à utiliser et estime qu'elle ne répond pas pleinement à ses besoins.

Il décide d'adopter une autre solution de gestion de projet qui lui semble plus simple, accessible sur le cloud et qu'il a découvert dans son cadre personnel.

@aneol

Motivations du salarié

Il est satisfait de son choix car cela lui permet d'être plus efficace et de mieux organiser ses tâches.

Cependant vous n’avez aucune visibilité sur les données traitées par cette application, sur l’endroit où elles sont stockées et sur ce que l’éditeur de ce logiciel à le droit de faire avec.

Tout cela peut poser de sérieux problème de confidentialité ou de conformité.

QUELS SONT LES RISQUES AUXQUELS CET EMPLOYÉ EXPOSE SON ENTREPRISE ?

@aneol

Des risques bien réels...

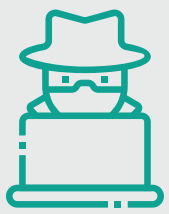
VIOLATION DES DONNÉES

Le salarié contourne les protocoles de sécurité de l'entreprise. Ainsi, les données sensibles sont vulnérables au piratage informatique.

PERTE DE PROPRIÉTÉ INTELLECTUELLE

Le salarié peut copier des fichiers sensibles et des courriels contenant des éléments de propriété intellectuelle de grande valeur grâce à un logiciel non autorisé.

RISQUES DE CYBERATTAQUES



Un échange de fichiers via un e-mail ou un logiciel installé sans approbation sur un ordinateur est un potentiel point d'ouverture pour les cyberattaques.

@aneol

Comment
mettre fin au Shadow IT ?

@aneol

1 | SENSIBILISER LES SALARIÉS

Au cours de sessions de sensibilisation régulières, présentez des exemples concrets d'incidents liés au shadow IT et expliquez les conséquences pour l'entreprise et les individus concernés.

Il est primordial de s'assurer que les nouvelles recrues reçoivent une formation sur ce sujet lors de leur intégration.

@aneol

2 | INSTAURER UNE CHARTE INFORMATIQUE CLAIRE

Elaborez une charte informatique dans laquelle sont définis les logiciels, les applications, le matériel et les services cloud approuvés que les employés peuvent utiliser.

Elle doit aussi spécifier le processus de demande et de validation de nouvelles applications ou de nouveaux services.

Cette charte doit être facilement accessible et compréhensible par les salariés.

@aneol

3 | RÉALISER DES AUDITS

Les équipes informatiques peuvent utiliser des outils de surveillance du réseau et des solutions d'inventaire logiciels pour détecter les applications ou services non autorisés au sein de l'entreprise.

Une fois la découverte faite, les services informatiques peuvent travailler avec les employés pour trouver des alternatives appropriées et approuvées.

@aneol

4 | ÉVALUER LES BESOINS DES ÉQUIPES

Incitez vos collaborateurs à s'exprimer librement sur les difficultés qu'ils rencontrent avec les outils informatiques officiellement approuvés en menant des sondages pour recueillir leurs opinions.

Demandez-leur spécifiquement s'ils utilisent des solutions de Shadow IT et, le cas échéant, les raisons qui les motivent.

@aneol

5 | FAVORISER LA COMMUNICATION ENTRE LES SERVICES

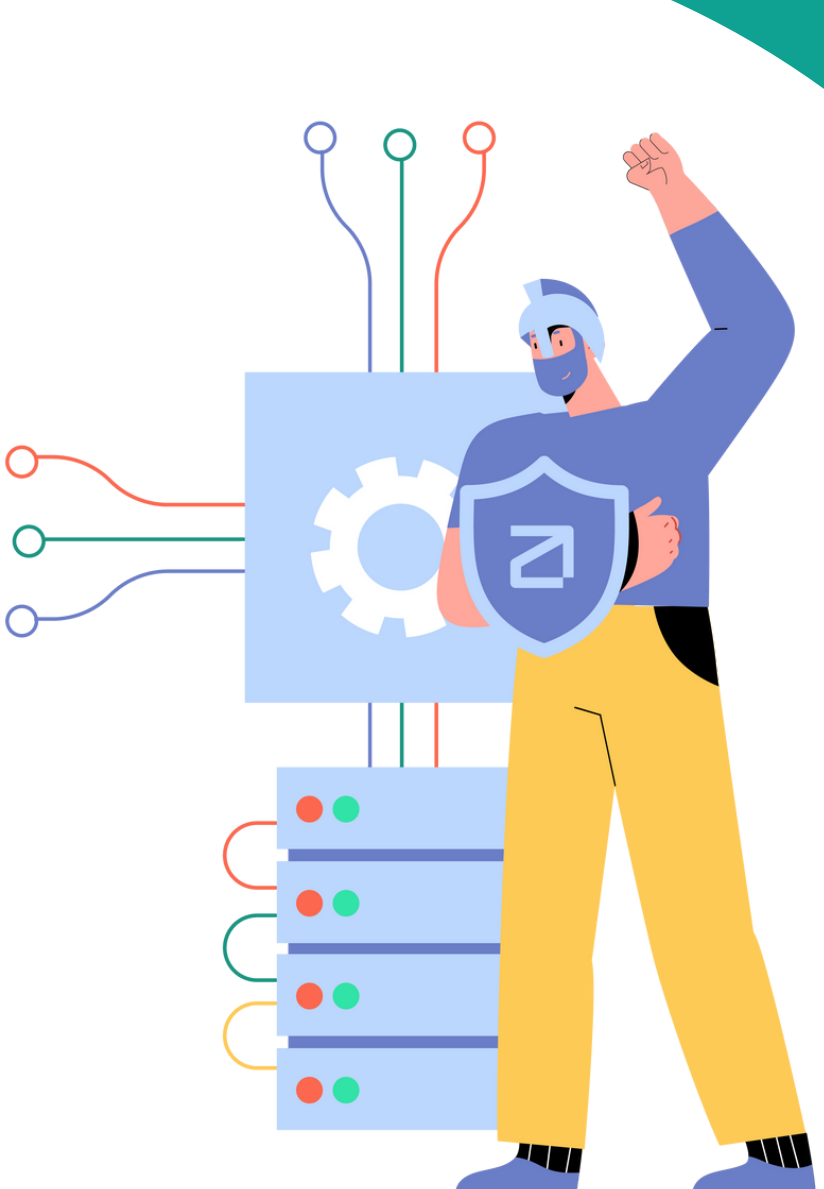
En créant des canaux de communication accessibles à tous les salariés, ils pourront facilement poser des questions, partager leurs préoccupations et proposer des idées aux équipes informatiques.

Ces échanges permettront à la direction de réévaluer les outils en place et de mener à une simplification de ces derniers pour répondre aux besoins des salariés.

@aneol

Nos experts du numérique vous aident à minimiser les risques du shadow IT

CONTACTEZ-NOUS SUR WWW.ANEOL.COM



@aneol