Le Shadow IT : un facteur de risque majeur pour la sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 19/10/2015 13:00:00

Chacun ou presque dans le monde de lâ□□informatique connaÃ®t lâ□□expression Â« Shadow IT. Â» Lâ□□utilisation de produits et de services provenant de lâ□□extÃ©rieur de lâ□□entreprise, gÃ©nÃ©ralement basÃ©s sur le cloud sans lâ□□accord prÃ©alable du service informatique interne reprÃ©sente une source dâ□□inquiÃ©tude croissante pour les DSI dans le monde entier.

Â
En 2000, environ 20% des dÃ©penses informatiques des entreprises ne dÃ©pendaient pas du budget du dÃ©partement informatique, dâ□□aprÃ¨s le cabinet Gartner. Mais cela câ□□Ã©tait avant. Gartner prÃ©voit aujourdâ□□hui que les dÃ©penses non contrÃ´lÃ©es par les DSI reprÃ©senteront 90% du total dâ□□ici la fin de la dÃ©cennie.

Ce qui donne une autre dimension au Â« Shadow ITâ□□ ! Avec la montÃ©e des services cloud et des solutions SaaS, les entreprises ont du mal Ã sâ□□adapter et Ã reprendre le contrÃ´le de la situation.

Beaucoup considÃ¨rent le â□□Shadow ITâ□□ comme une sorte de Far West, car il permet aux employÃ©s et aux dÃ©partements de fonctionner indÃ©pendamment du contrÃ´le et du support de la DSI. Cette absence de contrÃ´le centralisÃ© est un modÃ¨le qui inquiÃ¨te les DSI. Beaucoup le considÃ¨re comme une pratique coÃ»teuse et inefficace qui rÃ©duit la capacitÃ© des entreprises Ã gÃ©rer et coordonner efficacement leurs ressources informatiques.

Mais une autre menace rentre en ligne de compte : la sÃ©curitÃ© ! Car le â□□Shadow ITâ□□ gÃ©nÃ¨re des risques nouveaux et sÃ©rieux en matiÃ¨re de sÃ©curitÃ©.

Imaginez ce scÃ©nario : chaque dÃ©partement dans votre entreprise utilise sa propre solution de partage de fichiers sans lâ□□approbation du service informatique : Dropbox, Google Drive, Box, etc.

Ces applications cloud dÃ©pendent de serveurs externes et de rÃ©seaux hors de votre contrÃ´le, ils ne peuvent Ãªtre surveillÃ©s par des outils de sÃ©curitÃ© traditionnels.

De plus, elles peuvent ouvrir la voie Ã un grand nombre de problÃ¨mes de conformitÃ© et de sÃ©curitÃ© externe. Plus important encore, le service informatique Ã©tant dans lâ□□ignorance complÃ¨te, il ne pourra Ãªtre dâ□□aucun secours lorsquâ□□il sâ□□agira de contrÃ´ler et de corriger ces problÃ¨mes.

Quels sont les risques rÃ©els quâ□□induit le â□□Shadow ITâ□□ ?

â□¢ Fuite de donnÃ©es. Des services cloud tels que Dropbox ont subi des attaques par le passÃ©, qui se sont traduites par des vols de mots de passe client. Si lâ□□un de vos employÃ©s dÃ©pose des fichiers dâ□□entreprise sensibles sur Dropbox, un attaquant pourrait avoir accÃ¨s Ã ces fichiers.

â□¢ Pas de contrÃ´le sur la gestion des attaques. Un service cloud se rÃ©sume Ã un serveur et un rÃ©seau quelque part dans le monde. Il est soumis aux mÃªmes risques de sÃ©curitÃ© que votre propre rÃ©seau. Nous supposons que le fournisseur de cloud a mis en place des mesures de sÃ©curitÃ© et quâ□□il emploie les meilleures pratiques, mais nous ne savons pas dans quelle mesure.

Les services informatiques doivent avoir la possibilitÃ© de valider le niveau de sÃ©curitÃ© de leurs partenaires extÃ©rieurs, et de dÃ©cider si la valeur quâ□□ils apportent vaut le risque potentiel quâ□□ils font supporter.

â□¢ ProblÃ¨mes de conformitÃ© non prÃ©vus. Vous Ãªtes toujours responsable de la protection de vos donnÃ©es (les informations client par exemple) mÃªme si vous les dÃ©placez en dehors de votre rÃ©seau dâ□□entreprise.

Lâ□□adoption de services cloud suscite dÃ¨s le dÃ©part des interrogations, car vous avez moins de visibilitÃ© sur la faÃ§on dont des fournisseurs extÃ©rieurs gÃ¨rent vos donnÃ©es. Mais imaginez maintenant que vous ne savez mÃªme pas que des donnÃ©es sensibles ne sont plus sur votre rÃ©seau et ont Ã©tÃ© dÃ©placÃ©es ailleurs !

â□¢ Perte de moyens de contrÃ´le sur les donnÃ©es. Par exemple, imaginons quâ□□un employÃ© tÃ©lÃ©charge la liste de vos clients dans le cloud avec son mot de passe personnel, et quâ□□ensuite il soit licenciÃ© ou dÃ©missionne. Il aura toujours accÃ¨s Ã votre liste de clients, mais vous nâ□□aurez plus la possibilitÃ© de lâ□□effacer.

Il ne fait pas de doute que la â□□Shadow ITâ□□ et les services cloud vont devenir toujours plus populaires auprÃ¨s des employÃ©s. En consÃ©quence, les entreprises doivent Ãªtre prÃ©parÃ©es Ã gÃ©rer les risques associÃ©s Ã ces services.
Les quelques mesures suivantes vous aideront Ã limiter les risques associÃ©s au â□□Shadow ITâ□□.

1 â□□ Etablissez des rÃ¨gles claires pour lâ□□utilisation de services cloud. Si vous nâ□□avez pas informÃ© vos employÃ©s comment procÃ©der pour demander un nouveau service cloud en interne, ou quelles sont les rÃ¨gles en vigueur dans lâ□□entreprise en matiÃ¨re dâ□□utilisation de services cloud externes, il est quasi certain quâ□□ils les adopteront dâ□□eux-mÃªmes sans vous demander la permission.

AprÃ¨s tout, beaucoup de ces services cloud sont gratuits, rapides Ã mettre en Å□uvre et simples Ã utiliser. La sÃ©curitÃ© passe donc dâ□□abord par lâ□□Ã©tablissement de rÃ¨gles. Si vous ne voulez pas que vos employÃ©s utilisent certains services sans votre accord, vous devez les en informer explicitement.

Le mieux Ã©galement est que vous fixiez une procÃ©dure permettant de demander rapidement la mise en place de tels services quand vos employÃ©s en ont rÃ©ellement besoin. Mettez-vous dans lâ□□air du temps pour ne pas Ãªtre contournÃ©.

2 â□□ Aidez proactivement vos utilisateurs Ã obtenir les services dont ils ont besoin. Si vous contactez rÃ©guliÃ¨rement les diffÃ©rents dÃ©partements de votre organisation pour vÃ©rifier quâ□□ils disposent des services informatiques dont ils ont besoin, ils rÃ©aliseront que vous Ãªtes lÃ pour les aider Ã remplir leurs objectifs. Ceci les encouragera Ã venir Ã vous Ã chaque fois quâ□□ils auront un nouveau besoin informatique, plutÃ´t que de vous considÃ©rer comme un obstacle.

3 â□□ Si des dÃ©partements contournent le service informatique, dÃ©couvrez pourquoi et changez les choses. Les employÃ©s veulent simplement que leur travail soit fait. Lorsquâ□□ils font appel au â□□Shadow ITâ□□ et utilisent des services cloud externes, câ□□est gÃ©nÃ©ralement pour Ãªtre plus efficaces dans leur travail quotidien.

Vous devez dÃ©couvrir pourquoi ils nâ□□ont pas fait appel Ã vous. Est-ce en raison de lâ□□absence dâ□□une rÃ¨gle claire ? Le dÃ©partement informatique a-t-il la rÃ©putation de refuser systÃ©matiquement les nouvelles applications que demandent les utilisateurs ? Les services autorisÃ©s par lâ□□entreprise se sont-ils rÃ©vÃ©lÃ©s inefficaces par le passÃ© ?

Le dÃ©partement informatique est-il dÃ©bordÃ© par les demandes, et incapable de dÃ©livrer rapidement de nouvelles autorisations ? Voici les questions que vous devez vous poser si vous voulez comprendre les causes.

4 â DÃ©finissez les fonctions dont les utilisateurs ont REELLEMENT besoin avant de dÃ©livrer un nouveau service informatique. Lorsque les dÃ©partements veulent quelque chose de nouveau, listez toutes leurs demandes et cas concrets dâutilisation.

Ceci vous aidera Ã garantir que le service informatique est en mesure de dÃ©livrer un service rÃ©ellement efficace pour les utilisateurs, et quâils ne contourneront pas le systÃ¨me en cherchant eux-mÃªmes dâautres solutions.

Par exemple, il est probable que les utilisateurs auront besoin de fonctions modernes dâÃ©change dâinformations, et dâapplications accessibles indiffÃ©remment sur mobile et sur des plates-formes traditionnelles.

Si vous ne pouvez offrir des services fonctionnant efficacement et en toute sÃ©curitÃ© de nâimporte oÃ¹ et Ã partir de nâimporte quel terminal, alors ils pourront Ãªtre tentÃ©s de contourner le dÃ©partement informatique.

5 â Parfois le service cloud est le choix le meilleur et le plus sÃ©curisÃ© .
Rappelez-vous, le problÃ¨me avec le âShadow ITâ nâest pas nÃ©cessairement que quelquâun a choisi dâexternaliser quelque chose dans le cloud, mais le fait que cette personne lâa fait sans que le dÃ©partement informatique nâen ait Ã©tÃ© informÃ© ni lâait approuvÃ©.

Dans certains cas, les services cloud peuvent Ãªtre la solution la meilleure et la plus sÃ©curisÃ©e, pourvu que le dÃ©partement informatique puisse gÃ©rer et contrÃ´ler les donnÃ©es partagÃ©es dans le cloud. Au bout du compte, Ã©viter le âShadow ITâ ne veut pas dire tout conserver en interne ; câest avant tout faire participer les bonnes personnes Ã toute dÃ©cision dâexternalisation.

6 â Disposez dâoutils de visibilitÃ© capables dâidentifier le âShadow ITâ . Les Firewalls de Nouvelle GÃ©nÃ©ration et les boÃ®tiers UTM les plus rÃ©cents intÃ¨grent de nouvelles fonctionnalitÃ©s qui leur permettent dâidentifier les diffÃ©rentes applications qui communiquent sur un rÃ©seau, quels que soient les ports et les protocoles que ces applications utilisent.

Les boÃ®tiers les plus performants offrent mÃªme la fonction dâidentification HTTPS, ce qui veut dire que les services âShadow ITâ ne peuvent pas passer au travers. Si vous disposez de boÃ®tiers de ce type, ceux-ci sont dotÃ©s de bons outils de visibilitÃ© et de reporting, et peuvent vous aider Ã dÃ©couvrir quand des dÃ©partements commencent Ã utiliser un nouveau service cloud sans lâaccord du dÃ©partement informatique.

Ceci permettra Ã ce dernier de contacter ces utilisateurs, et soit dÃ©terminer sâil peut proposer une solution alternative, soit incorporer le nouveau service avec des procÃ©dures et un contrÃ´le adÃ©quats.

7 â Choisissez vos combats. La sÃ©curitÃ© a trait Ã la gestion du risque, et certains types de donnÃ©es peuvent revÃªtir une importance plus ou moins grande par rapport Ã dâautres. Certains services cloud concernent des donnÃ©es moins sensibles pour votre organisation ou dont le facteur de risque est plus faible.

Dans ces cas particuliers, le mieux est peut-Ãªtre pour vous de laisser faire, et de rÃ©server vos efforts pour des services qui gÃ©nÃ¨rent un risque potentiel trÃ¨s Ã©levÃ©.

8 â□□ Bloquez les applications les plus dangereuses en dernier ressort. Les technologies dâ□□identification et de contrÃ´le des applications mentionnÃ©es plus haut sont Ã©galement capables de bloquer certains services.

Si le dÃ©partement informatique identifie que des applications dangereuses sont en cours dâ□□utilisation et si vous ne pouvez absolument pas autoriser vos employÃ©s Ã y accÃ©der, vous pouvez vous rÃ©soudre Ã les bloquer.

Toutefois, souvenez-vous que si aucune solution approuvÃ©e ne rÃ©pond rÃ©ellement aux besoins des employÃ©s, ceux-ci continueront de chercher des alternatives sans votre accord.