Shadow IT : identifier les zones d'ombre de l'entreprise pour garantir sa sécurité

Disposer dâ€™une visibilitÃ© complÃ¨te sur le rÃ©seau de son entreprise est primordial pour assurer sa bonne gestion et sa sÃ©curitÃ©, mais aussi pour surveiller lâ€™expansion des infrastructures, logiciels et services non prÃ©vus par la DSI, le fameux Shadow IT.

Pour les administrateurs rÃ©seau, la simple pensÃ©e dâ€™un systÃ¨me IT inconnu ou mÃªme partiellement inconnu sur leur rÃ©seau peut suffire Ã les faire frissonner. Des rÃ©seaux IT fantÃ´mes (ou Shadow IT) comprenant des infrastructures complexes peuvent en effet se dÃ©velopper Ã partir de pratiques rÃ©guliÃ¨res des collaborateurs, et cela sans lâ€™accord ou la connaissance de l'Ã©quipe IT, rÃ©seaux et sÃ©curitÃ©. Ces systÃ¨mes peuvent Ãªtre aussi bien des environnements matÃ©riels managÃ©s ou encore des solutions dâ€™ERP complÃ¨tes utilisÃ©es quotidiennement dans toute lâ€™entreprise et exploitant les donnÃ©es du systÃ¨me ERP officiel, mais tout en restant inaccessibles au service IT.

Des systÃ¨mes fantÃ´mes indÃ©pendants apparaissent gÃ©nÃ©ralement en raison dâ€™une offre dâ€™outils IT ne correspondant pas aux attentes des collaborateurs. Ainsi, si un dÃ©partement ne se voit pas proposer des solutions adaptÃ©es Ã son travail, ou encore si les chefs de services ne sont pas formÃ©s Ã la nÃ©cessitÃ© de travailler Ã partir dâ€™un rÃ©seau dâ€™entreprise centralisÃ©, il est probable que des solutions seront acquises ou crÃ©Ã©es Ã partir de zÃ©ro, sans consultation du service IT.

Dâ€™aprÃ¨s un sondage publiÃ© par Entrust Datacard et menÃ© auprÃ¨s de 1000 professionnels de lâ€™industrie du numÃ©rique, 40% dâ€™entre eux dÃ©clarent avoir eu recours au Shadow IT en utilisant un dispositif, une application ou autre nouvelle technologie sans avoir obtenu au prÃ©alable lâ€™approbation de leur service IT. Par ailleurs, 37% des employÃ©s estiment que leur entreprise ne possÃ¨de pas de rÃ¨gles internes clairement dÃ©finies sur le sujet.

Il faut dire que le dÃ©veloppement du Shadow IT dans une entreprise peut avoir ses avantages, en permettant aux collaborateurs dâ€™Ãªtre plus productifs ou plus engagÃ©s, par exemple. Mais le Shadow IT peut Ã©galement Ãªtre Ã lâ€™origine dâ€™une multitude de risques involontaires pour les rÃ©seaux et lâ€™IT de lâ€™entreprise dans son ensemble :

1. VulnÃ©rabilitÃ©s Ã dÃ©couvert

Lâ€™exposition des vulnÃ©rabilitÃ©s est le premier risque majeur qui vient Ã lâ€™esprit lorsque lâ€™on pense Ã la prÃ©sence dâ€™un systÃ¨me inconnu sur le rÃ©seau. Une infrastructure mise en place Ã lâ€™insu du service IT nâ€™a souvent pas le niveau de sÃ©curitÃ© requis pour assurer une protection suffisante contre une multitude de cyber-risques. Dans certains cas, le matÃ©riel peut ne pas avoir reÃ§u les derniÃ¨res mises Ã jour ou encore ne pas disposer de pare-feu ou dâ€™antivirus. Et cela dans un monde oÃ¹ la sÃ©curitÃ© dâ€™un rÃ©seau est Ã©gale Ã celle de son appareil le moins sÃ©curisÃ©, ce dernier laissant lâ€™ensemble du rÃ©seau vulnÃ©rable aux attaques.

2. Pertes de donnÃ©es catastrophiques

Les systÃ¨mes et applications en Shadow IT fonctionnent en dehors du plan de sauvegarde et de restauration Ã©tabli par le service IT, mais utilisent et crÃ©ent tout de mÃªme des donnÃ©es critiques de lâ€™entreprise. Cela signifie que des opÃ©rations essentielles peuvent avoir lieu sans aucune solution de sauvegarde. En cas dâ€™incidents entraÃ®nant des pertes de donnÃ©es, tel quâ€™une cyberattaque, les donnÃ©es critiques de lâ€™entreprise peuvent totalement disparaÃ®tre sans aucune chance de rÃ©cupÃ©ration. Dans le pire des cas, cela pourra entraÃ®ner des dommages importants aux opÃ©rations de lâ€™entreprise, avec le risque de graves rÃ©percussions financiÃ¨res.

3. DonnÃ©es non sÃ©curisÃ©es

MÃªme en mettant de cÃ´tÃ© les problÃ¨mes liÃ©s Ã un fonctionnement sans sauvegarde suffisante, un rÃ©seau en Shadow IT ne permet pas dâ€™obtenir une vision globale des accÃ¨s aux donnÃ©es par les utilisateurs. Ce qui veut dire que des prestataires de service externes, des sous-traitants et mÃªme dâ€™anciens employÃ©s peuvent potentiellement avoir accÃ¨s Ã des donnÃ©es sensibles. Sans une vue dâ€™ensemble des autorisations dâ€™accÃ¨s, il nâ€™y a aucun moyen de savoir qui peut accÃ©der aux donnÃ©es et quel usage il va en Ãªtre fait.

4. InefficacitÃ© des opÃ©rations

Le matÃ©riel et les logiciels en Shadow IT sont souvent installÃ©s sans tests prÃ©alables et nÃ©cessaires, pouvant entraÃ®ner des opÃ©rations inefficaces. Bien que ces systÃ¨mes puissent bÃ©nÃ©ficier directement aux activitÃ©s individuelles de ceux qui les ont installÃ©s, le fait quâ€™ils ne soient pas testÃ©s peut ralentir ou mÃªme stopper dâ€™autres systÃ¨mes critiques de lâ€™entreprise connectÃ©s au rÃ©seau. MÃªme dans les rÃ©seaux en Shadow IT qui fonctionnent correctement, une double maintenance ainsi quâ€™une double administration sont impÃ©ratifs pour garantir que le systÃ¨me continue de bien fonctionner en parallÃ¨le du rÃ©seau dâ€™entreprise officiel.

5. ConformitÃ©

Un processus crÃ©Ã© en Shadow IT, et donc en dehors du protocole Ã©tabli par le service IT, a une grande probabilitÃ© de violer les rÃ¨gles de conformitÃ© informatique dâ€™une entreprise. Plus grave toutefois, lâ€™introduction de systÃ¨mes en Shadow IT dans les dÃ©partements mÃ©tiers peut constituer une violation fondamentale des rÃ©glementations externes telles que la loi sur la protection des donnÃ©es (RGPD). Ce type de cas peut entraÃ®ner de lourdes amendes de la part des rÃ©gulateurs, pouvant mÃªme entraÃ®ner la chute de lâ€™entreprise.

Le Shadow IT nâ€™est pas une fatalitÃ© et des moyens existent pour le contrÃ´ler

Tout ceci peut faire peur, mais la situation nâ€™a pas Ã dÃ©gÃ©nÃ©rer de la sorte. Heureusement, mÃªme des problÃ¨mes de Shadow IT largement rÃ©pandus dans lâ€™entreprise peuvent Ãªtre contrÃ´lÃ©s si les bonnes stratÃ©gies sont mises en place par le service IT et soutenues activement par la direction.

La premiÃ¨re Ã©tape pour supprimer les systÃ¨mes en Shadow IT, câ€™est de commencer par les localiser. La visibilitÃ© sur lâ€™ensemble du rÃ©seau de lâ€™entreprise constitue le facteur numÃ©ro 1 permettant de dÃ©tecter les pratiques fantÃ´mes et dâ€™y mettre fin. MÃªme une infrastructure parallÃ¨le bien cachÃ©e peut Ãªtre dÃ©tectÃ©e, par exemple via le relevÃ© dâ€™un trafic inhabituel de donnÃ©es Ã travers un routeur ou un switch.

Au final, câ€™est avant tout Ã la direction de mettre en place des solutions qui empÃªcheront la crÃ©ation de rÃ©seaux et dâ€™outils parallÃ¨les. Mais avec de bons outils tels quâ€™une solution

de supervision offrant une visibilitÃ© suffisante, les services IT peuvent dÃ©jÃ Ãªtre correctement Ã©quipÃ©s pour lutter contre les menaces du Shadow IT.