Le responsable IT qui a anéanti le « Shadow IT »

Combattez le « Shadow IT » et reprenez le contrôle sur votre pile de logiciels

Le « Shadow IT » est une expression que l'on entend de plus en plus dans les entreprises modernes d'aujourd'hui, mais ce que beaucoup d'entreprises ne réalisent pas est le nombre de risques que ce phénomène peut entraîner si elles ignorent ces installations non autorisées. Selon une étude, une grande entreprise utilise en moyenne environ 1 220 services cloud individuels, soit un nombre 13 fois plus important que les 91 services reconnus par les départements IT. Non seulement, le « Shadow IT » va directement à l'encontre des départements IT, mais il peut également entraîner des failles de sécurité et des coûts inutiles. En général, les employés ont recours au « Shadow IT », car ils pensent que l'utilisation de ces outils peut permettre à leur entreprise et à leur département IT de gagner du temps et de faire des économies. En réalité, le fait de contourner le département IT revient à ignorer les procédures de protection stratégiques mises en place pour la gestion, l'intégration, la sécurité et la conformité des processus.

Imaginez un monde dans lequel le « Shadow IT » a pénétré tous les niveaux de l'entreprise, et, au-delà de toute attente, menace la sécurité, la rentabilité et l'efficacité de toute l'entreprise. C'est le Far West : des fusillades dans les rues, des demoiselles en détresse et un vieux piano qui retentit en arrière-plan dans un saloon. Arrivent Clark, le responsable IT (et le héros de cette histoire), sa supérieure Cynthia, directrice des systèmes d'information et son fidèle acolyte Steven l'administrateur système. Ces trois protagonistes s'assoient ensemble en silence. Leur département a perdu le contrôle et personne ne sait de façon sûre quelles technologies sont utilisées au sein de l'organisation. La consumérisation de l'informatique, ou le cycle des employés apportant des technologies grand public populaires dans l'enceinte de l'entreprise depuis leur domicile a permis aux employés de déployer facilement des technologies sans que le département IT n'en soit averti.

Clark et son équipe ne sont pas les seuls à être confrontés à ce problème. Dans une étude Intel Security, 23 % des personnes interrogées ont affirmé que leur service gère la sécurité sans l'aide du département IT.

Un beau jour, Clark décida que tout ceci devait cesser. Il en eut assez d'être contrôlé par les caprices du « Shadow IT » et de ne pas savoir quelle technologie était utilisée pour faire fonctionner l'entreprise. Il décida donc d'agir. Il réunit son équipe, élabora un plan d'action et se lança tête baissée dans la bataille contre le « Shadow IT »

En tant qu'entreprise qui dépend fortement de l'approbation du département IT, nous voulions en apprendre plus sur le sentiment de Clark à propos des applications approuvées et mieux comprendre son approche systématique pour combattre le « Shadow IT » et créer une culture de gestion informatique plus transparente.

Lifesize
Fournisseur de logiciels de collaboration et de communication sur le cloud

Clark
L’incarnation du responsable IT héroïque pour une entreprise qui ressemble beaucoup à la vôtre

Comment avez-vous découvert le problème ? Qu’avez-vous fait pour trouver les pires contrevenants ?

Tout a commencé par un article que j'ai lu et qui affirmait que : « **7 dirigeants d'entreprise sur 10 ne savent pas combien d'applications de type Shadow IT sont utilisées dans leur organisation.** » J'ai donc voulu vérifier la véracité de cette déclaration dans mon entreprise. Mon équipe avait souvent entendu parler de toutes ces différentes applications utilisées par d'autres départements de l'entreprise, sans que personne n'en parle directement. Et bien que certaines applications ne posaient aucun problème, d'autres pouvaient potentiellement être néfastes — un risque que nous ne pouvions pas prendre. Nous avons donc commencé à effectuer un suivi étroit des outils et applications utilisés en interne pour déterminer la présence de logiciels nouveaux ou inconnus. Cette initiative s'est ensuite transformée en une analyse de vulnérabilité à l'échelle de l'entreprise.

Il existe des programmes spécifiquement créés pour détecter de nouvelles applications sur le réseau. Des « renifleurs » réseau et des outils d'analyse de la sécurité peuvent fournir des informations détaillées sur les flux de données d'un nouveau type et ceux qui sont inconnus. Bien évidemment, cette surveillance n'élimine pas complètement la menace que pose le Shadow IT, mais elle en donne un certain aperçu. Non seulement cette analyse a montré que nos employés utilisaient des outils dont nous ignorions l'existence, mais elle nous a également fourni suffisamment d'informations pour entamer une évaluation des risques et, dans le pire des cas, rechercher des solutions alternatives mieux adaptées à nos besoins.

Avez-vous rencontré une certaine

Bien sûr. Nous gérons un grand nombre de télétravailleurs dans notre entreprise, et l’un des défis que nous avons

résistance lorsque votre département IT n'a pas pu prendre en charge les outils souhaités par un autre département ?

rapidement identifiés est que si vous n'avez pas des procédures approuvées par le département IT permettant aux employés de travailler à distance ou en déplacement, ceux-ci trouveront un moyen d'y parvenir eux-mêmes. C'est à ce moment-là que les choses se corsent, car des documents peuvent être transmis de façon non sécurisée, des périphériques peuvent être volés ou perdus et ainsi de suite. Nous avons constaté qu'en faisant preuve de transparence sur nos exigences en matière de sécurité et de réseau et qu'en encourageant nos employés à communiquer avec le département IT lors de la phase de découverte de nouveaux logiciels, ceux-ci nous incluaient davantage dans la discussion et nous mettaient dans une meilleure position pour prendre une décision finale. Vous seriez surpris de voir à quel point les gens apprécient votre aide pour rechercher et sélectionner des solutions, au lieu de tourner autour du pot et tenter de trouver une réponse par leurs propres moyens.

Comment avez-vous obtenu de vos employés qu'ils vous donnent des informations sur leurs

Au début, oui. Le Shadow IT représente un danger absolu pour les sociétés peu disposées à résoudre le problème. Nous nous en sommes donc chargés. Les départements IT ont tendance à enfoncer les portes et à menacer de prison les employés qui utilisent des logiciels non approuvés, ce qui est un peu dur à mon goût. Nous, au contraire, avons décidé d'adopter une approche pacifiste. Nous avons donc proposé

outils Shadow IT ? Cela a dû être difficile.

une sorte de grâce aux départements qui utilisent des outils informatiques cachés. Au lieu d'arrêter et de supprimer aussitôt ces programmes, nous avons pris du recul afin d'évaluer les risques et d'offrir des solutions comparables le cas échéant pour atteindre les objectifs que ces départements se sont fixés. Ainsi, nous avons ouvert un dialogue sur les risques associés à chaque programme. Cet exercice nous a vraiment permis de mettre tout le monde sur la même page et d'établir un sentiment de confiance et de franchise entre « nous » et « eux ».

Comment assurez-vous la pérennité de cette stratégie ? Votre problème de Shadow IT est désormais résolu, mais comment vous assurez-vous qu'il ne reviendra pas dans votre entreprise ?

Vous savez, de nombreuses personnes m'ont posé cette question et la réponse est assez simple. Tout dépend du rapport que vous établissez avec les gens. J'ai établi une forte relation avec chaque chef de département. Je les ai régulièrement rencontrés pour discuter de la stratégie technologique et j'ai créé un dialogue d'ouverture entre le département IT et les autres services de l'entreprise. En outre, il était essentiel que ma cheffe, Cynthia, la directrice des systèmes d'information, maintienne un dialogue étroit avec le reste du personnel travaillant à distance sur la transparence technologique et les risques potentiels que peut poser l'adoption de technologies non approuvées.

Vous avez réussi à combattre le « Shadow IT ». Quels conseils donneriez-vous aux

N'hésitez pas à créer un dialogue d'ouverture avec vos collègues au sein de l'entreprise (ou vos clients). Écoutez leurs commentaires, tâchez d'en savoir plus sur les problèmes qu'ils essaient de résoudre et soyez prêts à faire des contributions. Une fois, il m'est arrivé de devoir vérifier un outil qui avait déjà été approuvé et déployé par un autre département de l'entreprise. Dans ce cas, l'application de

départements IT qui abordent tout juste le problème dans leurs organisations ?

notre plan a été beaucoup plus facile et beaucoup moins coûteuse, car il nous a suffi d'acheter un certain nombre de licences supplémentaires. Nous n'avons donc pas eu à commencer un tout nouveau contrat. Le dernier conseil que je vais vous donner est de ne pas sous-estimer la puissance d'une interface utilisateur simple. Veillez à équilibrer vos besoins en termes de sécurité et de réseau avec la facilité d'utilisation finale des applications. L'une des choses que j'aime rechercher est une solution qui s'intègre à notre système d'identification SSO. Ainsi, vous réduisez le nombre de mots de passe que les employés doivent mémoriser et mettre à jour tout au long de l'année.

La combinaison de mauvaises pratiques de protection des mots de passe avec des applications du « Shadow IT » peut créer d'importantes failles de sécurité. Consultez notre blog pour découvrir les meilleures méthodes de protection contre les attaques DDoS dans le cadre de l'Internet des Objets, et pour protéger votre réseau.

À propos de Lifesize

Lifesize est un système de collaboration approuvé par les départements IT et conçu dans l'objectif de répondre à leurs besoins tout en les aidant à assurer la sécurité, la résilience et la fiabilité du réseau. Cela fait maintenant plus de 10 ans que nous nous consacrons à la conception de caméras HD et de téléphones à écran tactile. De plus, notre interface intuitive et notre répertoire partagé offrent aux utilisateurs tout ce dont ils ont besoin pour collaborer plus efficacement avec des applications approuvées par leur département informatique, éliminant ainsi le besoin de recourir à des applications non autorisées. Les flux de communication Lifesize prennent en charge par défaut le chiffrement AES 128 bits et TLS (Transport Layer Security) pour la totalité de la signalisation, et nous exploitons un réseau privé à fibre optique via IBM Cloud. Pour couronner le tout, nous sommes fiers de notre service primé qui s'appuie sur un accord de niveau de service avec soutien financier et une assistance disponible 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

SOURCES

http://blogs.cisco.com/cloud/shadow-it-rampant-pervasive-and-explosive
http://www.csoonline.com/article/3083775/security/shadow-it-mitigating-security-risks.html
http://www.digitalistmag.com/resource-optimization/2016/02/11/2016-state-of-shadow-it-04005674