Pourquoi la séparation des tâches est si importante + bonnes pratiques et politiques

Devolutions

LE VOLUME ET LA GRAVITÉ DES CYBERATTAQUES CONTRE LES PME ONT AUGMENTÉ

Les pirates informatiques d'aujourd'hui ne visent pas seulement les entreprises et les gouvernements. Ils lancent également des attaques contre les PME. Pourquoi? C'est simple : en raison de leur petite taille et de leurs fonds limités, les PME ont généralement moins de spécialistes et de ressources en cybersécurité que les grandes organisations. Les deux tiers des PME ont subi une cyberattaque au cours des 12 derniers mois et 80% des PME disent que les logiciels malveillants ont échappé à leur logiciel antivirus. En plus, le volume et la gravité des cyberattaques contre les PME ont augmenté pendant la COVID-19.

Les ennemis intérieurs

Les mêmes facteurs qui rendent les PME particulièrement vulnérables aux pirates externes les rendent également sensibles aux attaques d'employés ou ex-employés mécontents, de fournisseurs, de sous-traitants et autres personnes qui gravitent autour de l'entreprise. Évidemment, les violations de données sont parfois le résultat d'une négligence, d'une incompétence ou d'une erreur humaine. Et c'est là que la séparation des tâches (parfois appelée ségrégation des tâches) entre en scène.

Qu'est-ce que la séparation des tâches?

La séparation des tâches (de l'anglais Segregation of Duties ou SoD) est une politique qui interdit à une seule personne d'être responsable de l'exécution de tâches conflictuelles. L'objectif, comme indiqué dans la norme ISO/CEI 27001, est de réduire les possibilités de manipulation ou d'utilisation abusive ou non autorisée des actifs organisationnels. Autrement dit, lorsque plusieurs personnes sont impliquées dans des tâches à caractère sensible, il y a moins de chances qu'une personne essaie d'enfreindre les règles ou que les erreurs ne soient pas détectées.

SoD est utilisé depuis plusieurs décennies dans la comptabilité, la gestion de risques et l'administration financière. Cependant, ces dernières années, le concept est entré dans l'espace de la cybersécurité. Les objectifs sont les suivants:

- Prévenir les conflits d'intérêts (réels ou apparents), les actes fautifs, la fraude, les abus et la construction de « silos secrets ».
- Détecter les défaillances de contrôle, telles que les failles de sécurité, le vol d'informations et le contournement des contrôles de sécurité.
- Empêcher les erreurs de se produire parce que les employés portent plusieurs chapeaux.

SoD et POLP

SoD est ancré dans le principe du moindre privilège (de l'anglais ***Principle of least privilege*** ou POLP), par lequel les utilisateurs finaux ne bénéficient que de la quantité d'accès dont ils ont réellement besoin pour faire leur travail - ni plus ni moins. Bien que les utilisateurs ne soient souvent pas très contents des restrictions imposées par le POLP, l'objectif n'est pas de leur rendre la vie difficile. Le but est plutôt de minimiser la taille de la surface d'attaque et de réduire la probabilité et la gravité d'une cyberattaque. C'est particulièrement important maintenant que les pirates ciblent les comptes compromis au bas de l'échelle. Une fois qu'ils réussissent à entrer, ils se propagent latéralement sur les appareils et les réseaux, et accèdent finalement aux systèmes critiques et aux données sensibles.

Bonnes pratiques

Les PME devraient adopter rapidement les bonnes pratiques suivantes :

- Effectuez un audit interne et assurez-vous qu'aucune personne n'a accès aux systèmes sans contrôle et sans surveillance. L'exception à cette règle dans de nombreuses PME sera les administrateurs système, qui ont légitimement besoin d'accéder à toutes les applications, bases de données, etc.
- Mettez en place des bases de données selon le concept de séparation des tâches et des rôles et le principe du moindre privilège (comme indiqué ci-dessus).
- Faites des audits de sécurité des informations et portez une attention particulière aux activités potentiellement frauduleuses. Il est conseillé aux PME qui ne disposent pas d'une expertise interne dans ce domaine de travailler avec une firme ou un consultant externe, parce que les activités malveillantes sont presque toujours cachées et difficiles à détecter.
- Expliquez clairement que des audits et des vérifications sont en cours, comme l'examen régulier des journaux (logs) du réseau. Le simple fait que ces vérifications aient lieu aura un effet dissuasif.
- Offrez une formation en cybersécurité aux utilisateurs finaux, idéalement sur une plateforme en ligne. En plus de réduire le risque d'erreurs, la formation sensibilise les employés et favorise une culture de vigilance en matière de cybersécurité - ce qui est dissuasif en soi.
- Optez pour une technologie appropriée. Par exemple, Remote Desktop Manager, Devolutions Password Hub et Devolutions Password Server font tous partie d'une infrastructure de sécurité qui prend en charge la séparation des tâches. Les principales fonctionnalités intégrées incluent un contrôle d'accès basé sur les rôles, la prise en charge de l'authentification à deux facteurs et la gestion améliorée des comptes privilégiés. Toutes les solutions sont abordables pour les PME et offertes en différents modèles de licence.

Les politiques de ressources humaines

En plus des conseils ci-dessus, les PME devraient mettre en place des politiques de ressources humaines qui soutiennent un programme SoD complet.

- Procédez à un filtrage pré-employé et poursuivez le filtrage continu après l'embauche. L'existence même de cette politique découragera les candidats qui ont une intention malveillante de travailler pour l'entreprise. Elle empêchera probablement aussi les employés actuels d'avoir des activités illicites.
- Formez les superviseurs et les gestionnaires à reconnaître, documenter et (au besoin) communiquer tout changement dans les comportements et les habitudes de leurs employés, comme une apparente nervosité lorsqu'on leur pose des questions banales.

- Si possible, forcez les employés à prendre au moins deux semaines de vacances par année. L'ironie est que dans de rares cas, un employé qui semble très travaillant et qui prend rarement du temps pour lui (pas plus d'une journée ici et là) n'est peut-être pas aussi dévoué que vous le pensez. Il est plutôt terrifié à l'idée de voir ses actes illégaux exposés au grand jour. Jonathan Middup, associé chez ***Ernst & Young's Fraud Investigation*** and ***Dispute Services Practice***, affirme d'ailleurs que « le profil d'un fraudeur typique est un employé de longue date et de confiance, qui travaille de longues heures et hésite à prendre son congé annuel ».

Avec ceci en tête, il est important de noter que l'intention n'est jamais de créer une culture de peur et de suspicion. En vérité, la grande majorité des employés (de même que les sous-traitants, consultants, vendeurs, etc.) ne se livrent à aucune activité illicite et n'envisageraient jamais de le faire.

Néanmoins, les PME doivent être proactives et vigilantes, parce qu'il suffit d'une seule « pomme pourrie » pour déclencher une catastrophe. Le coût moyen d'une violation de données dans une PME est estimé entre 120 000 $ et 1,2 M$ et 60% des PME cessent leurs activités dans les six mois suivant une cyberattaque.

Conseils de notre Chef de la sécurité, Martin Lemay

En plus des menaces dont il est question dans cet article, le manque de SoD peut être similaire au concept de « défaillance unique » pour les professionnels des TI. Ce genre de point de défaillance unique doit être évité à tout prix pour réduire l'ampleur des impacts en cas de comportement inattendu ou de défaillance.

En gardant à l'esprit que le principal vecteur d'une menace externe est l'hameçonnage, quel serait l'impact si le directeur informatique, en supposant qu'il avait les clés de tout, se faisait prendre? Vous pensez que la sensibilisation à la sécurité est suffisante? Votre gestion de correction est adéquate? Seriez-vous prêt à mettre en jeu la survie de votre entreprise en vous basant sur ces hypothèses? Pas moi!

Le modèle de menace SoD doit être discuté et évalué avec tous les cadres, en utilisant une approche basée sur le risque qui s'aligne sur les objectifs de l'entreprise. L'impact d'un individu spécifique compromis est-il acceptable ou non pour l'entreprise? Non seulement du point de vue des menaces internes, mais également en tant que surface d'attaque? Si la réponse est non, il est peut-être temps de séparer les tâches et les responsabilités pour réduire l'exposition aux menaces et les impacts liés à cette personne.

Lorsqu'une entreprise met en place le principe de séparation des tâches, il y a souvent cette appréhension - comme pour tout problème informatique nécessitant une solution : la tendance à complexifier inutilement la solution, ce qui mène à des résultats décevants. Que se passe-t-il s'il y a une mauvaise conformité ou que les employés ont de la difficulté à accepter le changement? Et s'il y a une réduction de la productivité de l'entreprise, une augmentation des coûts opérationnels ou une confusion par rapport à la complexité de la communication? Si l'embauche d'un nouvel employé semble nécessaire pour appliquer le principe de SoD, cela peut être un signe d'une ingénierie excessive.

Cependant, à mesure que l'entreprise grandit, la délégation naturelle des responsabilités doit avoir lieu et ne doit pas être limitée à des fins injustifiées. Des contrôles compensatoires pourraient également être envisagés pour couvrir la faiblesse de la séparation des tâches dans l'organisation. Les audits, l'approbation des flux de travail et d'autres outils technologiques pourraient contribuer à réduire ces risques.

Il n'y a pas de recette magique pour une bonne séparation des tâches, mais ce processus devrait inclure les gestionnaires et des discussions sur les risques avec le personnel pertinent.

Conclusion

Bien que la séparation des tâches ne soit pas bulletproof (rien en cybersécurité ne l'est), elle aide considérablement les PME à réduire le risque d'être victime de menaces internes qui, dans certains cas, peuvent être beaucoup plus insidieuses, coûteuses et d'une durée plus longue que les attaques menées par des pirates externes.