Dans le domaine de la sécurité informatique, l'attention se porte sur un enjeu majeur : une gestion des accès efficace et orientée vers les évolutions futures. Pourquoi ? Parce que la plupart des attaques de réseau sont le résultat d'un abus de privilèges, qu'il s'agisse de comptes répertoriés ou de terminaux locaux. Les entreprises sont aujourd'hui confrontées au défi de protéger leurs réseaux informatiques et leurs données, mais aussi de répondre à des exigences légales strictes - et cela ne s'applique pas seulement aux infrastructures critiques (IC). C'est là qu'entre en jeu une approche fondée sur les risques, qui permet d'atteindre ces deux objectifs rapidement et de manière extrêmement efficace.

En février dernier, la télévision allemande a exposé une inquiétante faille de sécurité concernant les infrastructures critiques en Allemagne : des centrales solaires d'une capacité de 14 mégawatts, situées en Rhénanie-du-Nord-Westphalie, étaient insuffisamment protégées, utilisant des mots de passe prédéfinis qui n'avaient jamais été changés. Des centaines de pages de connexion non cryptées ont été découvertes sur des portails de contrôle de parcs éoliens et solaires. Les experts estiment qu'il existe environ 2 500 centrales solaires non sécurisées en Europe, d'une capacité d'environ 2,8 gigawatts. Ce risque de sécurité massif ouvre la porte à des pirates informatiques et pourrait avoir des conséquences désastreuses. Les cyberattaques contre des sociétés d'énergie éolienne soulignent déjà l'urgence de la situation, car elles pourraient mettre en péril la stabilité des réseaux d'approvisionnement en électricité. Il ne s'agit là que d'un exemple parmi de nombreuses autres.

Des lois plus strictes pour relever le niveau de protection

Le rapport met l'accent sur un secteur spécifique, mais la réalité montre que d'autres secteurs connaissent des problèmes similaires. Les secteurs des soins de santé et des services publics sont particulièrement touchés. Les établissements scolaires et d'enseignement sont aussi de plus en plus attaqués, bien que l'on ne s'attende pas à y trouver des données très précieuses ou à obtenir des demandes de rançon élevées. De plus en plus d'acteurs soutenus par des États agissent avec une vigueur impitoyable pour attaquer les identités, accéder aux données, aux actifs numériques IT/OT et à d'autres biens de l'entreprise nécessitant une protection particulière. Dans la plupart des cas, les techniques de défense conventionnelle se révèlent insuffisantes.

En réponse, les législateurs et les associations ont instauré des règles de sécurité rigoureuses pour les infrastructures critiques, élargissant considérablement le groupe d'entreprises considérées comme telles. Bien que nombre de ces règles soient conçues pour s'appliquer à toutes les entreprises, les exigences primordiales en matière de sécurité informatique incluent la norme ISO 27001, émise par l'Office fédéral allemand pour la sécurité de l'information (BSI) sous la forme de B3S. De plus, la norme IEC 62443 est devenue une référence internationalement reconnue pour la sécurité dans l'industrie des processus et de l'automatisation, tandis que les directives de la NIS 2 représentent également des repères essentiels.

La directive européenne NIS 2 doit être transposée en droit national d'ici octobre 2024, en Allemagne, par le biais de la loi sur la sécurité informatique 3.0. Cela sert à créer un cadre juridique moderne pour l'augmentation de la numérisation et de la cybercriminalité. Les entreprises doivent vérifier si les réglementations étendues affectent également les petites entreprises et les plateformes numériques. Les exigences en matière de gestion des cyberrisques, de

gestion de la continuité des activités, de contrôle d'accès, d'authentification et d'autres mesures de sécurité précédemment formulées dans la législation restent en place ou sont élargies. Ce qui est nouveau, c'est l'obligation de prendre en compte la sécurité tout au long de la chaîne d'approvisionnement, bien que cela ait déjà été stipulé dans la loi allemande sur la sécurité des technologies de l'information (IT Security Act 2.0).

La conformité est impérative et la sécurité y apporte une valeur ajoutée incontestable

Les entreprises et les organisations s'empressent aujourd'hui de prouver qu'elles respectent les réglementations. Cependant, lorsqu'il s'agit de savoir comment l'accès aux systèmes doit être réglementé, les avis divergent souvent : Les RSSI (responsables de la sécurité de l'information) et les responsables de la conformité privilégient souvent les approches axées sur le respect des listes de contrôle et des exigences légales. Leur principal objectif est de garantir la réussite des audits et le respect des réglementations. La réduction effective des risques joue un rôle moins important.

En revanche, les équipes chargées de la sécurité informatique préfèrent s'appuyer sur des modèles fondés sur le risque qui se concentrent sur la minimisation des risques et des menaces réels liés aux cyberattaques et aux atteintes à la protection des données. Toutefois, ces équipes se heurtent souvent à la résistance de la direction informatique. Ces derniers s'attendent souvent à des périodes de mise en œuvre (excessivement) longues, de l'ordre de deux à trois ans, et à des efforts considérables pour de tels projets.

Cependant, l'entreprise française WALLIX, spécialisée en cybersécurité, a démontré à plusieurs reprises qu'une gestion des accès basée sur les rôles, s'appuyant sur un modèle de sécurité axé sur les risques, peut être implémentée en seulement deux ou trois mois, avec un effort gérable. La première étape consiste à évaluer minutieusement la criticité de tous les systèmes utilisés et des données stockées au sein de l'entreprise, en s'appuyant sur les normes BSI et ISO ainsi que sur les outils associés. L'intervention d'un expert est précieuse pour définir les niveaux de risque adaptés et élaborer des stratégies sur mesure répondant aux besoins spécifiques de l'entreprise.
En fonction de ces niveaux de risque, des mesures de protection spécifiques sont ensuite définies pour répondre de manière adéquate aux exigences de sécurité.La mise en place d'une structure robuste de rôles et d'autorisations est essentielle pour réussir la gestion des accès à privilèges (PAM). Le modèle de classe de risque de WALLIX présente des avantages considérables dans ce domaine. De plus, des modèles pragmatiques facilitent grandement les processus d'autorisation nécessaires.

En prime, une transparence et un contrôle accrus

L'introduction d'un système de gestion des accès basé sur les risques offre une multitude d'avantages. Les entreprises peuvent l'utiliser pour contrôler et surveiller de manière précise l'accès à leurs systèmes. Cela leur permet d'exercer un contrôle accru sur leurs ressources, particulièrement lorsqu'il implique des employés ou des fournisseurs de services externes. Ce système comble les lacunes en fournissant des données détaillées sur les accès, identifiant qui a accédé à quelles données et à quel moment. Ceci s'avère crucial pour l'amélioration continue d'un système de gestion de la sécurité de l'information (SGSI).En outre, la mise en place d'un système de gestion des accès basé sur les risques présente des avantages manifestes. Elle simplifie les processus opérationnels et permet une traçabilité transparente des activités d'accès aux systèmes internes. Wallix propose des règles d'accès personnalisées, une gestion efficace des risques et une classification des risques, facilitant ainsi la mise en place rapide des processus nécessaires. Cette infrastructure de sécurité rehausse le niveau des organisations, jetant les bases de processus opérationnels efficaces et durables.

Aligner les responsables de la sécurité des systèmes d'information (RSSI) et les équipes de sécurité informatique sur les mêmes objectifs peut atténuer les conflits qui surgissent souvent autour de la gestion des accès, économisant ainsi les ressources de l'entreprise. Un système de gestion des accès basé sur les risques présente l'avantage de répondre aux besoins des deux parties. Sa mise en œuvre rapide et économique répond aux préoccupations financières des RSSI. De plus, en répondant à diverses exigences de conformité, ce système s'aligne sur les attentes réglementaires.
WALLIX accorde une attention particulière à la gestion des accès à l'échelle de l'infrastructure informatique, notamment en sécurisant les comptes à privilèges et les informations d'identification sensibles. Ainsi, la conformité et la sécurité informatique avancent main dans la main, permettant aux RSSI et aux équipes informatiques de collaborer pour atteindre des objectifs communs.

Il est crucial de souligner que pour maintenir l'efficacité du système, un système de gestion des accès basé sur les risques doit être constamment mis à jour, car les risques évoluent continuellement. Une surveillance et une révision régulières sont essentielles pour s'assurer que le système reste à jour par rapport aux exigences actuelles. Cependant, ces ajustements ne représentent pas un fardeau financier excessif, notamment avec les outils disponibles, pour autant que la première classification ait été soigneusement effectuée.
Dans l'ensemble, adopter une approche de gestion des accès basée sur les risques se révèle être une stratégie hautement efficace pour les organisations. Cela leur permet non seulement de se conformer aux exigences réglementaires, mais également de protéger efficacement leurs systèmes contre la multiplication croissante des menaces numériques. Wallix a brillamment démontré que cette approche peut être mise en œuvre avec peu d'efforts tout en générant des avantages considérables. L'investissement dans cette méthode vaut amplement la peine pour assurer la sécurité et la conformité au sein de toute organisation.

Pourquoi choisir WALLIX ?

WALLIX s'engage résolument à élever le niveau de sécurité des organisations et de leurs systèmes en proposant des solutions novatrices de gestion des accès.

En adoptant une approche axée sur les risques, WALLIX permet une définition précise des règles d'accès et d'interaction, basée sur des évaluations des risques et des analyses des besoins de protection. Cette approche cible restreint l'accès aux systèmes présentant des risques élevés, réduisant ainsi les menaces potentielles.

En tant que partenaire étroit des systèmes de gestion de la sécurité de l'information (ISMS), WALLIX contribue à garantir la conformité, notamment en respectant les normes telles que l'ISO 27001 pour les contrôles d'accès.

En classant méthodiquement les systèmes de l'entreprise selon leur importance critique et en assignant des niveaux de risque spécifiques, WALLIX propose des solutions sur mesure pour une mise en œuvre efficace de la gestion des accès, assurant ainsi un haut niveau de sécurité. Avec WALLIX, la protection optimale des données de l'entreprise va de pair avec le respect des exigences réglementaires.