Ressource de Petri IT Knowledgebase
Une propriété de BWW Media Group

Document technique de Petri
23 mai 2022

Cybersécurité et sécurité des TI : être responsable de la sécurité de l'information en entreprise

Survol

Protéger les ressources et les données TI des menaces internes et externes peut s'avérer ardu. Il est donc important, au moment de l'élaboration d'une stratégie de sécurité, de déterminer quelles sont les menaces qui peuvent affecter une organisation, quelles ressources doivent être protégées et à qui incombe cette responsabilité.

Dans ce document technique, nous détaillerons les différences et les similitudes entre la cybersécurité et la sécurité des TI. Pour ce faire, nous aborderons d'abord les fonctions d'un directeur des systèmes d'information (qui supervise le processus d'évaluation des risques et qui assure la protection adéquate d'une organisation), pour ensuite nous pencher sur la différence entre les outils nécessaires à la cybersécurité et à la sécurité des TI.

Qu'est-ce que la cybersécurité ?

La cybersécurité consiste à mettre en place des contrôles, des procédés, et des technologies afin d'empêcher des cyberattaques visant à s'emparer de données ou à compromettre des appareils.
Il s'agit donc d'un terme générique qui désigne de nombreuses manières de protéger des données, des serveurs, et des utilisateurs finaux. En somme, la cybersécurité sert à réduire les risques de cyberattaques et à prévenir l'exploitation non autorisée de systèmes, de réseaux et de technologies.

La cybercriminalité coûte des milliers de dollars aux entreprises chaque année, en plus de causer des interruptions importantes de leurs services.

Près de la moitié des entreprises basées au Royaume-Uni et aux États-Unis admettent subir au moins une brèche de sécurité par année.

Le groupe d'experts-conseils en stratégie Altman Vilandrie & Cie a réalisé un sondage auprès de 400 décideurs TI dans 19 secteurs d'activité. Ce dernier a révélé que 48 % des entreprises américaines ont été confrontées à une brèche dans leur sécurité. Au Royaume-Uni, un sondage commandé par le Département du Numérique, de la Culture, des Médias et du Sport (DCMS) a dévoilé que les entreprises britanniques estiment avoir essuyé 998 brèches de sécurité au cours des 12 derniers mois, et que 13 % d'entre elles en subissent quotidiennement.

Sécurité des TI et cybersécurité

La sécurité des TI est un sous-domaine de la sécurité informatique traditionnelle (qui se base sur l'utilisation d'équipes rouges et bleues, sur la séparation déontologique et sur les tests d'intrusion). Contrairement à la cybersécurité, la sécurité des TI désigne la protection de serveurs, de réseaux, d'ordinateurs et de données, et ce, peu importe s'ils sont connectés à un réseau public tel que l'Internet.

La sécurité des TI inclut, par exemple, la mise en place d'une politique de mots de passe forts pour Windows Server Active Directory (AD), ou encore le maintien d'un accès sécurisé aux partages réseau sur un serveur de fichiers. Bien que l'apparition du terme *cybersécurité* soit plus récente dans l'usage, ce dernier englobe beaucoup plus d'activités que *sécurité des TI*. Il existe néanmoins de nombreux recoupements entre les deux termes.

Qui est vulnérable ?

Il est important de souligner que ces atteintes à la sécurité n'affectent pas seulement les compagnies et les organisations financières d'envergure. En effet, toutes les organisations sont vulnérables aux cyberattaques, indépendamment de la taille ou du secteur d'activité. Dans les faits, qu'une organisation compte 5 utilisateurs ou 500 n'a aucune importance. Elle doit tout de même s'assurer que ses données, ainsi que celles de ses clients et de ses employés, sont sécurisées.

En résumé, la cybersécurité et la sécurité des TI font partie intégrante des mesures de sécurité informatique utilisées en entreprise pour empêcher les accès non autorisés à des ordinateurs, des réseaux ou des programmes.

Qui est responsable de la cybersécurité et de la sécurité des TI?

Tout d'abord, il faut bien comprendre que toutes les parties d'une entreprise peuvent être affectées par des problèmes de sécurité. Certes, l'impact d'une cyberattaque peut varier en fonction des méthodes utilisées et des départements touchés, mais toutes les branches d'une entreprise se voient confrontées à des problèmes de sécurité, qu'ils soient communs ou non.

Dans une perspective globale de l'organisation des TI, il existe des équipes spécialisées dans l'ensemble des aspects de sécurité réseau. De telles équipes s'occupent, par exemple, des pare-feu. Ces derniers servent à restreindre l'accès à un port sur une ou plusieurs adresses IP en autorisant seulement le trafic provenant de ports et de protocoles spécifiques.

Dans le domaine du stockage de données, une équipe peut prendre en charge la gestion des droits numériques (GDN) afin de s'assurer que les informations de l'entreprise ne puissent pas être utilisées en dehors de celle-ci en cas de brèche. Cette équipe classe les données en fonction de leur nécessité et de leur sensibilité. Il existe également des premiers répondants en cas de vol ou de fuite de données.

Puis, il y a les équipes de traitement de données. Puisqu'elles croient ardemment que l'étape du traitement des données est essentielle, ces équipes chiffrent toutes les données et s'assurent que seules les bonnes personnes y ont accès. Pour ce faire, ils utilisent une gamme de méthodes, dont l'octroi d'accès privilégiés.

Bien que ces domaines de compétences soient essentiels, la majorité des problèmes ne proviennent pas de la gestion ou du traitement des données, de l'empressement ou encore des réseaux; ce sont plutôt les utilisateurs eux-mêmes qui causent le plus de soucis de sécurité.

Le rôle de directeur des systèmes d'information

En tant que DSI, il est important de prendre en compte tous les facteurs de risques. Pour ce faire, il est nécessaire de comprendre où les données sont stockées, si elles sont chiffrées ou doivent l'être en transit, et quelles API sont utilisées lors de leur traitement.

Politique sur la sécurité des TI

De nombreuses entreprises disposent d'une politique sur la sécurité des TI . Pour s'y conformer, le personnel se doit de suivre des formations, en plus d'adhérer à certaines pratiques et procédures. Ces politiques peuvent varier selon les environnements de travail et les risques qui y sont associés. En d'autres termes : à chaque équipe ses problèmes.

La compréhension et la conscientisation des employés sont vitales pour la protection des données et des systèmes. En effet, la sécurité de l'information est une responsabilité qui incombe à chaque employé.

Au-delà du réseau, des services et du centre de données

En établissant une politique robuste sur la sécurité des TI basée sur une évaluation des risques, les professionnels TI peuvent déterminer quelles sont les pratiques et les procédures que doivent suivre les employés afin de garantir la sécurité des données et des systèmes.

La liste ci-dessous comprend trois aspects importants de la sécurité des TI qui font généralement partie d'une politique sur la sécurité des TI. Ces responsabilités reviennent habituellement aux équipes de sécurité des TI plutôt qu'aux équipes de cybersécurité.

1. **Stockage des données dans des endroits sanctionnés** – Stocker les données en lieux sûrs est primordial pour l'avenir d'une entreprise, que celles-ci contiennent des données touchant à la propriété intellectuelle ou encore des informations d'identités personnelles.

2. **Mots de passe sécurisés** – l'utilisation de mots de passe forts est absolument essentielle : il s'agit d'une mesure de sécurité de base. Des mots de passe faibles permettent à des acteurs malveillants d'accéder à des données et à des systèmes. Un mot de passe fort consiste en une séquence de lettres, de chiffres, ou d'autres caractères. Plus le mot de passe est long, plus il est fort.

   Les employés doivent être informés qu'il est inacceptable d'écrire ses mots de passe, de les garder sur leur téléphone portable ou dans un fichier. Si cette consigne est difficile à suivre pour le personnel, l'emploi de gestionnaires de mots de passe devrait être encouragé. De cette manière, les employés auront accès à un coffre sécurisé qui contiendra tous leurs mots de passe pour l'entreprise dans un seul endroit.

3. **Gestion des accès privilégiés (PAM)** – la gestion des accès privilégiés consiste à gérer et contrôler l'accès aux comptes privilégiés. Un système PAM est vital pour toutes les entreprises, peu importe leur taille.

   Les systèmes PAM servent à gérer l'accès des utilisateurs privilégiés aux systèmes. Les utilisateurs privilégiés sont des individus qui disposent d'un accès de niveau élevé à un réseau, un ordinateur, un système ou une fonctionnalité. Ils ont l'autorisation d'effectuer des actions qui sont interdites aux utilisateurs standards et élevés.

   Bref, un système de gestion des accès privilégiés protège les données et les systèmes auxquels les utilisateurs ne devraient plus accéder. Afin de réduire les risques qu'un accès non autorisé soit accordé, le système PAM utilise des mesures d'identification et d'authentification. Ensuite, il assure la bonne gestion des comptes d'utilisateur ainsi que l'audit des accès privilégiés.

   Les procédures PAM devraient inclure l'usage d'un coffre de mots de passe ainsi que l'utilisation d'une authentification à deux facteurs. Idéalement, une solution PAM devrait fonctionner nativement avec Active Directory (AD) et Office 365 pour permettre le contrôle des accès basé sur les rôles (RBAC) dans les systèmes des entreprises. Le tout, bien sûr, évite d'augmenter le trafic de service que génère la création de nouveaux comptes sur un système à part.

La réalité de la cybersécurité et de la sécurité des TI

Tandis que les équipes de cybersécurité effectuent des tests d'intrusion et que l'équipe bleue défend le réseau des menaces externes, les professionnels de la sécurité des TI assument la responsabilité pour les aspects opérationnels des événements relatifs à la sécurité de tous les jours. Il est alors question d'authentifier les utilisateurs et de leur accorder l'accès aux ressources dont ils ont besoin.

Évidemment, les outils requis par les professionnels de la sécurité des TI pour la protection de leur entreprise diffèrent de ceux des équipes de cybersécurité.

En revanche, la sécurité des TI n'est pas censée compenser toutes les vulnérabilités de l'entreprise aux dépens de la productivité des employés. Les départements de cybersécurité et de sécurité des TI doivent fonctionner tout en permettant aux utilisateurs finaux de travailler en paix. Bien souvent, un statu quo restrictif s'installe dans lequel l'organisation et ses employés, incluant le personnel TI, se voient dans l'impossibilité d'accomplir leur travail comme ils l'entendent.

La sécurité et la productivité servent le même but : le succès de l'organisation. L'intersection entre ces deux besoins se situe au niveau de l'intégration opérationnelle et de la conception d'une stratégie de sécurité.

Qu'est-ce que tout cela signifie? En quelques mots : une réduction des interruptions dans les activités de l'organisation. L'équipe de sécurité échoue lorsque les effets qui accompagnent une nouvelle procédure sont trop envahissants pour les employés. Cet échec rend l'entreprise vulnérable puisque les employés essaieront de trouver des méthodes pour contourner les procédures afin d'accomplir leur travail.

Les solutions de sécurité ne devraient donc pas aller à l'encontre de la productivité. En fait, les données rassemblées dans le cadre d'une opération de sécurité devraient, en toute logique, prouver cette théorie.

Plus une solution de sécurité est forte, meilleures seront nos suggestions et plus optimisée sera la sécurité au sein de l'entreprise. L'objectif principal est d'encourager la compréhension et l'adoption de bonnes pratiques, tout en protégeant les activités des entreprises et en empêchant les brèches de sécurité.

Conclusion

Le monde évolue et les procédures de sécurité standards, telles que les tests d'intrusion et le chiffrement des données, ne suffisent plus. Toutefois, les plus grands facteurs de risque au sein d'une entreprise ne découlent pas de son réseau, de ses serveurs, ou encore de son centre de données, mais bien de ses employés.

Informations supplémentaires

Pour plus d'informations concernant les enjeux et les solutions qui touchent les PME, veuillez consulter notre Portrait de la cybersécurité dans les PME en 2020-2021.

Devolutions