Conseils & astuces

11 idées pour –mieux– sécuriser votre entreprise

Quelques conseils ne suffisent pas pour réaliser une protection complète, mais cette liste est un bon début et résume les priorités essentielles.

1. Identifiez les risques

Si vous parvenez à identifier les risques au sein de votre réseau, vous pourrez les contrôler plus efficacement. Une analyse intégrale des risques permet de répertorier vos processus critiques ainsi que vos données, logiciels, équipements, réseaux, utilisateurs, etc. Si vous avez adopté la philosophie 'Bring Your Own Device' (BYOD), un inventaire de tous les appareils est indispensable.

2. Intégrez plusieurs mécanismes de sécurisation

Un bon système de sécurisation n'est jamais tributaire d'un seul produit ou mécanisme de défense. Une défense multiple accroît l'efficacité de votre protection.

3. Alignez votre protection sur vos processus d'exploitation

Pour ne pas entraver le fonctionnement de l'entreprise, votre protection doit être fondée sur une solide connaissance des processus d'exploitation.

4. Choisissez un partenaire de confiance pour votre protection

La sécurisation d'ordinateurs et de réseaux informatiques est un domaine éminemment complexe. Seules les grandes entreprises peuvent se permettre d'avoir leur propre expert en sécurité ; les autres opteront plutôt pour un partenaire externe. Pour choisir un tel partenaire, la confiance est un critère essentiel. Vérifiez quels certificats il a obtenus et s'il peut se prononcer sur des produits de sécurité en toute objectivité et indépendance. Les certificats CISSP, CISA et CEHA sont des exemples de certificats importants et garants de la qualité de votre partenaire.

5. Établissez une politique en matière de sécurité

Quelles applications et URL vos collaborateurs peuvent-ils ou non utiliser ? Peut-être souhaitez-vous autoriser l'utilisation des médias sociaux mais uniquement l'après-midi ? Ce type de politique peut être spécifié dans une charte en matière de sécurité, que signera ensuite chaque collaborateur. Et si vous voulez pouvoir supprimer à distance des logiciels ou données illicites chargés sur un appareil, vous mentionnerez également cette possibilité dans ce document.

6. Sensibilisez vos collaborateurs aux risques

La sécurité n'est pas un problème purement technique mais bien un problème humain. Apprenez à vos collaborateurs qu'il vaut mieux ne pas utiliser le même mot de passe pour toutes les applications. Signalez-leur les dangers du téléchargement, du social engineering, des appareils mobiles, etc.

7. Ne laissez vos collaborateurs accéder qu'aux données dont ils ont besoin

Un collaborateur du département marketing n'a pas besoin des données du service du personnel. Elles doivent donc lui être inaccessibles. La classification des données d'entreprise permet une filtrage précise. Vous pourrez ainsi déterminer qui est le titulaire des données, qui peut les consulter, les modifier, etc.

8. Continuez à évaluer et tester

Continuez à évaluer et tester votre système de protection. Les analyses détaillées telles que les tests de pénétration ne sont pas abordables pour toutes les entreprises. Mais les petites entreprises peuvent aussi tester régulièrement leur protection. Et si un test révèle des faiblesses, prenez les mesures adéquates.

9. Établissez un plan de back-up

Aucune protection n'est hermétique à 100 %. Tenez dès lors compte du fait que des problèmes peuvent aussi survenir dans un environnement bien protégé. Sachez quelles sont vos applications critiques, ce qui peut arriver en cas de 'plantage', et prenez les mesures requises pour pouvoir continuer à travailler dans une telle éventualité.

10. Installez un logiciel de gestion de journal de bord

Les journaux de bord vous permettent de savoir quels problèmes sont survenus et quel a été leur impact. Si vous n'avez pas de journal de bord, vous ne pourrez pas tirer les enseignements des incidents.

11. Établissez un plan de communication

Comment votre entreprise va-t-elle mener ses communications internes et externes en cas de problèmes de sécurité ? Qui allez-vous informer et comment ? Si vous disposez des journaux de bord adéquats, vous pourrez communiquer correctement et ouvertement sur la question. Cela vaut toujours mieux que tenter de cacher ou minimiser les problèmes.

Plus d'informations

- **Découvrez nos solutions de sécurisation sur www.telenet.be/security**
- **Appelez le 015 36 48 48 pour un rendez-vous avec nos experts en sécurisation**