Test rapide de cybersécurité pour PME

Pour les PME qui souhaitent répondre à toutes les questions

Votre entreprise est-elle bien protégée contre les attaques provenant du cyberespace et prête à réagir? Testez maintenant si vous remplissez les normes minimales pour PME.

Les risques de cyberattaques ont tendance à être fortement sous-estimés. C'est ce que révèle une enquête menée en 2017 auprès de dirigeants de PME suisses. La majorité des PME se croient protégées, alors que bien souvent elles n'en font pas assez contre les menaces.

Le présent questionnaire permet à votre entreprise de dresser un état des lieux et vous indique si vous avez mis en place les principales mesures techniques, organisationnelles et humaines visant à garantir au moins une protection de base sur le plan de la cybersécurité. Si vous avez répondu à une ou plusieurs questions par «non» ou «ne sait pas», vous trouverez des compléments d'information destinés aux PME sous le lien www.cybersecurity-check.ch.

	oui	non	ne sait pas
1. Tâches, compétences et responsabilités			
Un responsable de la cybersécurité a-t-il été désigné dans votre entreprise?			
La personne responsable possède-t-elle les connaissances, les compétences et le savoir-faire requis sur le terrain de la cybersécurité et suit-elle régulièrement de la formation continue?			
La personne responsable a-t-elle la position hiérarchique et les compétences nécessaires pour mettre en œuvre des mesures de cybersécurité?			
Y a-t-il des directives visant à une utilisation sûre des appareils informatiques et des données?			
Ces directives ou mesures de cybersécurité sont-elles mises en œuvre de manière cohérente et systématique et font-elles l'objet de contrôles réguliers?			

2. Sensibilisation du personnel, de la clientèle, des fournisseurs et des prestataires			
Existe-t-il dans votre entreprise des directives sur l'utilisation sûre par les collaborateurs des courriels, des données numériques et d'Internet?			
Les collaborateurs connaissent-ils et comprennent-ils les directives?			
Les collaborateurs suivent-ils rigoureusement les directives?			
Les collaborateurs sont-ils régulièrement formés ou sensibilisés à la cybersécurité, par ex. à la manière correcte de traiter les courriels?			
Votre entreprise a-t-elle des échanges sur la cybersécurité avec ses clients et ses fournisseurs? (ceux-ci devraient également effectuer le test rapide).			

	oui	non	ne sait pas
3. Directives sur la protection des données			
Les données sont-elles chiffrées sur vos systèmes (archives numériques, supports de stockage, terminaux, serveurs)?			
Détenez-vous ou traitez-vous des données à caractère personnel (notamment des données concernant la santé, la religion, etc. qui sont particulièrement dignes de protection) sous forme électronique ?			
Connaissez-vous vos devoirs découlant des prescriptions relatives aux données à caractère personnel?			
Les réglementations actuelles en matière de protection des données sont-elles appliquées de manière cohérente et correcte dans votre entreprise?			
Des mesures de protection adéquates sont-elles prévues dans votre entreprise contre l'accès physique de tiers à votre infrastructure (ordinateurs, serveurs, réseau)?			
4. Directives sur les mots de passe et l'administration des utilisateurs			
Y a-t-il dans votre entreprise des directives sur l'usage des mots de passe?			
Y a-t-il des directives systématiquement appliquées pour l'octroi des droits d'administrateur?			
Y a-t-il des directives définissant quels collaborateurs ont accès à quelles données?			
Ces directives sont-elles correctement et systématiquement appliquées?			
5. Protection à jour face aux logiciels malveillants			
Vos appareils sont-ils protégés contre les logiciels malveillants (par ex. antivirus, filtre anti-pourriel)?			
6. Pare-feu configuré et actualisé			
Votre réseau d'entreprise et vos systèmes informatiques sont-ils protégés par un pare-feu?			
Votre pare-feu est-il régulièrement actualisé?			

	oui	non	ne sait pas
7. Mises à jour des appareils et systèmes reliés à Internet (postes de travail, installations de production, systèmes de gestion technique de bâtiments, etc.)			
Utilisez-vous la possibilité de mise à jour automatique des logiciels?			
Au cas où les logiciels de vos appareils ou systèmes ne seraient pas automatiquement mis à jour, leur actualisation est-elle régulièrement assurée (par ex. par le fabricant)?			
Les appareils mobiles utilisés à des fins professionnelles font-ils l'objet de mises à jour régulières?			

8. Réseau local sans fil (WLAN) protégé et crypté			
Votre réseau sans fil est-il crypté et protégé?			
Le réseau sans fil mis à disposition des invités est-il séparé de celui prévu pour les collaborateurs?			

9. Cryptage du trafic de données (par ex. VPN)			
Utilisez-vous de façon générale des liaisons Internet sécurisées et chiffrées de bout en bout?			

10. Sauvegarde des données (backup)			
Utilisez-vous un processus de sauvegarde des données?			
Contrôlez-vous régulièrement l'état de fonctionnement et la lisibilité des copies de sauvegarde?			
Les copies de sauvegarde sont-elles stockées à un endroit séparé (offline)?			

11. Précautions minimales face aux situations d'urgence			
Les mesures d'urgence à prendre en cas d'incident informatique ont-elles été définies?			
Le responsable ou la personne de contact en cas d'incident informatique (dysfonctionnement, cyberattaque, etc.) sont-ils définis et joignables?			

12. Externalisation (outsourcing)			
Si vous avez externalisé des services informatiques: le contrat avec votre partenaire informatique règle-t-il les points 1 à 11 de ce questionnaire?			