Auto-évaluation destinée à la direction d'entreprise

À quel point votre entreprise est-elle bien protégée contre les attaques du cyberespace et y est-elle préparée?

Cette auto-évaluation doit permettre à la direction de l'entreprise de réfléchir aux questions-clés relatives à une cyberprotection minimale. Plus vous cochez de «oui», mieux c'est. Un «je ne sais pas» ou un «non» signifie que vous devriez clarifier la question. Une chose est sûre: les mesures pour se protéger des cyberattaques ne peuvent pas être déléguées à votre personnel, mais doivent être prises et coordonnées par la direction.

Vous trouvez d'autres informations sur www.cybersecurity-check.ch et www.melani.admin.ch

	oui	non	je ne sais pas
Tâches, compétences, responsabilités			
Votre entreprise a-t-elle défini qui est responsable de la cybersécurité?	○	○	○
La personne responsable a-t-elle les connaissances nécessaires en cybersécurité et la capacité de la gérer? Continue-t-elle à se former régulièrement?	○	○	○
La personne responsable a-t-elle la position hiérarchique nécessaire et les compétences spécifiques pour mettre en œuvre les mesures de cybersécurité?	○	○	○
Disposez-vous de directives relatives à l'utilisation sûre des appareils et données informatiques?	○	○	○
Ces directives et les mesures de cybersécurité sont-elles rigoureusement mises en œuvre et régulièrement vérifiées?	○	○	○
Sensibilisation du personnel			
Existe-t-il des directives internes relatives à l'utilisation sûre des courriels, des données numériques et d'internet à l'intention de votre personnel?	○	○	○
Votre personnel connaît-il et comprend-il ces directives?	○	○	○
Votre personnel met-il ces directives rigoureusement et correctement en œuvre?	○	○	○
Votre personnel est-il régulièrement informé et sensibilisé à la cybersécurité, par exemple à l'utilisation correcte des courriels?	○	○	○
Directives de protection des données			
Les données de vos systèmes (dispositifs de stockage et de sauvegarde des données, terminaux, serveurs) sont-elles cryptées?	○	○	○
Avez-vous connaissance des prescriptions légales relatives à la sauvegarde et au traitement des données?	○	○	○
Connaissez-vous vos devoirs résultant des prescriptions sur les données à caractère personnel?	○	○	○
Les prescriptions en vigueur relatives à la protection des données sont-elles rigoureusement et correctement mises en œuvre?	○	○	○
L'accès physique à l'infrastructure des ordinateurs, serveurs et au réseau de votre entreprise est-il correctement protégé contre des tiers?	○	○	○
Directives sur les mots de passe et administration des utilisateurs			
Votre entreprise dispose-t-elle de directives sur l'utilisation des mots de passe?	○	○	○
Existe-t-il des directives définissant qui a accès à quelles données?	○	○	○
Ces directives sont-elles rigoureusement et correctement mises en œuvre?	○	○	○

	oui	non	je ne sais pas
Protection à jour contre les logiciels malveillants			
Vos appareils sont-ils protégés contre des logiciels malveillants (programme antiviral)?	○	○	○
Pare-feu configuré et actualisé			
Le réseau de votre entreprise et ses systèmes informatiques sont-ils protégés par un pare-feu?	○	○	○
Des règles spéciales pare-feu ont-elles été définies (p.ex. restriction géographique)?	○	○	○
Votre pare-feu est-il régulièrement actualisé?	○	○	○
Segmentation du réseau			
Les différents secteurs de votre entreprise, par exemple personnel, comptabilité et production, sont-ils séparés?	○	○	○
Utilisez-vous un ordinateur ou système séparé uniquement pour vos transactions cyberbancaires?	○	○	○
Accès à distance			
L'accès extérieur à l'infrastructure d'ordinateurs, des serveurs et au réseau de votre entreprise est-il protégé (réseau privé virtuel [VPN], authentification à deux facteurs)?	○	○	○
Actualiser les appareils et systèmes liés à internet (p.ex. places de travail, sites de production, gestion technique des bâtiments)			
Utilisez-vous la possibilité d'actualiser automatiquement vos logiciels?	○	○	○
Les appareils et systèmes dont les logiciels ne sont pas automatiquement actualisés sont-ils régulièrement mis à jour, par exemple par le producteur?	○	○	○
Les appareils mobiles utilisés dans l'environnement de votre entreprise sont-ils régulièrement actualisés?	○	○	○
Le système de gestion du contenu (CMS) de votre site internet est-il à jour?	○	○	○
Réseau sans fil (WLAN) sécurisé et crypté			
Votre réseau sans fil est-il crypté et sécurisé?	○	○	○
Existe-t-il un réseau sans fil séparé pour votre personnel et pour vos hôtes?	○	○	○
Backup			
Appliquez-vous un processus de sauvegarde (backup) des données?	○	○	○
Vérifiez-vous régulièrement le fonctionnement et la lisibilité des sauvegardes?	○	○	○
La sauvegarde est-elle stockée de manière séparée (offline) et hors murs (offsite)?	○	○	○
Précautions minimales pour gérer les situations d'urgence			
Avez-vous défini des mesures d'urgence en cas d'incident informatique?	○	○	○
La personne responsable et l'interlocuteur/l'interlocutrice en cas d'incident informatique (p.ex. dysfonctionnement, attaque, etc.) sont-ils définis et disponibles?	○	○	○
Externalisation			
Au cas où vous avez externalisé votre service informatique, le contrat qui vous lie au prestataire comprend-il les points susmentionnés?	○	○	○

Document basé sur le Test rapide de cybersécurité pour PME d'ICTswitzerland et d'autres partenaires, www.cybersecurity-check.ch.
En collaboration avec la Police cantonale bernoise et MELANI.