Sécurité de l'information -10 mesures immédiates	Mesures	Considération
1. Responsabilités	• Définir les responsabilités, y compris le budget • Intégrer et contrôler les prestataires de services externes • Formation continue et rapports réguliers	La sécurité de l'information est l'affaire du chef - au plus tard lorsque l'entreprise est à l'arrêt. Conclure et vérifier les contrats avec les prestataires de services.
2. Sauvegarde et restauration	• Rédiger le concept de sauvegarde • Vérifier si le "temps de récupération" est supportable • Tester régulièrement la restauration	L'assurance-vie d'une PME ! On ne voit si la sauvegarde fonctionne vraiment que lorsque la restauration est réussie. Respectez la règle 3-2-1.
3. Identité et accès	• Définir et vérifier les droits d'accès (en particulier pour les administrateurs) • Gestionnaire de mots de passe et authentification multifactorielle • Accès externe sécurisé	Verrouillage de l'écran en cas d'inactivité, accès à distance, autorisations d'accès, comptes personnels, authentification multifactorielle, VPN ou cryptage.
4. Mises à jour régulières	• Installer les mises à jour de sécurité en temps voulu, en particulier pour l'antivirus. • Installer automatiquement les mises à jour lorsque cela est possible • Tenir compte du cycle de vie des anciens systèmes	Idéalement, les vulnérabilités critiques (CVE) sont surveillées.
5. Sensibilisation et formation	• Formation à la sécurité informatique • Simulations de phishing	La plupart des attaques commencent par un e-mail contenant un lien ou une pièce jointe.
6. Plan d'urgence	• Identifier et prioriser les systèmes les plus importants • Contacts sur papier dans le coffre-fort • Documentation informatique, y compris les mots de passe, sur papier dans le coffre-fort	Une équipe de réponse aux incidents définie peut réduire considérablement le temps de réaction en cas d'urgence, comme une attaque de ransomware.
7. Segmentation du réseau	• Séparer WLAN interne & invité (BYOD pour les employés) • Créer des réseaux différents • Placer les appareils de diagnostic dans un réseau séparé si possible	Les données et systèmes sensibles doivent être isolés sur des réseaux distincts afin de minimiser le risque de fuite de données.
8. Destruction de données	• Élimination des documents papier et des supports de données • Définir le processus de sortie • Supprimer les données des véhicules d'occasion et de service de l'ancien client	Des services de destruction certifiés éliminent les vieux papiers et les anciens supports de stockage électroniques de manière appropriée. Ce que vous n'avez pas, vous ne pouvez pas le perdre.
9. Contrôle des applications	• Droits d'installation limités pour les employés • Créer un inventaire informatique pour les terminaux (mobiles et statiques) et les applications. • Éviter les comptes d'utilisateurs communs	Les dangers tels que les macros Office sont-ils connus ? Éviter les comptes partagés, car les anciens employés peuvent toujours accéder aux données.
10. Assurance cyber	• Protection contre les dommages financiers • Externalisation du savoir-faire en cas d'absence d'expertise dans l'entreprise. • Le catalogue de l'assurance cyber montre déjà la protection de base	Les coûts de récupération, l'interruption des activités et l'extorsion par ransomware.
Amendes et dommages et intérêts en cas de violation de la sécurité	• LPD art. 8 en relation avec l'art. 61 let. c Violation de la sécurité de l'information ; procédure pénale avec amende jusqu'à CHF 250'000 • CO Art. 754 **Responsabilité en dommages-intérêts** des directeurs/administrateurs envers les actionnaires/propriétaires pour violation intentionnelle ou par négligence de leurs obligations.	

Enregistrement avec
Rapport d'expérience
Sur le piratage informatique
(DE)

Sécurité de l'information - 10 mesures immédiates pour les garages ! ; 3 juillet 2024;
Auteurs: Impunix AG – Micha Strässler & Leo Krähenbühl - info@impunix.ch

impunix
datenschutz full-service