Guide pour la sécurité informatique (protection des données)

Un produit de l'Institut Fiduciaire 4.0 de FIDUCIAIRE |SUISSE

État : 29 juillet 2020 - Version 1.0

Contenu

Introduction

Ce guide est destiné aux membres de FIDUCIAIRE|SUISSE et à toutes les PME suisses intéressées. Ce document devrait les aider à analyser leur sécurité informatique et à prendre les mesures nécessaires pour accroître la sécurité des informations dans leur environnement informatique et dans le réseau de l'entreprise.

La ligne de conduite est divisée en différentes mesures de protection, qui peuvent être considérées comme des recommandations et optimisées si cela est nécessaire.

Mesures de protection

Protection par une organisation et des processus appropriés

De quoi s'agit-il ?

En cas d'incident cybernétique, le temps de réaction rapide est un élément clé. C'est pourquoi les mesures organisationnelles nécessaires doivent être prises à l'avance pour pouvoir réagir rapidement et efficacement en cas de besoin.

Quelles mesures dois-je prévoir - Quelle est la procédure à suivre ?

D'un point de vue organisationnel, les risques doivent être identifiés et des solutions doivent être mises en place pour garantir que les opérations soient aussi ininterrompues que possible - Il doit également être possible de terminer les activités si l'informatique ne fonctionne plus complètement ou partiellement. Cela résulte d'une cyber-attaque, mais aussi de pannes de courant, de défaillances d'Internet, d'incendies, etc. Des solutions alternatives ou des systèmes de sauvegarde doivent être envisagés dès le début.

Évaluation des dépendances des processus commerciaux de l'infrastructure informatique - Quelles sont les conséquences d'une impossibilité d'accès aux données ou d'une défaillance du système ? Quelles mesures de prévention puis-je adopter ?

Désignation d'une personne responsable de la sécurité informatique - Tous les employés doivent savoir exactement qui contacter s'ils ont des questions concernant la sécurité (par exemple, s'ils reçoivent un courriel suspect d'un client) ou si un incident concernant potentiellement la sécurité se présente.

Définition de la responsabilité entre l'entreprise et le prestataire de services informatiques en matière de sécurité informatique – Si des services liés à la sécurité (par exemple, le backup) sont externalisés, des contrôles réguliers doivent être effectués pour s'assurer que les mesures soient correctement mises en œuvre. Les contrats de service correspondants ne doivent pas générer de malentendus et toutes les responsabilités doivent être clairement définies.

Création d'un plan d'urgence – Le plan d'urgence préparé guide proprement la personne responsable à travers les tâches prédéfinies en cas d'incident.
Des points doivent être abordés ici, tels que l'identification des systèmes critiques (par exemple, courrier, CRM, clients de la comptabilité, données fiscales, etc,) la mise en route de systèmes de repli (par exemple, infrastructure de remplacement ou planification), la définition des procédures exactes (par exemple, écarter un client du réseau en cas de suspicion de virus) ou la définition précise d'une récupération du système.

Protection par l'implication des collaborateurs (facteur humain)

De quoi s'agit-il ?

Toutes sortes de support technique sont inutiles si les collaborateurs ne sont pas impliqués dans la sécurité informatique. Il est essentiel d'informer les collaborateurs sur les dangers actuels et de définir clairement les règles les plus importantes pour leur comportement.

Quelles mesures dois-je prévoir - Quelle est la procédure à suivre ?

Formation des collaborateurs – Les collaborateurs doivent être sensibilisés en permanence à la sécurité informatique dans la vie professionnelle quotidienne et il faut leur montrer où les problèmes/erreurs possibles peuvent survenir dans l'utilisation de l'internet, du courrier électronique et de l'infrastructure informatique en général. Il est conseillé de proposer aux collaborateurs une formation de base sur des sujets tels que les avantages de la sécurité informatique, les mots de passe et l'utilisation sécurisée de l'internet et du courrier électronique.

Définir une politique de mots de passe – Des règles contraignantes pour les mots de passe sécurisés doivent être définies pour l'entreprise. Une authentification à deux facteurs devrait être utilisée dans la mesure du possible. On peut également montrer aux collaborateurs comment mémoriser des mots de passe complexes.

Protection par des mesures au niveau technique

De quoi s'agit-il ?

La sécurité absolue ne peut être atteinte même avec les mesures techniques. Cependant, des failles de sécurité peuvent permettre à des personnes non autorisées de pénétrer dans votre système ou réseau et de détruire ou manipuler des données. Les mises à jour de sécurité fournies par les fabricants comblent les lacunes de sécurité connues. Si le trafic de données en dehors du réseau de l'entreprise n'est pas crypté, il peut être lu ou même manipulé.

Quelles mesures dois-je prévoir - Quelle est la procédure à suivre ?

Planifier une sauvegarde – Pour prévenir la perte de données, une sauvegarde doit être effectuée au moins une fois par semaine sur un support de données externe, qui est stocké à l'extérieur dans un endroit protégé. Il doit être hors connexion, c'est-à-dire pas dans le réseau. Il est également important de vérifier régulièrement si les données peuvent être restaurées à partir de la sauvegarde.

Utilisation de la protection anti-virus – Tous les postes clients et serveurs doivent être équipés d'une protection antivirus à jour, régulièrement mise à jour et qui effectue des analyses complètes du système.

Mise à jour régulière des applications utilisées – Les applications obsolètes sont la porte d'entrée des logiciels malveillants. Assurez-vous que tous les ordinateurs, serveurs, pare-feux, etc. du réseau sont mis à jour avec les mises à jour de sécurité disponibles, si possible automatiquement ou rapidement après un test préalable dans les meilleurs délais. Les anciens appareils, pour lesquels aucune mise à jour de sécurité n'est plus disponible, ne doivent pas être connectés au réseau de l'entreprise.

Utilisation de firewalls – Chaque ordinateur utilisé doit être doté d'un pare-feu actif. En outre, le réseau de l'entreprise doit être protégé contre l'Internet par un pare-feu supplémentaire. Une grande attention doit être accordée à la configuration correcte du pare-feu et à sa mise à jour régulière.

Utilisation de filtres anti-spam – Les courriers électroniques non désirés doivent être bloqués en utilisant des outils et des configurations appropriés. En général, les courriers électroniques de certains pays peuvent être bloqués ou les pièces jointes potentiellement dangereuses des courriers électroniques peuvent déjà être filtrées par le gateway de messagerie ou le filtre anti-spam.

Application d'une segmentation du réseau – Les ordinateurs du service fiscal, de la comptabilité et des ressources humaines doivent être connectés à un réseau distinct, de sorte qu'ils ne puissent pas être joints les uns par les autres. Il convient également de faire preuve de prudence lors de l'utilisation des partages de réseau, car ils peuvent également servir à diffuser des logiciels malveillants. Renseignez-vous auprès de votre fournisseur de services informatiques à ce sujet.

Désactivation des macros – Cette fonction est utilisée pour automatiser les documents de l'Office. Malheureusement, les macros sont de plus en plus utilisées pour diffuser des logiciels malveillants. Le nouveau format de Microsoft (par exemple docx) ne contient pas de macros. Il est recommandé de travailler avec les produits Microsoft actuels qui prennent en charge les nouveaux formats.

Sécuriser les accès externes – Si les collaborateurs doivent accéder au réseau de l'entreprise lorsqu'ils sont en déplacement, il faut s'assurer que l'accès à distance (par exemple VPN) est utilisé, ce qui nécessite une authentification forte, idéalement à deux facteurs.

Protection du système CMS – si une présence sur Internet avec l'aide d'un CMS est offerte, il faut s'assurer qu'il est à jour.

Protection des données

De quoi s'agit-il ?

Chaque entreprise est responsable de la sécurité du traitement des données personnelles et de la propriété intellectuelle. La perte de données ou les violations de la protection des données peuvent donner lieu à des poursuites pénales, à de lourdes amendes et à une atteinte grave à l'image de l'entreprise.
La nouvelle ordonnance de l'UE sur la protection des données (ODPD) est en vigueur en 2018 et s'applique également en partie aux entreprises suisses.
La protection des données dépend aussi directement de la sécurité informatique, car les criminels peuvent avoir accès à des données sensibles.

Quelles mesures dois-je prévoir - Quelle est la procédure à suivre ?

Traitement des données dans le respect de la loi – Tous les travaux effectués avec les données des clients (acquisition, stockage, conservation, utilisation, modification, archivage et suppression) doivent être protégés de manière adéquate.
Pour la mise en œuvre correcte de l'ODPD pour votre site Internet conformément au droit suisse, veuillez également consulter notre guide de pratique

Protection par l'inclusion de l'entourage

De quoi s'agit-il ?

Si le partenaire d'externalisation, le fournisseur ou le prestataire de services est touché par une attaque de pirates informatiques, cela peut également affecter directement votre entreprise. C'est pourquoi il est important que les mesures de sécurité informatique les plus importantes soient également mises en œuvre par ces entreprises.
Si les services sont sous-traités à un prestataire de services externe, un contrôle précis est nécessaire.

Quelles mesures dois-je prévoir - Quelle est la procédure à suivre ?

Sécurité relative aux services cloud – Le grand avantage des services cloud est qu'il n'est pas nécessaire d'exploiter des infrastructures informatiques coûteuses. C'est également la raison pour laquelle ces services cloud sont très populaires. Toutefois, leur utilisation ne vous dispense pas de la responsabilité de la sécurité informatique. Il convient d'examiner attentivement où les données sensibles sont stockées et comment elles peuvent être protégées de manière exhaustive. Avant de conclure un contrat avec un fournisseur de services dans un cloud, il convient également de vérifier qui a accès aux données, où se situe la souveraineté des données, comment la protection des données est réglementée, etc.

Contrôles lors de l'externalisation de services de sécurité informatique – Avant de coopérer avec un prestataire de services, il convient de vérifier les certificats et la conformité aux mesures de sécurité informatique, et de demander les preuves appropriées.

Vérifier la sécurité informatique du prestataire de services et du fournisseur – Assurez-vous que les exigences de sécurité de votre entreprise sont également respectées dans votre entourage. Il peut s'agir, par

exemple, de règles de sauvegarde, de l'existence d'un plan d'urgence, du respect de directives d'utilisation, de spécifications pour l'administration des utilisateurs, etc.

Checklist

Mesure	oui	non	Ne sait pas
Protection par une organisation et des processus appropriés			
Identification des risques organisationnels			
Évaluation de l'interdépendance des processus d'entreprise			
Définition de la personne responsable de la sécurité informatique			
Définition des responsabilités entre les entreprises et les prestataires de services informatiques externes			
Préparation d'un plan d'urgence			
Protection par l'implication des collaborateurs (facteur humain)			
Formation des collaborateurs			
Définir une politique de mots de passe			
Protection par des mesures au niveau technique			
Prévoir une sauvegarde			
Utilisation de la protection anti-virus			
Mise à jour régulière des applications utilisées			
Utilisation de firewalls			
Utilisation de filtres anti-spam			
Réalisation d'une segmentation du réseau			
Désactivation des macros			
Sécuriser l'accès externe			
Protection du Content Management System			
Protection des données			
Traitement des données dans le respect de la loi			
Protection par l'inclusion de l'entourage			
Sécurité relative aux services cloud			
Contrôles lors de l'externalisation de services de sécurité informatique			
Vérifier la sécurité informatique du prestataire de services et du fournisseur			

Toutes les mesures qui ne sont pas marquées par "Non" ou "Ne sait pas" nécessitent une attention particulière. Veuillez consulter votre prestataire de services informatiques ou nous demander, nous serons heureux de vous aider.

Conclusion / décharge

Ce guide ne prétend pas être complet. Ce document est principalement destiné à vous guider dans le développement de votre propre concept de sécurité informatique afin de protéger votre propre infrastructure au sein de l'entreprise, avec la participation de vos collaborateurs. Car en fournissant des informations consciencieuses aux collaborateurs, un travail préparatoire important peut déjà être effectué. Les précautions techniques et conceptuelles peuvent être aussi bonnes qu'elles le sont, même si le facteur humain dans l'entreprise ne reçoit pas l'attention nécessaire.

Selon le milieu des affaires et la complexité de l'infrastructure informatique, une assurance contre les risques informatiques peut être vérifiée parallèlement à la mise en œuvre de votre propre sécurité informatique.

L'Institut Treuhand 4.0 a rédigé ce guide avec le plus grand soin et dans un effort pour s'assurer que le contenu était correct au moment de la publication. Le guide ne remplace pas les conseils professionnels dans des cas individuels et l'adaptation à la situation concrète. L'exhaustivité et l'exactitude ne sont pas garanties. L'Institut Fiduciaire 4.0 n'est pas tenu de mettre à jour et d'actualiser les lignes directrices. Elle n'assume aucune responsabilité pour les dommages résultant de l'utilisation de ce guide.

Informations complémentaires

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Melde- und Analysestelle Informationssicherung MELANI
ICTswitzerland
Merkblatt für IT-Sicherheit - MELANI
Informationssicherheit im KMU – KMU Portal