TEST RAPIDE DE CYBERSÉCURITÉ POUR PME

Conseils et compléments d'information destinés à assurer une protection minimale

Les explications suivantes indiquent pourquoi les points mentionnés dans le test www.cybersecurity-check.ch sont cruciaux pour assurer une protection minimale sur le terrain de la cybersécurité.
Elles proviennent en majeure partie de deux sources:

- Publication «Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME)», adaptée en 2016 par l'Information Security Society Switzerland (ISSS)[1]
- Informations destinées aux PME publiées par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI sur son portail, y c. sa publication «Sécurité de l'information: aide-mémoire pour PME», actualisée en 2018[2]

Les autres sources sont indiquées comme telles.

[1] www.kmu.admin.ch/dam/kmu/fr/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf.download.pdf/InfoSurance_10_Points_Programme_FR.pdf
[2] www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

1. Tâches, compétences et responsabilités

Si les tâches, les compétences et les responsabilités pour ce qui touche à la sécurité informatique n'ont pas été réglementées, cela indique que le thème de la cybersécurité n'est pas suffisamment pris au sérieux.

Plus du tiers des PME suisses ont déjà été victimes de cyberattaques. Même les petits établissements (restaurants, salons de coiffure, etc.) ne sont pas à l'abri[3]. Beaucoup d'entreprises sous-estiment le risque[4] et ne se protègent pas suffisamment. Pour garantir une protection de base efficace, il est nécessaire de nommer un responsable de la cybersécurité, qui dirige avec compétence le domaine de la sécurité informatique. Les petites entreprises peuvent très bien ici faire appel à des spécialistes externes.

Compléments d'information

ISSS
Cahier des charges des responsables informatiques
Sécurité de l'information des PME, point 1

MELANI
Mesures au niveau organisationnel portant sur la définition des responsabilités
Aide-mémoire pour PME, pp. 2-3

2. Sensibilisation du personnel, de la clientèle, des fournisseurs et des prestataires de services

Les meilleures mesures techniques adoptées contre les cyberrisques ne servent à rien si les collaborateurs ignorent, ne comprennent pas ou appliquent mal les directives sur la cybersécurité et les règles de comportement.

La priorité sera donnée aux formations apprenant à repérer les courriels renfermant des maliciels ou des liens menant à des pages infectées. La plupart des cyberattaques reposent sur de tels courriels. La méfiance s'impose face à tout courriel non sollicité et contenant des annexes ou des liens. Mais il y a aussi des dangers qui se cachent dans d'autres activités simples exécutées par pratiquement tous les employés, qui sont souvent sous-estimées, par exemple si l'on navigue sur Internet, ou si l'on a mal choisi ses mots de passe. Au cas où un maliciel s'infiltrerait dans le système, il peut y avoir de lourdes conséquences financières et même juridiques.

Compléments d'information

ISSS
Promotion des directives auprès des utilisateurs
Sécurité de l'information des PME, point 8

Sensibilisation des collaborateurs
Sécurité de l'information des PME, point 15

MELANI
Comment se protéger?
Règles de comportement
Portail MELANI

[3] Les PME pas assez réactives face à la cybercriminalité, publication du Portail PME du Département fédéral de l'économie, de la formation et de la recherche (DEFR): Lien vers la publication
[4] Cyberrisiken in Schweizer KMUs: Schlussbericht 2017, étude conjointe de l'ASA, de SQS, d'ICTswitzerland, de l'ISSS, de l'UPIC et de la Commission d'experts de la Confédération (en alleand): Lien vers l'étude

3. Directives sur la protection des données

En cas de fuite de données ou de violation des règles sur la protection des données, une entreprise s'expose à des suites pénales, à de lourdes amendes et à un grave dégât d'image. Le cas échéant, son existence même est menacée.

Il incombe à votre entreprise de faire un usage sûr des données confidentielles et à caractère personnel, en respectant notamment la loi sur la protection des données (LPD), la loi sur le droit d'auteur (LDA) et le code des obligations (CO). En dressant une liste d'invités pour un événement festif de votre entreprise, vous collectez déjà des données à caractère personnel, dont vous devez assurer la protection. En outre le nouveau Règlement européen sur la protection des données (RGPD), en vigueur depuis le 25 mai 2018 dans toute l'UE, s'appliquer aussi dans certains cas aux entreprises suisses. Vérifiez sans tarder si la vôtre est concernée et prenez les mesures utiles, car des sanctions pécuniaires élevées sont prévues en cas de violation du RGPD.

Compléments d'information

ISSS
Respect des règles de confidentialité
Sécurité de l'information des PME, point 11

Protection des données électroniques ainsi que des documents sur papier confidentiels
Sécurité de l'information des PME, point 13, 14

Préposé fédéral à la protection des données et à la transparence (PFPDT)
Gestion des données à caractère personnel
Portail du PFPDT

Département fédéral de l'économie, de la formation et de la recherche (DEFR)
Défis liés au RGPD
Portail PME du DEFR

Economiesuisse
RGPD – Votre entreprise est-elle concernée?
Online Check et Fiche d'information

4. Directives sur les mots de passe et l'administration des utilisateurs

Les mots de passe faibles ou utilisés pour des usages différents, d'une part, et une gestion laxiste des droits d'accès ou d'administrateur, d'autre part, constituent de graves risques de sécurité, qu'il serait facile d'éviter.

Apprenez à vos collaborateurs à utiliser des mots de passe robustes et à employer un mot de passe différent pour chaque service. Utilisez un gestionnaire de mots de passe, n'écrivez pas les mots de passe et ne les transmettez jamais à des tiers. Utiliser l'authentification à deux facteurs dans la mesure du possible. Réglez l'accès aux données dans une gestion centrale des utilisateurs que vos collaborateurs connaissent, comprennent et respectent en tout temps. Veillez à ce que chaque utilisateur ne dispose que des droits d'accès nécessaires et à les supprimer lorsque les employés quittent l'entreprise.

Compléments d'information

ISSS
Choix de mots de passe compliqués
Sécurité de l'information des PME, point 6

Protection de l'accès aux données
Sécurité de l'information des PME, point 12

MELANI
Comment se protéger?
Règles de comportement
Portail MELANI

Contrôle des mots de passe
Testez la force de vos mots de passe
Portail Passwortcheck.ch

5. Protection à jour face aux logiciels malveillants

Il est indispensable d'installer un programme antivirus actuel sur chaque appareil informatique, pour bénéficier d'une protection de base contre les virus, les vers et les chevaux de Troie.

Les virus informatiques sont souvent propagés à l'aide de pièces jointes de courriels usurpant l'identité d'expéditeurs connus[5]. Ainsi déguisés, les maliciels peuvent facilement s'introduire dans votre système pour y détruire ou manipuler des données, voire paralyser toute votre infrastructure informatique. Les ordinateurs mal protégés risquent encore d'être utilisés par des cybercriminels pour lancer des attaques ciblées et pour propager des virus. Une telle intrusion constitue une menace non seulement pour votre propre entreprise, mais aussi pour des tiers.

Compléments d'information

ISSS
Mises à jour de l'antivirus
Sécurité de l'information des PME, point 3

MELANI
Comment se protéger?
Logiciel et paramètres
Portail MELANI

Mesures au niveau technique
Aide-mémoire pour PME, pp. 4-5

Liste de logiciels antivirus
Page Web de MELANI

6. Pare-feu configuré et actualisé

L'usage d'un pare-feu performant réduit le risque de cyberattaque. Au même titre que l'antivirus, le pare-feu fait partie de la protection de base de tout appareil informatique. Il est souvent fourni gratuitement avec les programmes antivirus.

Compléments d'information

ISSS
Protection par pare-feu face au trafic Internet
Sécurité de l'information des PME, point 4

MELANI
Comment se protéger?
Logiciel et paramètres
Portail MELANI

Informations sur les pare-feu
Aide-mémoire pour PME, p. 6

[5] Publication de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI sur le thème des maliciels: Lien vers la publication

7. Mises à jour des appareils et systèmes reliés à Internet

Faute de mise à jour des systèmes d'exploitation, des antivirus, des pare-feu et des diverses applications, les failles de sécurité connues peuvent livrer accès à des cybercriminels. Des données risquent d'être détruites ou manipulées, ou votre infrastructure d'être utilisée à des fins criminelles.

Actualisez régulièrement vos ordinateurs et veillez à ce que tous vos logiciels soient régulièrement mis à jour pour combler les failles de sécurité; la consigne vaut aussi pour tous les appareils mobiles utilisés à des fins professionnelles. Utilisez autant que possible les mises à jour automatiques. Définissez la fréquence des contrôles systématiques de tous vos appareils, pour en garantir la sécurité.

Compléments d'information

ISSS
Maintenance des systèmes informatiques
Sécurité de l'information des PME, point 16

Mises à jour régulières de logiciels
Sécurité de l'information des PME, point 5

Protection des appareils portables
Sécurité de l'information des PME, point 7

MELANI
Comment se protéger?
Logiciel et paramètres
Portail MELANI

8. Réseau local sans fil (WLAN) protégé et crypté

Les réseaux sans fil non sécurisés et non chiffrés, ou seulement avec un protocole désuet, sont une proie facile pour des tiers non autorisés et des cybercriminels. Tous les appareils reliés à votre réseau sans fil, avec les données qu'ils renferment, peuvent être espionnés, manipulés et utilisés pour des activités criminelles.

Protégez votre réseau sans fil par un pare-feu, en chiffrant vos connexions et en utilisant des mots de passe forts. Prévoyez un accès séparé destiné à vos clients ou invités.

Compléments d'information

ISSS
Protection par pare-feu face au trafic Internet
Sécurité de l'information des PME, point 4

Verrouillage de l'accès aux appareils portables et cryptage des données transférées
Sécurité de l'information des PME, point 13

CHIP.de (en allemand)
5 conseils pour protéger efficacement son accès à Internet
Page Web de CHIP.de

MELANI
Comment se protéger?
Équipement / Périphériques
Portail MELANI

9. Cryptage du trafic de données (par ex. VPN)

Des informations confidentielles ainsi que des données à caractère professionnel ou personnel risquent de tomber en de mauvaises mains au moment de leur transfert.

Un cryptage fiable de vos communications et des données pendant leur transfert réduit un tel risque.

Compléments d'information

ISSS
Verrouillage de l'accès aux appareils portables et cryptage des données transférées
Sécurité de l'information des PME, point 13

Computerwoche (en allemand)
Méthodes de cryptage des disques durs, des courriels, des données lors des transferts
Page Web de Computerwoche

10. Sauvegarde des données (backup)

Datenverluste sind nicht immer auf kriminelle Handlungen zurück zu führen, bereits ein Wasserschaden kann wichtige Daten und Informationen zerstören. Sichern Sie Ihre Daten regelmässig, um einen dauerhaften Datenverlust zu vermeiden – denn für manche Daten gilt eine gesetzlich vorgeschriebene Aufbewahrungspflicht.

Führen Sie eine regelmässige Datensicherung durch, die Sie an einem externen, geschützten Ort aufbewahren und überprüfen Sie regelmässig, ob sich die Daten von den Sicherheitsmedien zurückspielen lassen. Jedes KMU sollte täglich ein Backup erstellen. Definieren Sie einen Prozess, der regelt, in welchem Turnus Sie bestimmte Daten sichern und halten Sie sich konsequent daran.

Compléments d'information

ISSS
Protection des données à l'aide de backups
Sécurité de l'information des PME, point 2

MELANI
Comment se protéger?
Logiciel et paramètres
Portail MELANI

11. Précautions minimales face aux situations d'urgence

En cas d'incident informatique, il faut pouvoir agir rapidement pour circonscrire les dégâts et limiter ainsi les coûts.

Fixez pour les collaborateurs la conduite à suivre et les mesures à prendre en cas d'urgence. Et à supposer que toute l'infrastructure informatique cesse provisoirement de fonctionner, définissez des solutions de repli afin que les principales tâches puissent continuer d'être assumées. Désignez les personnes de contact, et veillez à ce qu'elles soient joignables en cas d'incident.

Compléments d'information

ISSS
Alimentation sans interruption des ordinateurs
Sécurité de l'information des PME, point 17

Redondance des modules importants
Sécurité de l'information des PME, point 18

Établissement d'un plan d'urgence
Sécurité de l'information des PME, point 19

12. Externalisation (outsourcing)

Vérifiez que les contrats que vous avez conclus avec vos partenaires externes règlent tous les points abordés dans le test rapide.

Vous avez abordé les questions les plus importantes pour une protection minimale en matière de cybersécurité. Vous trouverez une compilation d'informations supplémentaires – spécialement destinées aux PME – sur www.cybersecurity-check.ch.

Impressum

Auteurs:

Umberto Annino (ISSS) | Norbert Bollow (SNV) | Maya Bundt (SVV) | Daniel Caduff (BWL) | Lucius Dürr (SQS) | Xaver Edelmann (SQS) | Andreas Kaelin (ICTswitzerland) | Marcel Knecht (SNV) | Arié Malz (EFD) | Felix Müller (SQS) | Gunthard Niederbäumer (SVV) | Reinhard Niederer (Druckerei AG Suhr) | Peter Reber (SQS) | Daniel Rudin (ISB – MELANI) | Ronald Trap (SNV)

Rédaction:

Annalena Kassner (ICTswitzerland) | Lena Schneider (ICTswitzerland) | Adrian Sulzer (SATW) | Nicole Wettstein (SATW)