ALLIANZ
DIGITALE SICHERHEIT
SCHWEIZ

Guide de cybersécurité pour les PME

Version 2.1 | 8. février 2022

Le présent guide a été conçu pour aider les PME à atteindre un niveau minimal de cybersécurité, et donc à mieux se protéger des cyberattaques les plus fréquentes.

Les PME sont toujours plus souvent la cible de cyberattaques, qui peuvent être lourdes de conséquences. Or quelques mesures importantes garantissent déjà une protection de base face aux cybermenaces. Le présent guide les passe en revue. Formulé dans un langage clair, il propose des actions simples et concrètes – spécifiquement adaptées aux besoins des PME.

Ce guide complète le test rapide de cybersécurité pour PME, dont il reprend la structure thématique. Nous vous recommandons vivement d'effectuer ce test rapide, afin de constater par vous-même si votre entreprise prend suffisamment au sérieux les questions de cybersécurité

Ce guide et le test rapide pour PME qui le précède s'inscrivent dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Un groupe d'experts en a formulé le contenu, en tenant expressément compte des besoins des PME.

Les partenaires qui ont participé à l'élaboration de ce guide s'engagent ensemble afin que les PME suisses, auxquelles il s'adresse, soient en mesure de se protéger de façon optimale contre les cyberrisques. Sur le site internet www.cybersecurity-check.ch vous en apprendrez plus sur ce groupe d'experts.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

ICTSWITZERLAND ISSS Information Security Society Switzerland satw it's all about technology SNV standards connect the world SQS ASA | SVV

Vue D'ensemble

Sécurité dans le domaine de l'organisation et des processus

Pourquoi est-ce si important?

En cas de cyberincident, un bon degré de préparation et une réaction adéquate sont déterminants pour la reprise rapide, le cas échéant, de la marche normale des affaires.

Une réaction rapide et adéquate peut réduire sensiblement les dommages, voire empêcher leur survenance: d'où l'importance d'axer votre organisation sur ces menaces et de définir les processus correspondants – à l'instar de sauvegardes régulières de vos données (*backup*) –, d'accorder les droits d'accès de manière sélective, ainsi que de prévoir un plan d'urgence.

Que puis-je faire?

☐ Protégez vos informations par des **sauvegardes de données** (backup) régulières.

☐ Accordez de l'importance à votre **administration des utilisateurs**.

☐ Établissez un **plan d'urgence**.

Comment procéder?

Protégez vos informations, en définissant une routine de sauvegarde (backup)

- Effectuez au moins une sauvegarde hebdomadaire sur un disque dur externe.
- Stockez les copies de sécurité à un emplacement externe dûment protégé et séparé du réseau (sauvegarde hors connexion, offline backup).
- Contrôlez régulièrement la lisibilité des données de vos supports de sécurité.

Réduisez votre vulnérabilité grâce à une administration des utilisateurs optimale

Une administration des utilisateurs bien conçue compliquera la tâche des criminels qui cherchent à s'emparer de vos données sensibles.

- Créez des comptes séparés (nom d'utilisateur, login) pour les tâches d'administration (données sensibles, système d'information, systèmes) et pour les tâches «normales».
- N'accordez à chaque utilisateur que les droits d'accès absolument nécessaires. C'est l'unique manière d'éviter que des agresseurs se procurent un accès illimité à tous vos systèmes.
- N'utilisez si possible que des comptes personnels (évitez les comptes auxquels plusieurs personnes peuvent accéder avec le même nom d'utilisateur ou mot de passe).
- Déterminez qui peut accéder à certaines applications informatiques ou à des informations spécifiques. Attribuez les droits d'accès sur la base de rôles (p. ex. comptabilité, administration du personnel, secrétariat, administration du système, vente).
- Lors de départs de votre entreprise, verrouillez les comptes d'utilisateur et les données d'accès des personnes concernées.

Adoptez un plan d'urgence, pour faire face à toute situation critique

Élaborez un plan d'urgence, afin de savoir comment procéder en cas de besoin.

- Identifiez vos systèmes critiques (base d'adresses, système de messagerie, calendrier, etc.), ainsi que les données personnelles et les données de clients en votre possession.
- Consignez qui utilise quel système (noms et numéros de téléphone).
- Définissez des solutions de repli (fourniture d'ordinateurs de remplacement; équipement de tous les postes de travail avec au moins deux navigateurs; accord avec les fournisseurs précisant leur temps de réaction et leurs délais de livraison).
- Définissez la première réaction à adopter en cas d'incident: désactivez les connexions réseau (câble, accès au réseau local sans fil, WLAN) des systèmes touchés.
- Définissez des mesures permettant une récupération rapide de vos systèmes.
- Définissez les compétences et les rôles, autrement dit qui doit être informé et comment en cas d'incident (p. ex. demande de rançon ou panne d'un système critique):
    - personne/société chargée de réparer la panne informatique;
    - personne/société responsable des mesures immédiates à prendre sur le plan juridique. En cas par exemple de fuite de données personnelles, il est recommandé de prendre contact avec un service juridique ou un juriste;
    - personne/société responsable des mesures urgentes de communication;
    - personne chargée d'annoncer l'incident: elle informera le poste de police le plus proche, ainsi que la Centrale d'enregistrement et d'analyse pour la sûreté de l'information www.melani.admin.ch. En cas de cyberfraude entraînant un dommage financier, il est vivement recommandé d'alerter la banque, la police ou une entreprise spécialisée, afin de stopper les éventuels paiements effectués.
- Entraînez le plan d'urgence dans votre entreprise.

Sécurité grâce au facteur humain

Pourquoi est-ce si important?

Malgré tous les moyens techniques déployés, ce sont en définitive les employés qui jouent un rôle-clé dans la sécurité de votre entreprise: d'où l'importance que tous vos collaborateurs et vous-même connaissiez les dangers actuels, et que vous sachiez vous servir des moyens techniques à votre disposition, tout en respectant les règles essentielles.

Que puis-je faire?

☐ **Sensibilisez** les collaborateurs dans leur quotidien professionnel.

☐ Veillez par des **mots de passe sûrs** à une protection optimale des applications.

☐ Définissez des **directives visant** à une utilisation sûre d'Internet et des courriels.

Comment procéder?

Faites de la sécurité une priorité, grâce à la sensibilisation

- Parlez régulièrement des questions de sécurité, notamment du comportement réfléchi sur Internet que vous attendez dans votre entreprise.
- Organisez pour vos collaborateurs une formation de base ayant la teneur suivante:
    - À quoi sert la sécurité informatique?
    - Qu'est-ce qui caractérise les mots de passe robustes? (voir plus loin)
    - Qu'implique une «utilisation sûre» d'Internet et des courriels? (voir plus loin)

Des mots de passe complexes, pour une protection optimale de vos applications

- Choisissez des mots de passe sûrs, et donc privilégiez des mots de passe d'au moins douze signes.
- Utilisez un gestionnaire de mots de passe, avec des mots de passe générés automatiquement.
- Comme variante, utilisez une phrase secrète (passphrase): choisissez une phrase que personne ne pourra aisément deviner. Puis retenez la première ou les deux premières lettres de chaque mot, qui constitueront votre mot de passe. Évitez pour votre phrase secrète les titres de livres ou les tournures courantes, etc.

- Ne réutilisez pas vos mots de passe, et donc employez un mot de passe différent par service utilisé (compte de messagerie, e-banking, logiciel de comptabilité, applications CRM, etc.).
- Privilégiez toujours l'authentification à deux facteurs (p. ex. Google Authenticator).
- Modifiez les mots de passe impersonnels quand des collaborateurs quittent l'entreprise.

Directives visant à une utilisation sûre d'Internet et des courriels

Formulez des directives visant à une utilisation sûre d'Internet et des courriels. Elles traiteront notamment les points suivants:

- Ne révélez en aucun cas à des tiers vos données d'ouverture de session (nom d'utilisateur et mot de passe).
- N'indiquez votre numéro de carte de crédit que sur des sites dignes de confiance, en veillant par exemple à ce que l'adresse affichée dans le navigateur comporte le préfixe https://.
- Ne téléchargez jamais de programme inconnu depuis Internet.
- Utilisez votre smartphone plutôt qu'un réseau public non protégé comme point d'accès sans fil. Cette règle vaut tout particulièrement pour l'e-banking. Les connexions à distance non protégées sont peu sûres, et donc il existe un risque que des tiers interceptent vos données.
- Faites preuve de méfiance chaque fois que vous recevez un courriel, et veillez notamment aux points suivants:
    - Si vous recevez des courriels suspects (adresse de l'expéditeur, fautes d'orthographe, ton employé, logos, etc.), n'ouvrez pas les documents ou programmes annexés et ne cliquez pas non plus sur les hyperliens indiqués.
    - En cas de doute, ne divulguez jamais d'informations confidentielles, mais cherchez à prendre contact avec l'expéditeur d'une autre manière (p. ex. par téléphone), afin de savoir si le courriel reçu est digne de confiance.
    - Examinez d'un œil critique même les messages émanant de personnes que vous connaissez ou de membres de la direction de votre entreprise. Il se pourrait que des escrocs aient accédé à leur compte de messagerie et expédié des courriels en leur nom.

La sécurité grâce à des mesures techniques adéquates

Pourquoi est-ce si important?

Des personnes non autorisées sont susceptibles de s'introduire dans vos systèmes, en tirant parti de leurs failles de sécurité. Elles pourront ainsi effacer ou manipuler des données, ou se servir de votre infrastructure informatique à des fins criminelles. Les mises à jour logicielles comblent de telles vulnérabilités.

Un pare-feu à jour protégera votre ordinateur de tout accès non autorisé. En outre, un antivirus actuel vous protège contre les virus, les vers et les chevaux de Troie.

Des escrocs sont susceptibles de lire, voire de manipuler vos échanges de données, si votre communication n'est pas chiffrée.

Que puis-je faire?

☐ Utilisez des **logiciels** adéquats (p. ex. pare-feu, antivirus) pour renforcer votre sécurité.

☐ Veillez à **actualiser régulièrement** vos logiciels.

☐ Ne raccordez jamais à Internet les **appareils désuets**, pour lesquels il n'existe plus de mise à jour

logicielle.

Comment procéder?

Renforcez votre sécurité par des moyens techniques adéquats (logiciels et matériel)

- Actualisez régulièrement vos systèmes d'exploitation, votre pare-feu et vos autres applications.
- Vérifiez régulièrement si des mises à jour sont disponibles pour votre ordinateur, et installez-les pour combler les lacunes de sécurité.
- Activez autant que possible les fonctions de mise à jour automatique. Faites de même pour tous vos logiciels, ainsi que pour vos appareils reliés à Internet (imprimantes et autres équipements, solutions domotiques, appareils électroménagers, smartphones, etc.).
- Déconnectez d'Internet les appareils pour lesquels aucune mise à jour n'est fournie, ou mettez-les hors service.
- Installez un antivirus à jour et actualisez-le régulièrement (les mises à jour sont en général automatiques). Un test de Ktipp de mai 2019 recommande en particulier les antivirus «Internet Security» de Bitdefender ou de Kaspersky, ainsi qu'«Antivirus Pro» d'Avira. Le produit gratuit proposé par Avast a également obtenu un bon résultat lors de ce test.
- Protégez votre communication par une bonne solution de cryptage (p. ex. réseau privé virtuel, virtual private network, VPN).

Cybersécurité et protection des données

Pourquoi est-ce si important?

Il incombe à votre entreprise de faire un usage sûr des données personnelles, en respectant le droit à la propriété intellectuelle d'autrui. En cas de fuite de données ou de violation des règles sur la protection des données, elle s'expose à des suites pénales, à de lourdes amendes et à un grave dégât d'image. Le cas échéant, l'existence même de votre entreprise peut être menacée.

Le nouveau Règlement général sur la protection des données (RGPD), en vigueur depuis 2018 dans l'UE, concerne aussi dans certains cas les entreprises suisses. Ainsi, les sociétés ou sites Internet suisses qui traitent des données de citoyens de l'UE, ou qui offrent des biens ou des services à ces personnes,

relèvent aussi de son champ d'application. Le RGPD s'applique aussi aux sites Internet qui utilisent des *cookies* pour analyser les habitudes de navigation de leurs visiteurs en provenance de l'UE.

La cybersécurité fait partie intégrante de la protection des données: en lançant une cyberattaque, des criminels peuvent s'emparer de données sensibles.

Que puis-je faire?

☐ En adoptant des mesures de cybersécurité, vous contribuerez au respect de la loi sur la protection des données, à laquelle votre PME est soumise.

Comment procéder?

Traitez les données de manière conforme à la loi sur la protection des données

- Dès que vous traitez d'une quelconque manière des données de personnes (p. ex. clients ou collaborateurs), vous devez les protéger suffisamment (ou vous limiter à leur collecte).
- On entend par traitement, toute opération relative à des données personnelles, notamment la collecte, l'enregistrement, la conservation, l'exploitation, la modification, la communication, l'archivage, l'effacement ou la destruction des données.
- Vérifiez si le RGPD s'applique à votre PME: Online-Check d'economiesuisse; fiche d'information

La sécurité grâce à un environnement adéquat

Pourquoi est-ce si important?

Si un de vos fournisseurs ou prestataires est victime d'une cyberattaque, vous risquez d'en faire les frais, par exemple si des données de vos propres clients sont perdues. Il est donc important que les tiers avec lesquels vous collaborez mettent aussi en œuvre les principales mesures de cybersécurité.

Si vous externalisez votre sécurité informatique à un tiers, il est important de le surveiller de près et de préciser avec lui les points essentiels.

Que puis-je faire?

☐ Exigez de vos **partenaires externes (en cas de sous-traitance) et de vos fournisseurs** qu'ils prennent au moins certaines mesures en matière de cybersécurité.

☐ En cas d'externalisation de **prestations de sécurité informatique**, contrôlez les certificats de vos partenaires et assurez-vous qu'ils respectent les principales mesures de sécurité.

Comment proceder?

Imposez en dehors de votre entreprise également, à vos partenaires externes et à vos fournisseurs, le respect de vos exigences de sécurité

Effectuez avec vos fournisseurs ou prestataires de services (sous-traitants) le test rapide de cybersécurité, et assurez-vous qu'eux aussi remplissent les exigences fixées pour votre entreprise. Vérifiez notamment les points suivants:

- Des sauvegardes (backup) sont-elles régulièrement effectuées et les copies de sécurité sont-elles conservées à un emplacement externe?
- Un plan d'urgence a-t-il été défini?

- Des prescriptions en vue d'une utilisation sûre d'Internet ont-elles été définies et sont-elles respectées?
- Des directives existent-elles pour l'administration des utilisateurs?
- Les collaborateurs sont-ils sensibilisés au thème de la cybersécurité (p. ex. courriels de phishing, emploi de mots de passe sûrs)?
- Les systèmes d'exploitation, le pare-feu et les autres applications font-ils l'objet de mises à jour régulières?
- La communication est-elle cryptée?
- Un antivirus est-il utilisé et fait-il l'objet de mises à jour régulières?

Sécurité en cas d'externalisation: rôle des fournisseurs de sécurité informatique

Assurez-vous que votre fournisseur de sécurité informatique satisfasse à vos principales exigences: parcourez avec lui le test rapide, ou vérifiez s'il possède un certificat (p. ex. ISO 27001).

À quoi nous référons-nous ?

Références et compléments d'information

MELANI: Sécurité de l'information: aide-mémoire pour PME

MELANI: Mesures de protection de base

ISSS: Sécurité informatique des PME

BNC: Cybersecurity und Datenschutz

PFPDT: Protection des données

Tagblatt: Datenschutzgesetz

kTipp: Antiviren-Software

UBS: Phishing