Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Unité de pilotage informatique de la Confédération UPIC

Centrale d'enregistement et d'analyse pour la sûreté de l'information MELANI

Sécurité informatique: aide-mémoire pour les PME

MELANI / GovCERT.ch

Version:	v1.03
Auteur:	MELANI / GovCERT.ch
Dernière modification:	24 juillet 2016

[1] http://creativecommons.org/licenses/by-nd/3.0/

Introduction

Le présent aide-mémoire a été conçu pour les PME suisses, afin de les aider à accroître la sécurité informatique de leurs réseaux d'entreprise.

Cet aide-mémoire s'articule en deux parties:

- mesures à prendre au **niveau organisationnel** pour renforcer ou garantir la sécurité informatique;
- mesures à prendre à cet effet au **niveau technique**.

Nous tenons à souligner qu'à elles seules, les mesures techniques ne suffisent pas à garantir la sécurité informatique d'un réseau d'entreprise. Des mesures organisationnelles s'avèrent également à chaque fois nécessaires. Dans le cas des mesures onéreuses ou mobilisant d'importantes ressources, chaque entreprise, plus précisément sa direction, doit trouver un juste équilibre entre le coût d'une telle mesure et les risques encourus en ne la réalisant pas. Autrement dit, la direction doit décider soit de supporter les risques en question, soit de fournir les ressources utiles pour les réduire au minimum.

Mesures au niveau organisationnel

Les mesures organisationnelles visent à garantir que l'entreprise ait défini à qui incombe la **responsabilité** des questions de sécurité informatique.

Au niveau organisationnel, il convient d'adopter les mesures suivantes:

- **Assurez-vous que les responsabilités soient bien réglées pour tout ce qui touche à l'informatique, en particulier à la sécurité informatique.** Il faut par ex. préciser à qui les collaborateurs doivent s'adresser en cas de question touchant à la sécurité informatique (par ex. en cas de réception d'un courriel suspect) ou qui doit être informé des incidents touchant à la sécurité informatique.

- **Formez régulièrement vos collaborateurs à se servir de l'infrastructure informatique en respectant les prescriptions de sécurité**. Vous trouverez sur notre site Web des règles de comportement utiles pour la navigation sur Internet:

  Règles de comportement:
  https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.html

- **Assurez-vous que les compétences soient clairement réglées entre votre fournisseur de services informatiques et vous, sur le plan de la sécurité informatique.** Les mesures techniques – sauvegardes externes, protection contre les virus, fichiers journaux – sont surtout concernées ici. Vérifiez régulièrement le respect des mesures prévues, au besoin en faisant appel à un tiers (prestataire spécialisé). Précisez encore dans votre contrat que toute négligence en matière de sécurité informatique aura des conséquences (responsabilité en cas de dommage).

- **Réexaminez régulièrement les risques actuels dans le domaine de la sécurité de l'information, et présentez-les à la direction.** Dans ce contexte, surveillez la dépendance de vos processus d'affaires face à votre infrastructure informatique, par ex. les effets que pourraient avoir la panne prolongée d'un système spécifique ou l'impossibilité d'accéder à un serveur de données.

- **Définissez une politique des mots de passe et mettez-la en œuvre sur le plan technique** (par ex.: changement de mot de passe tous les trois mois, au moins douze signes dont à chaque fois des lettres, des chiffres et des caractères spéciaux).

- **Exploitez les restrictions prévues par votre application e-banking.** Selon les circonstances, vous pouvez désactiver ou limiter certaines fonctions n'étant pas indispensables. Vous pouvez discuter des possibilités existantes avec votre banque, par exemple d'éventuelles limitations par pays.

- **La plupart des systèmes e-banking offrent des possibilités de contrats collectifs.** Dans ce cas, un virement devra être validé par un deuxième utilisateur. Vous pouvez discuter des possibilités existantes avec votre banque. Tous les processus liés au trafic des paiements devraient faire l'objet de règles internes précises, et les collaborateurs s'y tenir dans tous les cas.

N'oubliez en outre jamais qu'en tout état de cause, les risques informatiques relèvent de la responsabilité de la direction. Il est exclu de les déléguer.

Mesures au niveau technique

Les mesures techniques permettent certes de réduire le risque d'infection par un logiciel malveillant et d'accroître la sécurité informatique dans le réseau d'entreprise. Mais elles ne procurent jamais une sécurité à 100 %. Car bien souvent, ce n'est pas la technique, mais l'utilisateur qui constitue le maillon faible de la chaîne. S'il n'a pas reçu d'instructions pour utiliser prudemment les systèmes informatiques, bien des mesures techniques susmentionnées ne servent à rien.

Au niveau technique, il convient d'adopter les mesures suivantes:

- **Assurez-vous qu'un antivirus soit installé sur chaque ordinateur.** Veillez aussi à ce qu'il soit régulièrement actualisé (configuration des mises à jour)) et que des analyses complètes du système soient régulièrement faites (par ex. chaque semaine ou tous les mois).

- **Assurez-vous qu'une sauvegarde de toutes les données soit faite régulièrement (tous les jours).** Vérifiez ponctuellement que ces mises à jour puissent être utilisées. Conservez les sauvegardes dans un lieu sûr (*offline*). Veillez à conserver les versions antérieures des sauvegardes pendant un temps défini.

- **Les fichiers journaux (*logfiles*) sont essentiels pour la reconstitution d'un incident informatique.** Assurez-vous que les systèmes critiques, comme les logiciels de comptabilité, les contrôleurs de domaine, les pare-feu ou les serveurs de messagerie tiennent de tels fichiers journaux. Il est recommandé de les contrôler régulièrement pour y détecter d'éventuelles anomalies. Conservez vos fichiers journaux pendant au moins six mois, et veillez à les inclure dans vos sauvegardes.

- **Travaillez selon le principe du droit d'accès minimal (*least privilege*)[2].** Il convient de n'octroyer aux collaborateurs que les droits d'accès dont ils ont besoin pour accomplir les tâches leur étant confiées. Les collaborateurs ne devraient pas jouir par défaut de droits d'administrateur.

2 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04247.html

- **Segmentez votre réseau.** Comme précaution minimale, les ordinateurs de la comptabilité devraient faire partie d'un réseau séparé et ne pas être accessibles depuis les autres ordinateurs de votre réseau.

- **Utilisez un filtre anti-pourriel.** Il existe de nombreuses possibilités de bloquer les courriels indésirables. Si par ex. votre entreprise n'est active qu'en Suisse, une option consisterait à refuser les courriels provenant de pays spécifiques (connus pour relayer de nombreux pourriels).

- **Veillez à bloquer ou filtrer la réception de courriels contenant des fichiers potentiellement dangereux sur votre passerelle de messagerie ou filtre antispam.**
  Sont dangereux notamment les fichiers :
  .js (JavaScript)
  .jar (Java)
  .bat (Batch file)
  .exe (Windows executable)
  .cpl (Control Panel)
  .scr (Screensaver)
  .com (COM file)
  .pif (Program Information File)
  .vbs (Visual Basic Script)
  .ps1 (Windows PowerShell)
  .wsf (Windows Script File)
  .docm (Microsoft Word avec macros)
  .xlsm (Microsoft Excel avec macros)
  .pptm (Microsoft PowerPoint avec macros)

- **Veillez à ce que ces fichiers soient également bloqués lorsqu'ils sont envoyés à votre entreprise dans un fichier d'archive tel qu'un fichier ZIP ou RAR** ou dans un fichier d'archive protégé (par exemple un ZIP protégé par un mot de passe).

- **Par ailleurs, il est recommandé de bloquer tous les fichiers joints contenant des macros** (par ex. fichiers Word, Excel ou PowerPoint contenant des macros).

- **Utilisez un pare-feu sur chaque ordinateur.** Protégez en outre votre réseau d'entreprise des dangers d'Internet par un pare-feu supplémentaire. Ce pare-feu devrait par défaut refuser tout le trafic entrant ou sortant, en dehors du trafic expressément autorisé (par une règle de pare-feu).

- **Si vous avez prévu un accès à distance (par ex. RAS, VPN), assurez-vous qu'il soit fortement sécurisé**, par ex. par un deuxième facteur d'authentification (mot de passe unique, jeton SMS, etc.).

- **Définissez une politique des mots de passe et concrétisez-la par des moyens techniques.**

- Les logiciels désuets sont une cible de choix des maliciels. **Veillez à ce que tous les ordinateurs et les serveurs de votre réseau installent automatiquement les mises à jour (activation des mises à jour automatiques).** Corrigez également régulièrement les lacunes de sécurité des logiciels de tiers, comme par ex. Adobe Reader, Adobe Flash, Java, etc.

- **N'utilisez qu'avec retenue les services de stockage dans le nuage (*cloud*)**. Les

données sensibles ne devraient jamais se trouver dans le nuage, mais être sauvegardées au niveau local exclusivement.

- **Veillez à chiffrer les données importantes, en particulier lors de l'utilisation de services *cloud* ou sur des appareils mobiles**.

- Si votre entreprise possède un site Web, **assurez-vous le cas échéant que votre système de gestion de contenu (Content Management System, CMS) soit toujours à jour.** Utilisez un pare-feu pour les applications web (*web application firewall, WAF)* pour protéger votre site contre les cyberattaques. Notre site Web publie une liste des mesures servant à protéger les CMS:

  Mesures de prévention pour les systèmes de gestion de contenu (CMS)
  https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

MELANI recommande en outre, en cas d'infection par un virus ou de soupçon dans ce sens, de réinstaller l'ordinateur concerné (réinstallation du système d'exploitation). Cette précaution évite que des résidus de maliciels n'infectent à nouveau l'ordinateur. Il y a d'ailleurs de fortes chances qu'une analyse du système n'identifie et n'élimine pas tous les maliciels. Une réinstallation est donc à chaque fois la meilleure solution.

Liens vers des compléments d'information

- Règles de comportement pour la navigation sur Internet
  https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.html

- Mesures de prévention pour les systèmes de gestion de contenu (CMS)
  https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

- Portail PME de la Confédération: Sécuriser son infrastructure électronique
  https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/infrastructure-ti/infrastructure-technologie-information-ti/infrastructure-securite-ti.html