Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Secrétariat général

Centre national pour la cybersécurité NCSC
www.ncsc.admin.ch

NCSC

Sécurité de l'information: aide-mémoire pour PME

Table des matières

Introduction **2**

Mesures organisationnelles **2**
Mesures techniques **4**

Introduction

Le présent aide-mémoire a été conçu pour les PME suisses afin de les aider à accroître la sécurité de l'information au sein de leur entreprise[1].

Cet aide-mémoire s'articule en deux parties:

- les **mesures organisationnelles** qui augmentent ou garantissent la sécurité de l'information;
- les **mesures techniques** qui renforcent ou garantissent la sécurité de l'infrastructure informatique.

Les mesures techniques contribuent de manière essentielle à garantir la sécurité de l'information, mais elles doivent être complétées par des mesures d'organisation. En particulier en cas de mesures onéreuses et/ou mobilisant beaucoup de personnel, chaque entreprise doit trouver un juste équilibre entre le coût de ces mesures et les risques encourus en ne les réalisant pas. Les mesures qui ne sont pas mises en œuvre laissent ce que l'on appelle des risques résiduels. C'est pourquoi la direction doit décider de supporter ces risques résiduels ou de fournir les ressources utiles pour continuer à les réduire. Or même si les risques techniques des systèmes informatiques constituent un volet important de la sécurité de l'information, une entreprise ne devrait pas limiter son attention à cet aspect des risques et encore moins considérer que les risques sont du seul ressort de son service informatique. En effet, la responsabilité en matière de gestion des risques, la classification des informations et leur hiérarchisation, avec le cas échéant un déploiement plus ou moins grand de mesures de sécurité, sont autant de tâches fondamentales de la direction.

Mesures organisationnelles

Les mesures organisationnelles visent à garantir que l'entreprise ait défini à qui incombe la responsabilité des questions touchant à la sécurité de l'information:

Information de la direction concernant les risques
Surveillez la dépendance de vos processus d'affaires face à votre infrastructure informatique. Quels effets pourraient avoir la défaillance d'un système spécifique ou l'impossibilité d'accéder à un serveur de données? À quelles conséquences financières faut-il s'attendre? Quelles mesures vous permettraient d'y faire face?

Prise en compte des risques au niveau du gouvernement d'entreprise et de la gestion de la continuité
Les travaux nécessaires doivent pouvoir être effectués même quand toute l'infrastructure informatique ou une partie de cette infrastructure cesse provisoirement de fonctionner. Cela n'est pas toujours dû à une cyberattaque. Une panne électrique, un événement naturel ou d'autres scénarios encore peuvent provoquer une défaillance complète ou partielle de votre informatique. Définissez de bonne heure les alternatives possibles, et/ou les solutions de repli de chaque système.

Définition des responsabilités
Les collaborateurs doivent savoir à qui 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. Prévoyez assez tôt un plan de réponse aux incidents de sécurité. Contrôlez régulièrement l'efficacité du plan, par exemple avec des exercices, et adaptez-le en fonction des résultats de ces exercices.

[1] Voir aussi: «Informatique, sécurité TI et infrastructure: conseils», sur le Portail PME de la Confédération: https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/infrastructure-ti.html

Compétences de l'entreprise et du fournisseur de services informatiques
Beaucoup de petites entreprises externalisent leur informatique à des prestataires spécialisés. Les compétences respectives de l'entreprise et des fournisseurs de services informatiques doivent être clairement réglées. Précisez dans votre contrat les questions relatives à la responsabilité en cas de non-respect des consignes de sécurité ou de toute autre négligence en matière de sécurité informatique. Assurez-vous que le contrat est formulé de manière claire et sans équivoque. Si, par exemple, aucune sauvegarde des données n'est effectuée en raison d'un malentendu, les conséquences peuvent être catastrophiques.[2]

Sensibilisation des collaborateurs
Il est primordial de sensibiliser tous les collaborateurs au bon usage de l'infrastructure informatique. Formez régulièrement votre personnel aux dangers potentiels du monde numérique et incitez-le à la prudence concernant les courriels et la navigation sur Internet. Vous trouverez sur notre site Web des règles de comportement utiles.

Connaissance de la situation actuelle de la menace
Tenez-vous au courant des nouvelles menaces en matière de sécurité de l'information et des mesures permettant d'y faire face[3].

Traitement des données sensibles
Édictez des règles obligatoires pour la classification des données et veillez à ce qu'elles soient scrupuleusement respectées. Définissez en particulier la manière dont les données classifiées doivent être mémorisées et/ou transmises sous forme électronique[4]. Élaborez des directives pour la transmission des informations de l'entreprise. Aucune information confidentielle ne devrait en principe être transmise par l'intermédiaire de canaux anonymes (par ex. par téléphone ou par courriel).

Informations sur l'entreprise disponibles en ligne
Les criminels cherchent régulièrement des informations sur des victimes potentielles. C'est pourquoi il convient de réfléchir sérieusement aux informations que vous souhaitez diffuser par exemple sur votre site Web ou sur les réseaux sociaux. Réduisez au minimum la quantité d'informations sur votre entreprise qui sont disponibles sur Internet. Soupesez les avantages et les risques des informations disponibles. Élaborez des directives quant à la manière dont vos collaborateurs doivent par exemple procéder concernant les informations de l'entreprise dans le cadre de l'utilisation privée des réseaux sociaux.

Sécurité, de l'achat à la mise au rebut de l'infrastructure informatique
Les considérations de sécurité devraient toujours être dûment intégrées au processus d'achat. Au-delà de la mise en service, il faut envisager ici tout le cycle de vie d'un système, y compris sa maintenance et sa mise hors service. Informez-vous en particulier avant l'achat par exemple pour savoir pendant combien de temps les mises à jour de sécurité sont disponibles. Sont-elles automatiquement installées? Comment saurez-vous que de nouvelles mises à jour sont disponibles? Définissez la procédure de mise hors service de certaines parties de la structure informatique (par ex. comment éliminer de manière fiable des informations confidentielles des systèmes concernés).

---

[2] Pour plus d'informations, voir la collaboration avec les prestataires informatiques: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html

[3] Tous les six mois, le NCSC revient sur les principaux cyberincidents observés en Suisse et sur le plan international dans le cadre de son rapport semestriel. Les cinq menaces les plus importantes sont également régulièrement actualisées sur le site Web du NCSC.

[4] Des recommandations ainsi que les ordonnances relatives à la protection des données sont publiées sur le portail du Préposé fédéral à la protection des données et à la transparence (PFPDT): https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/generalites/protection-des-donnees.html.

Politique des mots de passe
Définissez des règles de mots de passe obligatoires, et mettez-les systématiquement en œuvre. Les mots de passe doivent comprendre au moins douze signes, dont des majuscules et des minuscules, des chiffres et des caractères spéciaux. Prévoyez autant que possible une solution d'authentification à deux facteurs. Évitez impérativement d'utiliser plusieurs fois le même mot de passe. Utilisez un gestionnaire de mots de passe et créez un mot de passe différent pour chaque application. Vous trouverez sur le marché plusieurs systèmes de gestion de mots de passe pour les différents systèmes d'exploitation et appareils. Certains programmes sont gratuits et d'autres sont soumis à une licence. Ne transmettez jamais vos mots de passe et vos données d'accès à qui que ce soit.

Autorisations d'accès
Très peu de collaborateurs ont besoin de droits d'administrateur étendus. N'octroyez aux collaborateurs que les droits d'accès dont ils ont absolument besoin pour accomplir leur travail (les collaborateurs du marketing, par exemple, n'ont pas impérativement besoin d'avoir accès aux informations du service du personnel). En particulier, vous devriez leur refuser les droits permettant d'installer n'importe quel logiciel.

E-banking
Utilisez pour tous les ordres de paiement numériques (logiciel de paiement hors ligne; e-banking) un ordinateur dédié avec lequel vous ne surfez pas sur Internet ni ne recevez de courriels. Définissez l'ensemble des processus qui concernent le trafic des paiements et respectez-les systématiquement (double contrôle, signature collective, etc.). Ce principe s'applique en particulier lorsque plusieurs collaborateurs sont autorisés à faire des paiements. Il est parfois possible de désactiver ou de limiter les fonctions non indispensables dans votre application e-banking. Discutez avec votre banque des mesures de sécurité possibles, par exemple concernant d'éventuelles restrictions par pays.

Mesures techniques

Les mesures techniques ne procurent jamais une sécurité à 100 %. Bien souvent, ce n'est pas la technique, mais l'utilisateur qui constitue le maillon faible de la chaîne. Si les collaborateurs n'ont pas été formés pour utiliser les systèmes informatiques avec prudence, cela peut avoir un impact considérable sur l'efficacité des mesures techniques décrites ci-après. Mais une combinaison judicieuse de différentes mesures techniques contribue de façon décisive à la sécurité informatique du réseau d'entreprise et réduit le risque d'infection par des maliciels.

Sauvegarde régulière des données
Définissez un processus de sauvegarde régulière des données (backup), et respectez-le scrupuleusement. Vous pouvez confier la sauvegarde de vos données et d'autres mesures techniques à un prestataire spécialisé.

Vérifiez ponctuellement que les sauvegardes des données peuvent être utilisées. Exercez-vous de temps à autre à restaurer les données sauvegardées, afin de vous sentir à l'aise avec le processus le jour où vous en aurez besoin.

La copie de sauvegarde devrait être mémorisée hors ligne, c'est-à-dire sur un support externe comme par exemple un disque dur externe. Après le backup, veillez à déconnecter de l'ordinateur le support contenant les données sauvegardées, faute de quoi ces données risqueraient d'être elles aussi cryptées et rendues inutilisables en cas d'infection de l'ordinateur par un rançongiciel. Conservez également les anciens backups pendant un certain temps.

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

Pare-feu
Utilisez un pare-feu sur chaque ordinateur. Protégez en outre votre réseau d'entreprise des dangers d'Internet par un pare-feu supplémentaire. Définissez au moyen de règles du pare-feu le trafic entrant ou sortant autorisé. Faites passer les protocoles prenant en charge des serveurs proxy, comme HTTP/HTTPS, etc. par un proxy. Analysez régulièrement les fichiers journaux du proxy.

Mises à jour de sécurité
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 de sécurité. Tous les logiciels installés doivent être régulièrement actualisés dès que des mises à jour de sécurité sont disponibles. Le matériel utilisé, à l'instar des imprimantes, routeurs, etc. doit lui aussi être actualisé.

Systèmes de gestion de contenu (CMS)
Les systèmes de gestion de contenu (*Content Management System*, CMS) pour la création et l'actualisation de sites Internet doivent toujours être à jour. La plupart des CMS offrent une fonction de mise à jour automatique facile à activer. 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[5]. Si votre entreprise est largement tributaire de son site Internet (par ex. boutique en ligne), vous devriez réfléchir à la manière de gérer une éventuelle attaque DDoS[6]. En Suisse, les principaux fournisseurs de services Internet proposent une protection DDoS que vous pouvez déjà acheter, mais qu'il ne vous faudra payer que si vous en avez vraiment besoin.

Fichiers journaux
Les fichiers journaux (*logfiles*) sont essentiels pour la reconstitution d'un incident informatique. Assurez-vous que les systèmes importants, 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. L'analyse des fichiers journaux nécessitant des connaissances approfondies, il peut être judicieux d'en charger un prestataire informatique.

Segmentation du réseau[7]
Partagez votre réseau d'entreprise en plusieurs domaines (par ex. réseaux séparés pour la production, le personnel, la comptabilité, etc.). Il n'y a pas de raison que les collaborateurs du service du personnel aient accès à votre installation de production. Vous éviterez ainsi par exemple que l'ordinateur de commande d'installations de production qui ne peuvent plus être mises à jour serve de porte d'entrée à des attaquants.

---

5 Mesures de protection pour les systèmes de gestion de contenu (CMS): https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html

6 Mesures contre les attaques DDoS: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html

7 Par ex. les prescriptions de l'Office fédéral allemand de la sécurité des technologies de l'information (BSI) sur une segmentation logique adéquate: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html

Comme précaution minimale, les ordinateurs de la comptabilité et ceux du service du personnel devraient faire partie d'un réseau séparé et ne pas être accessibles depuis les autres ordinateurs de votre réseau. N'oubliez pas que les maliciels peuvent se répandre dans le cadre des partages réseau. Votre prestataire informatique vous conseillera volontiers dans la planification et la mise en œuvre des mesures correspondantes.

Filtrage de courriels potentiellement dangereux
La réception de courriels contenant des fichiers potentiellement dangereux devrait déjà être bloquée ou filtrée sur votre passerelle de messagerie ou par votre filtre anti-pourriel. Vous trouverez sur le site Web du NCSC[8] une liste des extensions de fichiers potentiellement dangereuses. Veillez à ce que ces fichiers soient également bloqués lorsqu'ils sont envoyés dans un fichier d'archive tel qu'un fichier ZIP, RAR, ISO ou dans un fichier d'archive protégé (par ex. un fichier ZIP protégé par un mot de passe) à des destinataires situés dans votre entreprise.

Macros
Les macros ont pour but l'automatisation de tâches dans des documents Office. Mais elles peuvent également être utilisées pour diffuser des maliciels.
Les pièces jointes de courriels renfermant des macros (par ex. pièces jointes Word, Excel ou PowerPoint) devraient être systématiquement bloquées. Incitez vos collaborateurs à ne pas ignorer les mises en garde dans ce sens dans les programmes Office.

Accès à distance
Si des collaborateurs doivent pouvoir accéder au réseau de l'entreprise de l'extérieur (par ex. parce qu'ils sont en déplacement, en télétravail, etc.), cela ne devrait être possible que par le biais d'un réseau privé virtuel (VPN) au moyen d'une authentification à deux facteurs. Cette règle s'applique aussi à l'accès des prestataires informatiques externes et des administrateurs.

Services de stockage dans le nuage (*cloud*)
Les services de stockage dans le nuage vous dispensent notamment d'exploiter une coûteuse infrastructure informatique. N'utilisez toutefois qu'avec retenue de tels services. Les données sensibles ne devraient jamais se trouver dans le nuage, mais être enregistrées au niveau local exclusivement. En outre, avant de conclure tout contrat, renseignez-vous auprès du prestataire sur les principales mesures de sécurité (accès aux données, sauvegarde des données, etc.).

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

[8] Règles de comportement du NCSC spécifiques au courrier électronique: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html