Table des matières

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI de la Confédération suisse a édité des recommandations pour protéger les PME suisses en matière de sécurité informatique. Les voici compilées ici sur un même document.

Règles de comportements

Navigation sur le Web

La navigation sur le web expose aussi à des dangers susceptibles d'avoir une influence sur la sécurité de vos données et de votre ordinateur. Quelques-uns d'entre eux, et les mesures de protection adaptées, font l'objet de la liste suivante:

Virus, vers, chevaux de Troie, logiciel espion

Ne pas télécharger de programme inconnu
Ne téléchargez aucun programme inconnu (jeux, économiseurs d'écran, etc.) depuis Internet. Cliquez sur « Interrompre » ou sur « non » lorsqu'une fenêtre de téléchargement s'affiche sans que vous ne l'ayez voulu.

Se procurer les mises à jour auprès du fabricant seulement
Téléchargez les mises à jour ou les pilotes exclusivement sur les sites web du fabricant concerné. Vérifiez-les ensuite au moyen d'un logiciel antivirus actualisé.

Ingénierie sociale, hameçonnage (phishing), escroquerie

Prudence en cas de transmission d'informations
Ne donnez à personne votre nom d'utilisateur ou votre mot de passe. Aucun fournisseur sérieux ne vous demandera votre mot de passe (même par téléphone). Cette remarque vaut également lorsque la demande paraît crédible et comporte des caractéristiques d'identification évidentes du fournisseur (p. ex. adresse électronique, site Internet, etc.). En cas de doute, ne répondez pas et posez la question à votre fournisseur.

S'enquérir du sérieux du fournisseur
Lors d'achats en ligne, il faut veiller à ne traiter qu'avec les fournisseurs sérieux. N'entrez votre numéro de carte de crédit que sur des pages Web utilisant un protocole sécurisé. On les reconnaît à la petite clé dorée s'affichant sur le bord inférieur gauche du navigateur ou au protocole indiqué dans l'URL (https au lieu de http).

Prendre congé en bonne et due forme
Utilisez toujours la déconnexion prévue pour quitter les applications Web (p. ex. Webmail, transactions bancaires).

Protection des données

Etre sur ses gardes quand on remplit des formulaires web
Évitez de disséminer des données personnelles. Cela concerne spécialement le remplissage de formulaires sur le web.

Prudence en rédigeant des textes dans les forums de discussion
Pensez que ce que vous écrivez dans le cadre de groupes de discussion ou de forums, ou encore dans des livres d'hôte, reste accessible encore pendant des années.

Configuration du navigateur

Chaque page web est composée des instructions écrites en code HTML. Ces instructions indiquent au navigateur (Internet Explorer, Firefox, Chrome p. ex.) comment représenter le contenu du site sur l'écran du client. Certains sites du web ne comprennent que des documents sans fonctions additionnelles (ce sont des pages statiques). D'autres proposent des contenus dynamiques. Citons pour exemple les textes défilants, les formulaires électroniques pour des achats en ligne, des images animées ou des bannières publicitaires dynamiques. Ces fonctions dynamiques peuvent être implémentées à l'aide d'ActiveX Controls ou de JavaScript. Ceux-ci peuvent malheureusement être détournés pour définir et exécuter des actions indésirables ou nocives pour l'ordinateur client.

Restreindre javascript
MELANI recommande de limiter tant que possible l'exécution de javascript (active scripting) à travers les paramètres du navigateur ou certains modules (plugins), voire de le désactiver complètement. En cas de désactivation, il faut cependant être conscient que de nombreux sites web ne pourront plus fonctionner correctement. Si cette mesure s'avère trop contraignante, vous pouvez assouplir les limitations progressivement jusqu'à un niveau acceptable. Suivant la solution choisie, il est par ailleurs possible de définir sur quels sites web vous autorisez l'exécution de javascript (whitelisting).

Politique des mots de passe

Tant votre ordinateur que divers services en ligne exigent la saisie d'un mot de passe. Les mots de passe mal choisis ou trop courts - dits faibles - représentent un risque de sécurité considérable. Le choix d'un mot de passe doit respecter les principes suivants:

Longueur minimale de 8 signes

La longueur minimale du mot de passe doit être de 8 signes; par ailleurs, il devrait comprendre des lettres, des chiffres ainsi que des caractères spéciaux.

Facile à mémoriser

Le mot de passe doit être choisi de telle manière qu'il soit facile à mémoriser. Ne consignez pas vos mots de passe par écrit. Les meilleurs mots de passe sont des phrases entières comprenant des caractères spéciaux. Par exemple: « 1 m0t de p@$ qui va me rester !! »

N'utilisez pas plusieurs fois le même mot de passe

Utilisez des mots de passe différents pour des usages différents (p. ex. pour différents comptes utilisateurs). Si vous utilisez des services en ligne, il est recommandé d'utiliser à chaque fois un mot de passe différent.

Changer régulièrement de mot de passe

Un mot de passe devrait être changé à intervalles réguliers (tous les trois mois à peu près) mais au plus tard quand vous présumez que des tiers pourraient en avoir eu connaissance.

Vérificateurs de mots de passe

Divers programmes peuvent vous aider à tester votre mot de passe (faites ce genre de test non pas avec l'original mais avec un mot de passe construit d'une manière similaire).

Gestionnaires de mots de passe

Ce type de programmes propose de gérer les différents mots de passe d'un utilisateur. L'accès au service est généralement protégé par un « master password ».

Messagerie électronique

Le courrier électronique est un moyen de communication très apprécié. La plupart des maliciels infectent en général les ordinateurs via les annexes au courrier électronique. Se montrer prudent avec le courrier électronique contribue considérablement à la sécurité de vos données et de votre ordinateur. Les mesures suivantes vous protègent contre les virus, les vers, les chevaux de Troie, les pourriels (spam) et autres canulars (hoaxes):

Virus, vers et chevaux de Troie

Prudence avec le courrier électronique dont l'expéditeur est inconnu
Méfiez-vous du courrier électronique dont l'adresse d'expédition vous est inconnue. Dans un tel cas, n'ouvrez aucun document ou programme joint et ne sélectionnez aucun des liens y figurant.

S'assurer de la fiabilité des sources
N'ouvrez que des fichiers ou des programmes provenant de sources dignes de confiance et ne le faites qu'après les avoir vérifié avec un logiciel antivirus actualisé.

Prudence avec les noms de fichiers à deux extensions
N'ouvrez aucune annexe de courrier électronique à deux extensions (p. ex. picture.bmp.vbs). Ne vous laissez pas tromper par l'icône d'un tel fichier. Dans Explorer par exemple, désactivez l'option « Cacher les extensions des fichiers dont le type est connu ».

Mise à jour du programme de courrier électronique
Les programmes de courrier électronique peuvent aussi présenter des lacunes de sécurité. Vérifiez régulièrement l'existence de mises à jour pour ce programme et installez-les.

Pourriel (spam)

Communiquer son adresse e-mail avec parcimonie
Communiquez votre adresse électronique à un minimum de personnes et utilisez-la exclusivement pour la correspondance importante.

Se doter d'une deuxième adresse e-mail
Il est indiqué d'utiliser une deuxième adresse e-mail pour remplir des formulaires sur le web, s'abonner à des bulletins, écrire dans des livres d'hôte, etc. Il est possible d'en obtenir une gratuitement auprès de divers fournisseurs. Si du pourriel est distribué à cette adresse, on peut la supprimer ou en définir une nouvelle.

Ne pas répondre aux pourriels
Si vous répondez aux pourriels, l'expéditeur saura que votre adresse électronique est valable et continuera d'expédier du courrier non sollicité. Prudence aussi avec le pourriel offrant une « option de désabonnement ». On vous promet de vous tracer de la liste des destinataires si vous envoyez un courrier électronique d'une certaine teneur. On se montrera tout aussi prudent à l'égard des réponses automatiques en cas d'absence du bureau. Elles devraient être uniquement renvoyées aux expéditeurs connus.

Communication poste à poste

La communication entre « pairs » est appelée communication poste à poste (peer-to-peer; P2P). Ce modèle contraste avec celui du client - serveur usuel où un serveur propose des services utilisés par des clients. Un exemple est la navigation sur Internet. Le client (navigateur Internet) se connecte à un serveur Web et utilise les services mis à disposition (p. ex. achats en ligne). A l'opposé, avec le modèle poste à poste, chaque ordinateur est en même temps un client et un serveur, ce qui veut dire que chaque poste propose des services (mise à disposition de fichiers) et utilise les services d'autres ordinateurs du réseau.

Les bourses d'échange utilisent en particulier cette forme de communication. Chacun peut échanger des fichiers (p, ex. de la musique ou des films) avec tout un chacun. Pour cela, il faut en général installer un logiciel (qui peut être téléchargé depuis Internet). Comme les bourses d'échange permettent souvent d'accéder à des oeuvres protégées par le droit d'auteur ou à des contenus pornographiques, elles sont souvent controversées. Les fournisseurs de tels logiciels ont été la cible de plaintes de l'industrie musicale et cinématographique, et les possesseurs de documents de pornographie dure sont poursuivis par la police.

Prudence avec les réseaux poste à poste et les bourses d'échange

En plus des aspects de protection du droit d'auteur évoqué, la participation à des bourses d'échange va de pair avec d'autres risques. Nombre de fichiers proposés sont infectés par des virus ou des chevaux de Troie. Le logiciel poste à poste peut contenir du code espion ou de la publicité non désirée, ainsi que des lacunes de sécurité. Par ailleurs, la participation à de tels réseaux et à de telles bourses d'échange fait courir le danger que l'utilisateur rende accessible par mégarde des données personnelles et ou confidentielles.

Logiciels et paramètres

Software Updates

Des mises à jour des logiciels (patches), visant à améliorer la sécurité, remédient aux lacunes de sécurité que l'on découvre quasiment tous les jours. Des failles dans la sécurité peuvent permettre un accès non autorisé à vos données ou la prolifération de vers ; elles se produisent aussi bien dans les systèmes d'exploitation que dans les applications (p. ex. Adobe Flash, Adobe Reader, Sun Java etc.). Une importance capitale revient par conséquent à l'actualisation de vos logiciels pour augmenter la sécurité de vos données.

Mettre régulièrement à jour le système d'exploitation et les applications

Certains produits proposent une fonction de mise à jour automatique ; faites en impérativement usage. Vérifiez régulièrement si elle est toujours activée. Consultez les informations actuelles sur les mises à jour sur le site Internet du fabricant concerné.

Suivre les informations relatives aux mises à jour des logiciels

D'autres organes informent régulièrement sur les nouvelles failles de sécurité, vulnérabilités et les mises à jour pertinentes (et d'autres mesures).

Personal Firewall

Un pare-feu (firewall) protège les systèmes informatiques en surveillant et, éventuellement refusant, les connexions entrantes ou sortantes. Vu sous cet angle, il est comparable à un poste de garde surveillant la porte d'un château. La décision d'autoriser ou de refuser telle ou telle connexion intervient sur la base de règles simples mises en œuvre à l'établissement de toute nouvelle connexion. Les pare-feux réduisent le risque que des pirates informatiques (hackers) accèdent sans autorisation à des données informatiques et minimisent les dangers liés aux chevaux de Troie, aux logiciels espions ou aux vers. La plupart des entreprises protègent leur réseau à l'aide d'un pare-feu performant installé sur un ordinateur dédié, placé entre l'Internet et le réseau de la société. Un pare-feu personnel (personal firewall ou desktop firewall) est en revanche installé pour protéger un ordinateur unique; il est directement installé sur le système à protéger, c'est-à-dire sur votre ordinateur.

Recourir à un pare-feu personnel

Comme les programmes antivirus, les pare-feux personnels sont disponibles sous forme de logiciels additionnels et certains peuvent être téléchargés gratuitement depuis l'Internet. Quelques systèmes d'exploitation sont déjà équipés d'un pare-feu personnel.

Installer le pare-feu avant la connexion Internet

Si votre ordinateur est équipé d'un pare-feu personnel, activez-le impérativement avant de connecter votre ordinateur (pour la première fois) à l'Internet. Il ne faudrait procéder au téléchargement de mises à jour de logiciels, d'autres programmes et fichiers que lorsque le pare-feu personnel est activé.

Logiciels antivirus

Les logiciels antivirus protègent vos données contre les virus, les vers et les chevaux de Troie. Un programme antivirus actuel est absolument indispensable si vous échangez des données avec d'autres personnes et si vous téléchargez des programmes ou des fichiers depuis Internet. Comme de nouveaux virus, vers ou chevaux de Troie peuvent surgir quotidiennement, une actualisation régulière du logiciel antivirus est absolument nécessaire.

Installer un logiciel antivirus

Recourir sans faute à un logiciel antivirus actualisé.

Actualiser régulièrement votre logiciel antivirus

Assurez-vous que le logiciel antivirus est actualisé deux à trois fois par semaine au moins. La plupart des produits disposent d'une fonction de mise à jour automatique en ligne qui vous épargne ce travail et dont il faut absolument faire usage.

Vérifier la validité de la licence

Assurez-vous régulièrement que la licence du logiciel antivirus utilisé est encore valable. Certes, le logiciel continue de fonctionner même après la durée de validité, mais il n'est alors plus possible de profiter de mises à jour.

Sauvegarder des données

On ne peut jamais exclure que des données soient partiellement détruites, voire complètement perdues, en raison de défauts techniques, suite à des manipulations erronées, ou suite à l'attaque de virus ou de vers. Pour minimiser le risque d'une perte de données, la sauvegarde régulière des données (backup) est vivement recommandée.

Sauvegarder régulièrement les données

Les données à protéger devraient être copiées régulièrement sur des supports externes (CD-ROM, DVD, clé de mémoire USB ou disques durs externes). Pensez qu'il faut aussi de temps à autre effectuer une sauvegarde complète de toutes les données figurant sur votre ordinateur.

Conserver les supports de données en lieu sûr

Les supports de données sont à conserver dans un lieu protégé des influences extérieures. Il est déconseillé de conserver les copies de sécurité à proximité immédiate de l'ordinateur, car elles seraient également détruites en cas d'incendie, de dégât d'eau, etc.

Contrôler les copies de sauvegarde

Le contrôle régulier de l'exhaustivité et de la lisibilité des sauvegardes de données fait aussi partie intégrante de la sauvegarde des données. Essayez de temps à autre de reconstituer certains fichiers.

Partage des espaces disques

Vérifiez qu'aucune modalité de partage (Windows shares) ne soit installée sur votre ordinateur. Les partages permettent sur un système Windows de mettre à disposition d'autres utilisateurs via le réseau des fichiers, voire tous les disques. Les partages représentent non seulement des points d'attaque pour les virus et les vers mais peuvent également rendre accessibles vos données (même confidentielles) à un large cercle d'utilisateurs (dans le pire des cas à tous les internautes).

Browsers | Stratégie à deux navigateurs et autres possibilités

Il est aujourd'hui généralement d'usage d'installer régulièrement, de préférence automatiquement, les mises à jour de sécurité des systèmes d'exploitation et des applications. On rencontre néanmoins régulièrement des failles « zero day », soit des lacunes pour lesquelles il n'existe pas encore de mise à jour de sécurité. Presque tous les jours, de telles failles de sécurité sont identifiées dans toutes sortes d'applications. Les navigateurs Internet ne font pas exception à la règle. Selon la gravité de la vulnérabilité découverte, il peut être judicieux de changer de navigateur jusqu'à ce que le fabricant ait résolu le problème.

Ce qui n'est qu'une simple formalité pour un ordinateur privé peut s'avérer un vrai casse-tête dans le monde professionnel. Car à la différence des ordinateurs privés, il est souvent délicat pour une entreprise de changer de navigateur. Par exemple faute d'avoir prévu une stratégie à deux navigateurs. Cela est fréquemment le cas, afin que le service chargé des TIC ne doive assumer la maintenance que d'un seul navigateur.

En cas de grave faille de sécurité, des données confidentielles voire secrètes risquent aussi d'être menacées. Il est par conséquent judicieux de parer à toute éventualité, dans la vie privée comme dans le cadre professionnel, afin de pouvoir au plus vite se rabattre sur un navigateur de rechange.
Les possibilités suivantes seraient envisageables dans le monde professionnel (l'énumération n'étant pas exhaustive):

Equipement de tous les postes avec au moins deux navigateurs

Tous les postes de travail d'une entreprise comportent au moins deux navigateurs. En cas de nécessité, le personnel sera prié de ne plus utiliser le navigateur problématique jusqu'à nouvel avis. Il serait également possible, le cas échéant, d'agir directement via le serveur mandataire (proxy), en empêchant ce navigateur d'accéder à Internet. Mais une telle solution serait coûteuse, en obligeant à assurer la maintenance de plusieurs navigateurs. Quant aux utilisateurs, ils hésiteraient souvent sur le navigateur à utiliser.

Equipement ponctuel d'au moins deux navigateurs

Seuls les postes de travail ayant impérativement besoin d'Internet seront équipés de plusieurs navigateurs. A supposer que l'un d'eux présente une faille de sécurité, il ne sera plus utilisable et il faudra en changer. Le grave inconvénient de cette solution tient à ce qu'en cas d'urgence, une partie du personnel serait momentanément privée d'accès à Internet. Même si cela ne

joue peut-être pas un rôle important pour leur travail, les utilisateurs concernés risquent de se sentir infantilisés ou discriminés.

Liste blanche

Tous les départements de l'entreprise signalent au service TIC les URL dont ils ont absolument besoin même en cas d'urgence. Les liens correspondants seront inscrits sur une liste blanche. En cas de faille de sécurité, tous les URL absents de cette liste seront bloqués. Une telle mesure permettrait de faire l'économie d'un second navigateur. Le risque de dommages sera réduit au minimum, puisque seuls des URL bien précis resteront accessibles. Tout risque n'est pas pour autant écarté. D'où la nécessité d'installer au plus vite les mises à jour de sécurité, afin de pouvoir renoncer au blocage temporaire des URL absents de la liste blanche.

Equipements et périphériques

WLAN

Un WLAN (Wireless Local Area Network) est un réseau local sans fil. Dans un tel réseau, les terminaux (p. ex. ordinateurs portables, agendas électroniques (PDA), etc.) communiquent sans fil avec un point d'accès WLAN (WLAN Access Point), relié à Internet ou à un réseau local. L'avantage du WLAN est que ses utilisateurs sont davantage mobiles étant donné que leurs terminaux ne sont pas câblés. Dans les bâtiments, la portée dépend du type de construction et est nettement plus réduite qu'à l'extérieur où une connexion WLAN est possible à plus de 200 m.

Protection de la page administration

La plupart des points d'accès WLAN disposent pour l'administration d'une interface utilisateur accessible avec un navigateur (par une adresse de forme suivante: http://ADRESSE_IP_DU_POINT_D'ACCES). Cette interface permet les configurations ci-après. La page administration est protégée par un mot de passe standard, qu'il faut modifier immédiatement.

Modifiez l'identification du réseau (SSID) attribuée de manière standard.

Bloquer l'envoi de l'identification du réseau

Empêchez que le point d'accès envoie régulièrement son identification de réseau (SSID) en configurant l'option « Broadcast SSID » sur « Non ».

Restriction d'accès aux terminaux

Limitez l'accès à votre point d'accès WLAN afin que seuls vos terminaux puissent communiquer avec lui, en saisissant chacune de leur adresse MAC.

Enclencher le chiffrement

Activez le chiffrement WPA ou WPA2 de votre matériel WLAN en choisissant un mot de passe « fort », c'est-à-dire difficile à deviner.

Recours à des protocoles sûrs

Pour transmettre des données confidentielles via le WLAN, il est recommandé de recourir à des protocoles qui chiffrent les données à envoyer (p. ex. VPN, https, ssh, etc.).

Routeur

Les appareils directement reliés à Internet doivent être particulièrement protégés. Cela comprend non seulement le choix de mots de passe qui satisfont aux exigences les plus récentes, mais également une mise à jour conséquente des appareils avec les logiciels (software et firmware) les plus récents.

Smartphone

Les temps sont révolus où les téléphones portables ne servaient qu'à téléphoner! Actuellement, le grand nombre de fonctions (caméra intégrée, agenda, jeux, fonctions SMS et MMS, périphériques à infrarouge et Bluetooth, possibilité de surfer sur Internet), a transformé le portable en un petit appareil multifonction. Mais plus l'offre en fonctions est grande, plus la probabilité de points faibles augmente.

Mises à jour

Comme c'est le cas pour les ordinateurs, des mises à jour sont disponibles pour les smartphone. Il est recommandé d'installer régulièrement les dernières mises à jour.

Autorisations des applications
Afin de remplir ses fonctions, chaque application a besoin de certaines autorisations. Il y a cependant aussi des applications qui demandent des autorisations n'étant pas indispensables. Lorsque cela est possible, il est recommandé de limiter les autorisations. Si vous ne vous sentez pas en confiance, il est souvent plus sage de renoncer à l'application.

Sauvegardes
De nombreuses données importantes sont bien souvent présentes sur un smartphone, c'est pourquoi il est important d'effectuer des sauvegardes régulières. En plus de connaître des problèmes techniques, un smartphone peut également être volé ou perdu.

Code PIN et chiffrement des données
Etant donné qu'un smartphone peut être volé, il est recommandé de protéger son accès par un code PIN aussi sûr que possible et également de chiffrer vos données les plus sensibles.

Utilisation éclairée du cloud
Si vous utilisez un service de stockage dans les nuages (cloud), il convient de bien être conscient de ce qui est enregistré et où. Si vous ne voyez pas d'utilité à ce service, nous vous recommandons de le désactiver.

Attention en cas de SMS envoyés par des inconnus
Evitez de répondre aux SMS envoyés par des personnes inconnues.

Webcam

Les appareils directement reliés à Internet doivent être particulièrement protégés. Cela comprend non seulement le choix de mots de passe qui satisfont aux exigences les plus récentes, mais également une mise à jour conséquente des appareils avec les logiciels (software et firmware) les plus récents. MELANI recommande également de recouvrir la caméra avec une bande autocollante lorsque celle-ci n'est pas utilisée. Il existe même des produits destinés précisément à cette utilisation, qui permettent de recouvrir temporairement la lentille de la caméra.

Source	Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
Site	www.melani.admin.ch
Lien	https://www.melani.admin.ch/melani/fr/home/schuetzen.html