Information
Security Society
Switzerland

Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME)

Une protection accrue grâce au programme en 10 points élargi.

« De la pratique – pour la pratique » Cahiers des PME

Concept et textes
Groupe de travail PME + sécurité de l'information de l'association InfoSurance
Ueli Brügger, IBM, Zürich
Christof Egli, Ernst Basler + Partenaire, Zürich (chef du groupe de travail) Hanspeter Feuz, IT Projects, Thun
Tiziana Giorgetti, Symantec Switzerland AG, Bassersdorf
René Hanselmann, Microsoft GmbH, Wallisellen
Peter Neuhaus, Fondation PME Suisse, Berne
Le groupe de travail a été assisté par :
Jürg Altenburger, IBM, Zürich
Chris Baur, Trivadis AG, Zürich
Diego Boscardin, Symantec Switzerland AG, Bassersdorf
Herbert Brun, UPAQ Ltd., Küsnacht
Roger Halbheer, Microsoft GmbH, Wallisellen Andrea Müller, Microsoft GmbH, Wallisellen Peter Kunz, Omnisec, Dällikon
Anton Lagger, Office fédéral pour l'approvisionnement économique du pays, Berne
Marc Vallotton, InfoGuard AG, Zug
Christian Weber, Secrétaire d'Etat à l'économie (SECO), Bern
Carlos Rieder, Haute Ecole de Gestion, Lucerne
Chris Baur, Trivadis AG, Zürich
Wolfgang Sidler, SIDLER Information Security GmbH, Hünenberg
Concept et réalisation graphique
Künzli Communication AG, Lucerne
Impression
Gisler Druck AG, Altdorf

Chers chefs d'entreprise

La Suisse compte parmi les principaux utilisateurs de technologies de l'information et de la communication (TIC) dans le monde. Personne ne dépense autant d'argent par habitant pour les technologies informatiques que les Suisses.

Plus rien ne fonctionne sans l'informatique. Et c'est la même chose pour vous qui dirigez une petite ou une moyenne entreprise suisse. Or les PME sont le principal pilier de l'économie suisse. Vous jouissez d'une excellente réputation car vos produits et services sont synonymes de qualité, flexibilité et innovation.

L'Association InfoSurance s'occupe depuis plusieurs années des risques liés à l'utilisation de l'informatique dans les petites et moyennes entreprises. Pour aider les entreprises à mettre en oeuvre un système de protection adéquat, InfoSurance a publié en 2005 un **Programme en 10 points pour la mise en place d'une protection de base efficace en informatique.**

L'association InfoSurance complète aujourd'hui ce programme en ajoutant dix autres points qui s'adressent principalement aux entreprises nécessitant une grande disponibilité de leurs systèmes et la confidentialité absolue de leurs données.

Le **Programme en dix points élargi** se veut encore une fois compréhensible et peu onéreux dans sa mise en oeuvre. Mais pour tous les cas où des connaissances spécifiques s'avèrent nécessaires, n'hésitez pas à vous adresser à un expert externe.

En entreprise, une bonne gouvernance passe notamment par la gestion des risques. Ainsi, la loi exige depuis le 1er janvier 2008 la présence de données relatives à l'évaluation des risques de même que l'existence d'un système de contrôle interne (SCI). Cette brochure vous apportera également une aide précieuse dans le vaste domaine de l'informatique.

Dans l'espoir que vous accorderez à ce programme élargi la même attention qu'au premier, je vous adresse, à vous et à votre entreprise, tous mes voeux de succès pour votre marche vers une plus grande sécurité de l'information.

Edi Engelberger, membre du Conseil national suisse

Président de l'Union suisse des arts et métiers

Le programme en 10 points élargi : vue d'ensemble

10 mesures pour une protection de base efficace

Point n° 1 Etablissez un cahier des charges pour les responsables informatiques !
Point n° 2 Protégez vos données en faisant régulièrement des backups !
Point n° 3 Effectuez toujours les dernières mises à jour de votre antivirus !
Point n° 4 Protégez votre navigation sur Internet avec un pare-feu !
Point n° 5 Effectuez régulièrement les mises à jour de vos logiciels !
Point n° 6 Choisissez des mots de passe complexes !
Point n° 7 Protégez vos appareils portables !
Point n° 8 Expliquez vos directives pour l'utilisation des moyens informatiques !
Point n° 9 Protégez l'environnement de vos infrastructures informatiques !
Point n° 10 Adoptez un bon système de classement pour vos documents et dossiers !

5 mesures supplémentaires pour améliorer la confidentialité

Point n° 11 Respectez les règles !
Point n° 12 Réglementez la protection de l'accès aux données !
Point n° 13 Verrouillez l'accès à vos appareils portables et cryptez les données lors des transferts !
Point n° 14 Gérez les documents non électroniques de façon confidentielle !
Point n° 15 Sensibilisez vos collaborateurs !

5 mesures supplémentaires pour améliorer la disponibilité

Point n° 16 Vérifiez vos systèmes informatiques !
Point n° 17 Equipez vos ordinateurs d'une alimentation sans interruption !
Point n° 18 Misez sur la redondance des modules importants !
Point n° 19 Etablissez un plan d'urgence !
Point n° 20 Gérez et distribuez le savoir-faire !

Etablissez un cahier des charges pour les responsables informatiques !

La sécurité informatique repose sur des facteurs techniques, humains et organisationnels ! Des solutions techniques en matière de sécurité et des collaborateurs motivés, c'est bien ! Mais la direction doit elle aussi contribuer activement pour garantir une protection de base efficace.

Toute entreprise a besoin d'un responsable infor• _matique et de son remplaçant. Les connaissances nécessaires pour occuper un tel poste peuvent être acquises lors d'une formation spécialisée. Il arrive aussi souvent que les petites entreprises fassent appel à des spécialistes externes. Pour l'entreprise, cela représente bien sûr un coût, mais bien moindre comparé aux conséquences d'une perte des données ou de la violation de la loi sur la protection des données.

La direction délègue officiellement les questions de • _sécurité au responsable informatique et définit ses tâches dans un cahier des charges (cf. ci-dessous).

La direction vérifie que le responsable informatique • _s'acquitte correctement de sa tâche.

Tous les collaborateurs qui travaillent sur ordina• _teur doivent recevoir un guide contenant les directives pour l'utilisation des moyens informatiques. Ces directives décrivent les opérations que vos collaborateurs sont autorisés ou non à effectuer sur l'ordinateur (cf. point n°8).

Désignez un interlocuteur pour toutes les ques• _tions liées à la sécurité : perte d'un ordinateur portable par exemple ou infection par un virus, etc.

Trucs et astuces

Sauvegardez régulièrement vos données sur des • _serveurs, stations de travail, notebooks et autres appareils portables (cf. point n°2).

Effectuez les dernières mises à jour de vos sys• _tèmes d'exploitation, programmes antivirus, pare-feux et autres logiciels (cf. points n°3, 4 et 5).

Modifiez immédiatement les réglages de mots • _de passe internes sur les ordinateurs, systèmes d'exploitation et programmes d'application.

Etablissez une liste de tous les ordinateurs de • _l'entreprise en précisant les programmes installés et les mises à jour effectuées (cf. point n°5).

Déterminez les droits d'accès de vos collabora• _teurs aux différents programmes et données.

Etablissez une liste de toutes les personnes habilitées• _à accéder de l'extérieur au réseau de l'entreprise, en indiquant le cas échéant la durée précise de leurs droits. Assurez-vous que les programmes de protection sont régulièrement mis à jour.

Veillez au respect des mesures de sécurisation des • _données, à travers par exemple des programmes de protection et des mots de passe complexes (cf. points n°3, 4 et 6).

Contrôlez régulièrement la bonne application des • _directives contenues dans le guide informatique.

Abordez les questions de sécurité à travers un • _projet où vous définissez des objectifs ainsi que la durée et les moyens prévus pour les atteindre.

La sécurité est un processus : contrôlez régulière• _ment la sécurité dans l'entreprise et améliorez-la si nécessaire en vous basant sur la méthode de la « roue de Deming » (Plan-Do-Check-Act).

Protégez vos données en faisant régulièrement des backups !

Il existe différentes manières de perdre des données : elles peuvent être écrasées par erreur, rendues illisibles à cause d'un défaut sur le disque dur, voire détruites par un incendie ou un dégât des eaux. Vous pouvez éviter de tels désagréments en faisant régulièrement des backups de vos données.

En règle générale, il convient d'effectuer des back• _ups de sécurité pour toutes les données dont le contenu est vital pour la poursuite de votre activité. De même, les configurations de logiciels devraient également faire l'objet de sauvegardes.

La fréquence de ces backups dépend de l'activité • _et de la taille de votre entreprise. Ceci dit, une PME devrait sauvegarder ses données au moins une fois par semaine.

Un backup quotidien vous permet de réaliser un • _archivage de vos données conforme au droit des obligations et à l'ordonnance concernant la tenue et la conservation des livres de comptes (Olico) (cf. ci-dessous).

Désignez par écrit les responsables des sauve• _gardes de sécurité et établissez une liste des backups effectués.

Sauvegardez toujours vos données sur des sup• _ports mobiles (bande magnétique et autres supports amovibles).

De même, il serait bon d'effectuer des copies des • _documents importants dont vous ne disposez que d'une version papier (contrats ou autres) et de les conserver hors de l'entreprise.

Attention ! Certains documents comme les bilans, • _les comptes de résultats, les livres de comptes, les inventaires, les justificatifs comptables et la correspondance commerciale doivent être conservés pendant 10 ans.

Trucs et astuces

Du lundi au jeudi, effectuez un backup quotidien sur • _différents supports de stockage. La semaine suivante, procédez de la même manière en écrasant les données des précédents backups jour après jour. Conservez les backups journaliers en dehors du local où se trouve votre serveur.

Chaque vendredi, faites un backup pour la semaine • _écoulée sur un support de stockage différent que vous conserverez hors de l'entreprise. Les backups hebdomadaires seront écrasés au bout d'un mois.

A la fin du mois, faites un backup pour le mois • _écoulé. Cette sauvegarde de sécurité mensuelle ne sera pas écrasée et devra être conservée hors de l'entreprise.

A la fin de l'année, faites un backup de l'année écou• _lée. Cette sauvegarde de sécurité annuelle ne sera pas écrasée et devra être conservée elle aussi hors de l'entreprise.

Vérifiez régulièrement que les données sauve• _gardées sur les supports de stockage sont accessibles. Une sauvegarde n'a de sens que si les données ont été correctement copiées sur le support.

Effectuez toujours les dernières mises à jour de votre antivirus !

Des programmes nuisibles, tels que par exemple les virus et les vers, peuvent paralyser vos infrastructures informatiques et mettre ainsi la vie de votre entreprise en péril.

Les virus informatiques peuvent modifier, corrom• _pre, voire même détruire complètement données et programmes. Ces programmes malveillants peuvent vous être transmis en pièce jointe d'un email, par messagerie instantanée, etc. Sur Internet, ces virus sont souvent déguisés en programmes gratuits, pseudo-utiles ou de divertissement et s'activent en un simple clic de souris.

Les systèmes informatiques mal protégés sont sou• _vent pervertis pour propager des virus et pour lancer des attaques ciblées contre une société tierce. Un chef d'entreprise qui ne prend pas les mesures suffisantes pour protéger ses systèmes informatiques fait preuve de négligence et s'expose à des poursuites pénales.

Un programme antivirus offre une protection con• _tre les virus et les vers connus. Il identifie les intrus et les met hors d'état de nuire. Ces programmes sont en vente dans les magasins d'informatique mais on en trouve aussi en téléchargement gratuit sur la toile.

Les cybercriminels ne cessent de mettre au point • _de nouveaux virus, raison pour laquelle il convient d'actualiser continuellement votre programme antivirus. Selon le produit utilisé, le programme recherche lui-même les mises à jour sur la page d'accueil du fabricant. Demandez à votre vendeur si c'est le cas pour votre antivirus. Quoiqu'il en soit, les mises à jour doivent être effectuées chaque jour.

Trucs et astuces

Installez un programme antivirus sur tous les ser• _veurs, postes de travail (clients) et ordinateurs portables, et effectuez régulièrement les mises à jour (une fois par jour minimum).

Interdisez expressément la désactivation, même • _temporaire, du programme antivirus.

Demandez à vos collaborateurs de signaler immédiat• _ement au responsable informatique les messages d'avertissement virus.

Effectuez au moins une fois par semaine un scan • _complet de votre disque dur. Vous pourrez ainsi découvrir et éliminer des virus qui n'avaient pas encore été détectés.

Interdisez expressément tout test « maison » sur • _les virus.

Pour les réseaux d'une certaine importance, les • _mises à jour des antivirus doivent se faire de façon centralisée et automatique.

Protégez votre navigation sur Internet avec un pare-feu !

Si vous avez des portes coupe-feu dans votre entreprise, vous veillez certainement à ce qu'elles soient toujours bien fermées. Dans le monde de l'Internet et de l'échange électronique de données, c'est le pare-feu qui remplit cette fonction sécuritaire.

En l'absence de pare-feu, n'importe qui peut • _s'immiscer dans votre système informatique, exécuter des taches à votre insu, utiliser votre ordinateur pour lancer des attaques illégales contre des tiers, ou bien encore accéder à des données commerciales confidentielles relevant de la loi sur la protection des données.

Pour les réseaux d'entreprise d'une certaine taille, • _il est recommandé d'adopter un pare-feu autonome (appareil spécial) ainsi qu'un pare-feu intégré (dans le système lui-même) pour les différents ordinateurs fixes et portables.

Vous trouverez dans le commerce des produits • _faisant à la fois office de pare-feu et d'antivirus. Ces produits combinés sont particulièrement indiquées pour les petites entreprises.

Plusieurs systèmes d'exploitation disposent d'un • _pare-feu intégré. Profitez systématiquement de cette possibilité et activez ces pare-feux.

Si vous utilisez un réseau local sans fil (WLAN) • _dans votre entreprise, veillez à ce qu'il soit sûr et sécurisé. Un réseau local sans fil mal configuré anéantit toute la protection offerte par le système de pare-feu.

Toutes les passerelles réseau doivent être sécuri• _sées par un pare-feu. Toutes les connexions entre fournisseurs, clients, sous-traitants et collaborateurs (même en accès à distance) et votre réseau doivent être contrôlées par un pare-feu.

Trucs et astuces

Installez un pare-feu et effectuez régulièrement les • _mises à jour.

Tout le trafic Internet doit passer à travers le crible • _du pare-feu. N'autorisez aucun autre accès à Internet (par ex. via modem).

N'utilisez aucun ordinateur portable ou réseau local • _sans fil privé sans l'autorisation écrite du responsable informatique.

Protégez la configuration de votre pare-feu avec un • _mot de passe complexe.

Sauvegardez régulièrement la configuration du • _pare-feu central.

Effectuez régulièrement les mises à jour de vos logiciels !

Contrôlez-vous régulièrement le niveau d'huile et la pression des pneus de votre voi-ture ? C'est souhaitable… De la même manière que vous entretenez régulièrement votre voiture, vous devez veiller à ce que les programmes informatiques de votre entreprise soient régulièrement mis à jour pour être toujours au top niveau.

Les logiciels actuels contiennent souvent des mil• _lions de lignes codées. Or malgré les contrôles, il arrive parfois qu'une erreur se faufile à travers ces lignes. Pour un fabricant, il est pratiquement impossible de tester chaque application dans tous les environnements et configurations possibles. C'est pourquoi les fabricants proposent régulièrement des patchs correctifs qui permettent de rattraper les erreurs connues.

Si vous ne mettez pas à jour régulièrement vos • _programmes, des cybercriminels peuvent exploiter des failles connues pour manipuler des données ou abuser de votre infrastructure à des fins peu scrupuleuses.

La plupart du temps, les systèmes d'exploitation • _et les applications sont en mesure de télécharger automatiquement les mises à jour sur Internet. Les sites Internet des fabricants de logiciels et le manuel d'utilisation vous fourniront à ce sujet une aide utile.

Soyez le moins vulnérable possible et n'installez • _donc que les programmes dont vous avez vraiment besoin et désactivez les services, validations de réseaux et autres protocoles inutiles. Ce qui n'existe pas ne peut être piraté et ne nécessite pas de maintenance !

Si vous-même découvrez des points faibles ou si • _le logiciel répond de façon inattendue, il convient d'en informer le fabricant.

Trucs et astuces

Installez les tout derniers patchs correctifs de vos • _systèmes d'exploitation et applications.

Installez dès que possible les mises à jour de sécu• _rité disponibles.

Installez les mises à jour uniquement pour les ver• _sions des logiciels que vous utilisez.

Installez les patchs sur touts les ordinateurs fixes • _et portables, y compris ceux de vos collaborateurs externes !

Etablissez une liste pour recenser quelles mises à • _jour ont été installées et sur quel ordinateur.

Pour télécharger les toutes dernières mises à jour des produits Microsoft : www.windowsupdate.com.

Choisissez des mots de passe compliqués !

Il suffit de connaître le nom et le mot de passe d'un utilisateur pour se connecter dans un système à sa place et abuser de son identité (informatique !) et de tous ses droits d'accès. Le vol de mots de passe permet aux cyberpirates d'accéder, à peu de frais, à des informations commerciales confidentielles. Faites en sorte qu'on ne puisse usurper des identités au sein de votre entreprise.

- Les mots de passe permettant d'accéder aux ordinateurs, systèmes d'exploitation et applications de votre entreprise doivent être modifiés immédiatement par le responsable informatique (cf. Point n°1).
- Invitez vos collaborateurs à choisir des mots de passe compliqués qu'ils devront changer régulièrement. Ils doivent être conscients du fait qu'ils seront tenus responsables des actions commises sous leur nom d'utilisateur.
- Les mots de passe complexes sont composés d'au moins 8 caractères, dont des majuscules, des minuscules, des chiffres et des caractères spéciaux.
  Voici comment créer un mot de passe compliqué.
  Exemple n°1 : prenez un mot simple comme « nuage », intercalez un caractère spécial, introduisez des majuscules et complétez par un chiffre correspondant au mois courant. Vous obtenez ainsi un mot de passe complexe « Nu$aGe04 ».
  Exemple n°2 : à partir d'une phrase comme « Nous avons passé deux jours à Paris ! », vous pouvez tirer le mot de passe « Nap2jàP! » en mettant à la suite la première lettre de chaque mot et les chiffres. Il sera plus facile de mémoriser une phrase qui a du sens plutôt qu'un mot de passe cryptique !

Trucs et astuces

- N'utilisez aucun mot de passe pouvant se trouver dans un dictionnaire.
- N'utilisez pas de mots de passe contenant des le nom, le numéro de passeport ou d'AVS, ou la date de naissance d'un de vos proches.
- Contrôler le niveau de sécurité de votre mot de passe avec un testeur de mots de passe.
- Changer de mot de passe au moins tous les deux mois. L'idéal est que ce soit le système à vous demander de le faire.
- N'écrivez jamais vos mots de passe sur un bout de papier, à moins de le conserver sous clé ! Beaucoup d'utilisateurs laissent leurs mots de passe dans un rayon d'un mètre de leur ordinateur.
- Ne communiquez jamais votre mot de passe à des tiers. Une personne peut être remplacée sans qu'elle doive nécessairement révéler son mot de passe. Si vous constatez qu'un tiers connaît votre mot de passe, modifiez-le immédiatement.

Pour vérifier le niveau de sécurité de votre mot de passe : https://passwortcheck.datenschutz.ch.

Protégez vos appareils portables !

Les téléphones mobiles, ordinateurs portables et assistants personnels en connexion WLAN sont à la fois pratiques et multitâches. Mal employés, ces appareils représentent cependant un risque important. Aussi, quiconque est tenu, pour des raisons professionnelles, de stocker des données sensibles sur un appareil portable, doit prendre des mesures spéciales.

Tous les ordinateurs portables doivent être protégés par un mot de passe compliqué (cf. Point n°6). Sinon, n'importe qui pourrait accéder aux données commerciales de votre entreprise en cas de perte ou de vol d'un portable.

Les appareils portables ne devraient contenir que les données strictement nécessaires à leur fonction. N'oubliez pas d'effectuer régulièrement un backup de ces données (cf. point n°2).

Les données sensibles stockées sur un ordinateur portable doivent être protégées par un code d'accès pour éviter qu'elles ne puissent être exploitées par des personnes malintentionnées. Vous trouverez de bons programmes de cryptage dans le commerce, mais aussi en téléchargement sur Internet.

Les appareils portables doivent être passés régulièrement à l'antivirus, car ils sont synchronisés avec les autres ordinateurs de l'entreprise, à travers les fonctions de messagerie électronique par exemple.

Une connexion WLAN mal configurée peut permettre aux cybercriminels de s'immiscer, en quelques minutes et jusqu'à une distance d'un kilomètre, dans le réseau de votre entreprise. Il convient de réglementer tout particulièrement l'utilisation de points d'accès publics et externes à Internet (HotSpots).

Activez le Bluetooth sur vos appareils (téléphones et ordinateurs portables, PC de poche) uniquement en cas de besoin et à l'abri des regards indiscrets. Autrement, votre appareil peut réagir à votre insu à des sollicitations étrangères (dans un rayon allant jusqu'à 100 mètres).

Trucs et astuces

- Modifiez le nom attribué par le fabricant au réseau local de connexion sans fil (Service Set ID – SSID). Le nouveau nom de devra en aucun cas contenir le nom de votre entreprise.
- Désactiver l'émission SSID pour que votre point d'accès ne soit pas visible à des tiers.
- Activez le cryptage du transfert de données sans fil (WPA2, Wi-Fi Protected Access 2). Modifiez le mot de passe standard de vos points d'accès.
- Utilisez le filtre d'adresses MAC pour que seuls les appareils connus puissent communiquer avec le point d'accès.
- Pour acheminer des données ultraconfidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN).
- Pour crypter ou chiffrer vos données, vous pouvez utiliser le produit Pretty Good Privacy (PGP). Les packages de solutions PGP pour les entreprises sont disponibles sur le site officiel http://www.pgp.com/de/index.html le package.
- Pour utiliser le logiciel libre OpenPGP, rendez-vous sur le site http://www.gnupg.org/index.de.html.

Expliquez vos directives pour l'utilisation des moyens informatiques !

Sans directives claires et contraignantes, vos collaborateurs ne savent pas ce qu'ils ont le droit de faire et de ne pas faire en tant qu'utilisateur informatique. Mais les règles ne sont véritablement prises au sérieux que si elles sont respectées par les supérieurs. Vous devez donc servir d'exemple pour tous les aspects liés à la sécurité.

Formulez par écrit les directives pour l'utilisation • _des moyens informatiques et faites-les signer par vos collaborateurs.

Abordez régulièrement le problème de la sécu• _rité dans votre entreprise en multipliant les approches.

Organisez des campagnes de sensibilisation sur • _ce thème une à deux fois par an. C'est facile à réaliser et cela nécessite très peu de moyens : courriels à tous vos collaborateurs, circulaires internes, affichage à la cantine, articles dans le journal de l'entreprise, etc.

Organisez une formation de base pour tous vos • _collaborateurs (en vous inspirant de cette brochure par exemple). Objectifs :

– avantages de la sécurité informatique
– création de mots de passe compliqués
– pratique sécurisée d'Internet et de
la messagerie électronique
– utilisation de l'antivirus
– classement des documents

La version papier ne suffit pas ! Vos collaborateurs • _doivent être régulièrement sensibilisés au problème de la sécurité.

Trucs et astuces

Réglementez l'installation et l'utilisation de pro• _grammes et matériel n'appartenant pas à la sphère de l'entreprise (jeux, économiseur d'écran, clés USB, modems, ordinateurs portables privés, connexions LAN sans fil, assistants personnels, etc.).

Réglementez la navigation sur Internet et définissez • _ce que vos collaborateurs peuvent ou non télécharger (informations, programmes, etc.).

Interdisez la fréquentation des salons de discus• _sions (chatrooms) et la consultation de sites aux contenus pornographiques, racistes ou violents.

Définissez le mode de sauvegarde des données, en • _particulier pour les utilisateurs d'ordinateurs portables (cf. point n°2).

Imposez la création de mots de passe (cf. point • _n°6).

Réglementez la gestion des mises à jour de sécurité • _et des logiciels antivirus (cf. points n°3 et 5).

Réglementez l'utilisation de la messagerie élec• _tronique : interdiction de transmettre des données confidentielles, de transférer des messages sur les boîtes de messagerie privées, de diffuser les chaînes de lettres etc.

Définissez le mode de gestion des données et infor• _mations confidentielles et organisez un archivage sécurisé de vos fichiers.

Définissez la procédure à suivre en cas d'incident • _lié à la sécurité (ex : alertes virus, vol ou perte d'appareils portables ou de mots de passe).

Informez vos collaborateurs des sanctions aux• _quelles ils s'exposent s'ils ne respectent pas ces directives.

Protégez l'environnement de vos infrastructures informatiques !

Savez-vous qui entre et qui sort de votre entreprise chaque jour ? Quelques dispositions suffisent pour éviter que n'importe qui puisse accéder à des informations commerciales importantes. Un système de sécurité visible est aujourd'hui un critère de qualité qui ne manquera pas d'inspirer confiance à vos clients et à vos fournisseurs. A quoi bon s'équiper du meilleur pare-feu, si des inconnus peuvent s'introduire dans vos bureaux ?

Tous les accès à vos locaux et au site de votre entre• _prise doivent être fermés ou surveillés. Si cela n'est pas possible, limitez-vous à la partie bureaux.

Ne permettez pas aux visiteurs, clients et connais• _sances de circuler sans surveillance dans votre entreprise.

Toute personne tierce à l'entreprise doit être ac• _cueillie à la réception, accompagnée pendant toute la durée de sa visite et raccompagnée jusqu'à la sortie.

Si vous n'avez pas de réception permettant • _de surveiller l'accès, il convient de verrouiller la porte d'entrée et d'apposer une plaque « Prière de sonner ».

Assurez-vous que toutes les ouvertures (fenêtres, • _portes, etc.) disposent d'un système de protection efficace contre les effractions. Vous trouverez des brochures d'information à ce sujet dans les postes de police.

Clés et badges doivent être correctement gérés et • _leur listes mises à jour. Soyez parcimonieux dans la distribution des clés passe-partout qu'il convient de réexaminer au moins une fois par an.

Les collaborateurs qui quittent définitivement • _l'entreprise doivent remettre leurs clés, badges et autres droits d'accès.

Trucs et astuces

Installez votre serveur dans un local climatisé et • _fermant à clé. Si cela n'est pas possible, enfermez le serveur dans un caisson (rack).

N'entreposez pas d'objets inflammables (papier • _par exemple) ni dans le local du serveur, ni à proximité.

Placez un extincteur au CO• _^{2} dans le local du serveur en veillant à ce qu'il soit bien en vue.

Ne placez pas d'imprimante réseau dans des • _pièces accessibles au public pour protéger vos documents des regards indiscrets.

Enfermez les câbles de connexion réseau qui tra• _versent les pièces accessibles au public. Même chose pour vos modems, stations centrales (hubs), routeurs et commutateurs.

Classez vos documents et vos dossiers !

Cela peut paraître surprenant au premier abord, mais ordre et sécurité vont de pair. On perd moins de documents sur un bureau bien rangé. C'est la même chose pour votre ordinateur et vous éviterez de perdre des données en établissant un système de classement bien ordonné.

Une méthode de rangement rationnelle permet de réduire le risque, de voir des documents sensibles ressurgir au mauvais moment ou être exposés par hasard à des regards indiscrets.

Un espace bien rangé est aussi une question d'image : vos clients et vos fournisseurs seront sensibles aux apparences et des bureaux bien rangés leur donneront l'idée d'une gestion ordonnée.

Classez vos fichiers électroniques et vos documents papier selon la même logique de rangement, par exemple par client ou par projet. Le système doit avoir une structure logique et compréhensible pour vos collaborateurs.

Lorsque vous faites sortir des données de votre entreprise, utilisez des supports de stockage neufs n'ayant encore jamais servi, car il est relativement facile de rétablir des fichiers supprimés de façon conventionnelle. Mieux vaut donc se prémunir des regards indiscrets. Actuellement, seul le programme « Wipe » est en mesure d'effacer définitivement vos données. Vous trouverez sur Internet toutes les informations concernant ce logiciel.

Effacez des différents supports de stockage (CD-Rom, DVD, clés USB, disques durs) les données électroniques dont vous n'avez plus besoin en écrasant l'ensemble de l'espace mémoire. La commande « Supprimer » ne suffit pas ! Le mieux est de détruire physiquement ces supports avant de vous en débarrasser.

Les documents confidentiels (contenant par exemple des données personnelles) doivent être conservés systématiquement sous clé.

Détruisez les documents sur support papier dont vous n'avez plus besoin, de même que les notes contenant des données sensibles (destructeur de documents).

Lorsque vous travaillez à l'ordinateur sur des données sensibles, positionnez votre écran de sorte que vos collègues ou des visiteurs ne puissent pas lire ce qui y est affiché.

Pendant les pauses ou en cas d'absence, verrouillez l'accès de votre ordinateur par un mot de passe et mettez vos documents confidentiels sous clé.

Ne laissez pas traîner des documents imprimés sur l'imprimante, surtout si cette dernière est installée dans des espaces accessibles au public (accueil, etc.).

Trucs et astuces

10 points supplémentaires pour améliorer la confidentialité et la disponibilité de vos données !

Vous pensez que votre entreprise a de nouveaux besoins en matière de sécurité et qu'elle nécessite des mesures complémentaires ? Les points suivants vous aideront à évaluer la nécessité de mesures de sécurité supplémentaires. Ces mesures sont exposées dans les pages ci-après.

Protégez votre entreprise en prenant des mesurespour améliorer la **confidentialité**, si

la législation vous y contraint (comme par ex. la loi sur la protection des données ou sur le droit d'auteur) ;• _

l'utilisation malintentionnée de données confidentielles sensibles pourrait comporter d'importantes pertes • _financières et/ou porter préjudice au crédit et à la réputation de votre entreprise, comme par exemple la révélation de secrets d'entreprise ou d'offres commerciales ;

le détournement de données se rapportant à une personne aurait des conséquences considérables sur le • _statut social ou la situation économique de cette personne, comme par exemple la publication de fichiers clients confidentiels ;

de par son activité, votre entreprise se doit généralement de respecter le caractère confidentiel des informa• _tions maniées, comme c'est le cas par exemple pour les entreprises de conseil en personnel, les associations, les centres hospitaliers, des organismes fiduciaires, les cabinets médicaux et juridiques, etc.

Lire tout particulièrement les points 11-15 présentés dans les pages suivantes.

Protégez votre entreprise en prenant des mesurespour améliorer la **disponibilité**, si

une panne de votre système informatique pourrait paralyser votre entreprise au point de provoquer un dommage • _global important (comme par exemple des retards de livraison dus au traitement des commandes au ralenti) ;

une défaillance des applications informatiques pourrait se traduire par une perte de confiance ou de réputation • _(par ex. panne du système de réservation d'une agence de voyage ou panne du serveur Internet) ;

la panne d'une application ou du système informatique pourrait mettre directement en danger l'intégrité des • _personnes (par ex. panne d'un système automatique de fermeture) ;

de par son activité, votre entreprise se doit généralement de garantir la disponibilité des informations • _maniées, ce qui par exemple le cas pour les exploitations, les entreprises commerciales, les imprimeries et les boutiques en ligne.

Lire tout particulièrement les points 16 – 20 présentés dans les pages suivantes.

www.isss.ch

Respectez les règles !

En matière de confidentialité, une entreprise doit s'engager à respecter un certain nombre de règles pouvant émaner de la loi, d'obligations contractuelles ou autres directives. Le non-respect de ces règles peut avoir des conséquences judiciaires pour l'entreprise et nuire à son image.

Il convient de prendre en compte tout particu• _lièrement la Loi sur la Protection des Données (LPD), la Loi sur le Droit d'Auteur (DLA) et le Droit des Obligations (DO).

Lorsque des informations personnelles sur des • _clients ou des collaborateurs par exemple sont traitées de quelque manière que ce soit, il convient de se référer à la loi fédérale sur la protection des données.

Selon la loi sur la protection des données, ces • _informations doivent être protégées par un dispositif technique et des mesures appropriées contre une utilisation par des personnes non-autorisées. Par ailleurs, l'entreprise s'engage à garantir l'exactitude des données conservées.

Attention également aux contrats avec vos • _clients et partenaires : ils peuvent contenir des clauses spéciales de confidentialité.

Trucs et astuces

Familiarisez-vous avec la législation et la réglemen• _tation en vigueur. Prenez les dispositions nécessaires pour vous conformer à la législation.

Assurez-vous que les données ont été collectées • _conformément à la loi et que les informations conservées sont exactes.

Permettez aux personnes concernées de se ren• _seigner sur le contenu des données conservées.

Vous trouverez d'autres informations à ce sujet • _sur le site Internet du Préposé Fédéral à la protection des données et à la transparence (http://www.edoeb.admin.ch/) et sur le site du préposé à la protection des données du canton de Zurich (http://www.datenschutz.ch).

L'analyse des besoins de protection proposée par • _l'Unité de stratégie informatique de la Confédération (USIC) vous aidera à d'évaluer convenablement vos besoins en la matière (http://www.isb.admin.ch/themen/sicherheit/00151/00174/index.html).

Réglementez la protection de l’accès aux données !

Mettez votre entreprise à l’abri des accès non-autorisés et protégez vos données pour que seules les personnes habilitées puissent y accéder.

Quiconque accède à des données sans autorisa• _tion est susceptible de les consulter, de les copier, de les modifier ou de les supprimer, ce qui peut avoir des conséquences désastreuses. Imaginez un peu que votre offre commerciale tombe entre de mauvaises mains, que votre fichier clients soit effacé ou que les résultats de vos recherches atterrissent sur le bureau de votre concurrent.

Etablissez qui est habilité à accéder à telles ou • _telles ressources informatiques ou informations.

Il convient d‘attribuer les droits d‘accès selon la • _fonction occupée (secrétariat, vente, comptabilité, ressources humaines, administrateur système).

On prendra soin par ailleurs d‘accorder unique• _ment les droits d’accès nécessaires à l‘exécution des tâches de chacun (selon le principe de connaissance sélective).

Les droits d’accès doivent être accordés à travers • _un régime d’autorisation informatique ou une administration supérieure.

Trucs et astuces

Introduisez un système de classement des don• _nées.

Les droits d’accès seront établis à chaque fois par • _la personne responsable.

Le régime des autorisations doit faire l’objet d’une • _documentation. Il s’agit de consigner, pour chacun de vos collaborateurs, la fonction occupée au sein de l’entreprise et les droits d’accès correspondants. Ces autorisations devront être régulièrement passées en revue pour être adaptées le cas échéant à la situation courante.

Optez pour une méthode d’authentification forte • _combinant un nom d’utilisateur, un mot de passe et un troisième élément de sécurité comme une carte à puce par exemple.

Lorsque des collaborateurs quittent définitivement • _l’entreprise ou dans le cas de changements dans l‘organigramme interne, il convient de bloquer ou de modifier les comptes d‘utilisateur correspondants, ainsi que les droits d’accès qui vont avec.

Les comptes des responsables systèmes et des • _administrateurs feront bien sûr l’objet d’une attention particulière, dans la mesure où ils disposent généralement de droits très étendus.

Verrouillez l'accès à vos appareils portables et cryptez les données lors des transferts !

Le transfert non sécurisé de données confidentielles (par courriel par ex.) risque de les soumettre à des regards plus ou moins indiscrets. En cas de perte de votre ordinateur portable, vos données risquent de tomber dans de mauvaises mains. Pour garantir la confidentialité de vos données, vous devez procéder à leur cryptage aussi bien pour les stocker sur vos ordinateurs portables que lors des transferts.

Les courriels peuvent être lus par des tiers. Il con• _vient donc de crypter les messages dont le contenu est confidentiel.

Lorsque vous conservez des données confiden• _tielles – en particulier sur des ordinateurs portables, smartphones ou assistants personnels, il est nécessaire d'utiliser un système de cryptage ou de verrouillage. De cette manière, les informations ne seront accessibles qu'aux utilisateurs en possession du mot de passe ou de la clé de décryptage.

Trucs et astuces

Réglementez le système de verrouillage en faisant • _l'inventaire des données et des ordinateurs de l'entreprise qu'il convient de verrouiller. Formez vos collaborateurs sur le système de verrouillage. Réglementez également le système de déverrouillage, afin que les données archivées restent accessibles. En cas de départ définitif de l'entreprise, assurez-vous que vos anciens collaborateurs n'emportent pas avec eux une clé de verrouillage ouvrant l'accès à des données cryptées.

Installez un logiciel de cryptage ou de verrouillage • _sur tous vos appareils contenant des données sensibles. Le verrouillage doit se baser sur un mot de passe compliqué (cf. point n°6).

Utilisez un logiciel de cryptage pour vos courriels • _au contenu confidentiel.

Une solution simple consiste à regrouper des don• _nées sensibles dans un dossier compressé dont on verrouillera l'accès. On veillera ensuite à transmettre le mot de passe à travers un autre système de communication que les données, par exemple le dossier compressé par courriel et le mot de passe par SMS).

Vous pouvez également recourir à la solution Pretty • _Good Privacy (PGP). C'est un produit qui a fait ses preuves et qui dispose de fonctions techniquement avancées pour le cryptage, la signature numérique et la suppression sécurisée des données. Les packages de solutions PGP pour les entreprises sont disponibles sur le site officiel http://www.pgp.com/de/index.html.

Pour utiliser le logiciel libre OpenPGP, rendez-vous • _sur le site http://www.gnupg.org/index.de.html.

Gérez les documents non électroniques de façon confidentielle !

Pour les données électroniques comme pour les documents sous forme papier, la prudence est de mise. Alors protégez bien vos données confidentielles et faites en sorte que rien ne filtre.

Tout document a son propriétaire et sa place • _dans le classement. Les documents doivent être classés, verrouillés pour n'être accessibles qu'aux personnes autorisées et correctement détruits lorsqu'ils ne sont plus utilisés.

Les documents papier doivent être conservés en • _lieu sûr, c'est-à-dire sous clé.

Lorsqu'ils ne servent plus, les documents papier au • _contenu confidentiel doivent être soigneusement supprimés dans un destructeur.

Les conversations doivent également être traitées • _dans la confidentialité, comme par exemple lors de propos échangés en public. Avisez vos collaborateurs de la nécessité de rester discret dans les espaces ouverts au public afin d'éviter les risques de fuites d'informations confidentielles.

Attirez l'attention de vos collaborateurs sur les • _aspects de l'ingénierie sociale (« Social Engineering » en anglais, pratique consistant à manipuler des personnes dans l'objectif d'en tirer des informations protégées) et de l'espionnage. Les problèmes de confidentialité ne doivent jamais être traités à la légère ou de façon irréfléchie.

Trucs et astuces

Vos documents papier doivent être classés eux • _aussi.

A partir du moment où l'on travaille sur des infor• _mations confidentielles, on doit être équipé d'un destructeur de document.

Conservez vos documents dans un lieu sûr, dans • _une armoire de rangement avec serrure.

Conservez les documents confidentiels dans une • _armoire fermant à clé ou au coffre, qu'il s'agisse de documents sur support papier ou sauvegardés sur des supports de stockage amovibles.

Sensibilisez vos collaborateurs !

Vos collaborateurs n'appliqueront les mesures de sécurité que s'ils sont sensibilisés au problème. Expliquez-leur la raison de ces mesures et le comportement à adopter lorsqu'ils ont à traiter des données confidentielles. Faites-leur signer, le cas échéant, un accord de confidentialité.

Vos collaborateurs, qu'ils soient internes ou ex• _ternes à l'entreprise, manipulent souvent des données confidentielles. Ces personnes doivent donc avoir bien clair à l'esprit les mesures à adopter pour garantir la confidentialité des informations traitées.

Incluez une clause de confidentialité dans le con• _trat de travail de vos collaborateurs. De même, créez un cadre contractuel pour régir vos rapports avec collaborateurs externes et partenaires. Cet accord de confidentialité fixe les règles relatives à la protection et à l'utilisation des informations confidentielles. Attirez leur attention sur les conséquences d'une infraction à ces règles.

Informez les personnes concernées sur le cadre • _juridique (par ex. la loi sur la protection des données).

Trucs et astuces

Sensibilisez les nouveaux collaborateurs dès leur • _embauche aux questions liées à la sécurité de l'information

La sensibilisation est un processus qui s'inscrit • _dans le temps, d'où la nécessité d'organiser régulièrement des campagnes sur ce thème, à travers notamment de formations, sondages, circulaires d'information, brochures, etc.

Vous pouvez pour cela recourir à des tiers, • _comme par exemple ISSS http://www.isss.ch.

Vérifiez vos systèmes informatiques !

Votre système informatique doit toujours être opérationnel à 100%. Pour cela, il doit faire l'objet d'une maintenance préventive et régulière qui diminuera le risque de pannes et de préjudices.

- Contrôlez régulièrement l'opérationnalité de votre système informatique. Le système de backup est-il au point ? Les données sauvegardées sont-elles effectivement lisibles ? Le système d'alimentation sans interruption (ASI) est-il opérationnel ? Il y a-t-il des messages d'erreur dans l'historique système ?
- Les aspects organisationnels sont également à prendre en compte : les dispositions réglementaires sont-elles respectées ? Le plan d'urgence a-t-il été vérifié ?
- Vous pouvez vous charger vous-même de la maintenance des appareils et des systèmes ou bien faire appel à des partenaires spécialisés (par ex. fournisseur). Dans ce dernier cas, sélectionnez des partenaires fiables et accordez-leur uniquement des droits d'accès limités.
- Les opérations de contrôle et de maintenance doivent avoir lieu à intervalles réguliers.

Trucs et astuces

- Etablissez une liste de contrôle pour suivre le déroulement des opérations de maintenance. Ces dernières doivent être contrôlables et compréhensibles.
- Le contrôle des systèmes peut être automatisé jusqu'à un certain point. Un logiciel par exemple peut envoyer un message d'alerte à l'administrateur en cas de dépassement d'une valeur critique.
- Faites signer un accord de confidentialité au personnel externe chargé de la maintenance.
- Evitez dans la mesure du possible que des personnes externes aient accès à des données et informations de l'entreprise.
- Informez les personnes concernées sur les travaux de maintenance à venir.

Equipez vos ordinateurs d’une alimentation sans interruption !

Si votre activité nécessite de hauts niveaux de disponibilité de vos données et de vos systèmes informatiques, vous devez tout faire pour éviter une panne de courant. Une alimentation sans interruption (ASI) protège vos systèmes informatiques d’une coupure de courant et des surcharges (foudre), permettant ainsi d’éviter la perte de données.

L‘appareil d’alimentation sans interruption (ASI) • _doit être installé entre la source d’électricité habituelle et les appareils à protéger.

En cas de panne de courant, la batterie de l’ASI • _prend le relais et se charge d’alimenter les composants de façon à ce qu’ils puissent s’éteindre normalement.

Par ailleurs, les ASI permettent de stabiliser la ten• _sion d’alimentation de vos appareils.

Votre serveur bien sûr, mais aussi d’autres péri• _phériques importants doivent être équipés d’un appareil ASI,: comme les principaux ordinateurs d‘un réseau, le routeur, le système de backup, etc.

Trucs et astuces

Faites l’inventaire des composants qui doivent être • _branchés sur l’appareil de secours ASI.

Cette liste vous permettra de déterminer la puis• _sance nécessaire de votre appareil USV.

Contrôlez régulièrement les batteries de l’appareil • _ASI et remplacez-les le cas échéant (cf. point n°16).

Misez sur la redondance des modules importants !

Un serveur qui tombe en panne par exemple peut avoir de graves répercutions économiques et paralyser votre entreprise. Beaucoup d'entreprises ignorent à quel point elles dépendent de certains matériels informatiques essentiels. Pour permettre à votre entreprise de reprendre son activité le plus vite possible après une panne, il est recommandé de disposer de systèmes redondants (disques durs, composants de réseau ou serveurs complets).

La redondance signifie que vous disposez d'au moins • _un appareil ou système de rechange identique à même de prendre la relève en cas de panne.

Pour prévenir une panne de disque dur, on peut • _recourir à la méthode de la mise en miroir de disques. En cas de défaillance du disque dur de travail, d'autres disques durs prennent automatiquement le relais, sans interrompre les activités en cours.

Souscrivez des contrats de service après-vente • _avec vos fournisseurs de matériel informatique et de logiciels dans lesquels vous préciserez bien les temps de réaction, les délais de livraison, etc.

Vous pouvez également élaborer avec eux des • _scénarios d'urgence (cf. point n°19).

Trucs et astuces

N'utilisez que des composants de marques recon• _nues, dans la mesure où ils sont généralement de bonne qualité, ayant été soumis à des tests intensifs.

Au-delà de la redondance de vos systèmes infor• _matiques, songez également à une connexion Internet redondante.

L'essentiel est que vos modules de secours soient • _identiques et qu'ils soient préconfigurés afin de pouvoir prendre immédiatement le relais.

Etablissez un plan d'urgence !

Personne n'est à l'abri d'une catastrophe et on se sent souvent impuissant face aux situations les plus graves. Mais savoir quel comportement adopter en cas d'urgence peut permettre de limiter le sinistre. Pour cela, il est nécessaire de planifier à l'avance la conduite à tenir et les actions à mettre en oeuvre.

Envisagez les situations d'urgence qui pourraient • _se présenter dans votre entreprise et réfléchissez à la façon dont il faudrait réagir dans les différents cas. Imaginez les scénarios suivants : panne du système informatique, incapacité du personnel, perte des postes de travail ou des locaux et défaillances de partenaires externes et prestataires de services.

En cas d'urgence, il faut donner l'alerte rapide• _ment et agir vite. Chacun doit savoir exactement qui est la personne responsable et qui alerter. Pour cela, établissez un plan d'alerte et une note technique sur la répartition des responsabilités.

Votre plan d'urgence doit prévoir les mesures • _à prendre pour l'activation du plan d'urgence, la gestion de la situation d'urgence et le rétablissement rapide du fonctionnement normal de l'entreprise.

Enseignez à vos collaborateurs la conduite à sui• _vre en cas d'urgence et les premières mesures qu'ils doivent prendre.

L'homme réagit souvent de façon intuitive en • _situation de stress. C'est pourquoi il convient d'entraîner sa capacité à adopter la bonne conduite en situation critique.

Pour les risques importants, il peut être intéres• _sant de souscrire une assurance informatique, pour vos installations par exemple, ou bien une police supplémentaire pour couvrir les frais pour les supports de données et le remplacement du matériel endommagé.

Trucs et astuces

Documentez régulièrement tous vos composants • _informatiques. Cette documentation doit être conservée à l'extérieur de l'entreprise.

Etudiez un mode de fonctionnement dégradé pour • _les systèmes informatiques. Celui-ci devra garantir un haut niveau de disponibilité afin de permettre une prompte reprise de l'activité.

Testez le temps de réaction du système de secours • _selon vos besoins en disponibilité. Une panne de serveur peut-elle être vraiment réparée dans les temps ?

Impliquez vos fournisseurs et fabricants dans • _l'élaboration des plans d'urgence (cf. point n°18).

Diffusez le savoir-faire !

Dans les PME de plus petite taille, les connaissances informatiques stratégiques sont souvent détenues par une seule et même personne. En cas d'absence ou de départ de cette dernière, l'entreprise risque de se trouver en difficulté.

Le savoir stratégique repose sur la capacité à con-
figurer, faire fonctionner et entretenir les systèmes informatiques d'une entreprise.

La maladie, un accident, un décès ou le départ de votre responsable informatique peut provoquer la perte de ce précieux savoir.
Faites en sorte que le savoir stratégique soit documenté et partagé par plusieurs personnes.

Trucs et astuces

Veillez à ce que les procédures et systèmes importants fassent l'objet d'une documentation appropriée. Cela facilitera les successeurs et nouveaux collaborateurs à se repérer rapidement.

Cette documentation contiendra notamment une liste des utilisateurs, des groupes et des différentes autorisations (cf. point n°12), le plan du réseau, les configurations système, la description des installations, les concepts, les procédures de travail et la description des postes d'intérêt stratégique pour la sécurité. Procédez régulièrement à la mise à jour de cette documentation.

Utilisez un système de nommage unitaire dans le cadre de la documentation technique et indiquez pour chaque fiche le numéro de la version, la date, le motif de révision et le nom de son auteur.

Etablissez un plan de votre réseau avec indication de votre serveur et des différents composants.

Conservez les mots de passe importants en double dans un coffre.

Sécurisez les informations significatives liées aux activités de vos collaborateurs démissionnaires.

Glossaire

Accès à distance accès à un réseau ou à un ordinateur distant, généralement via Internet. Ces accès devraient toujours être sécurisés, grâce notamment à des pare-feux ou à la technologie VPN.

Adresse IP adresse numérique permettant d'identifier un ordinateur dans un réseau (Internet par ex.).

ADSL Connexion rapide à Internet. Avec ce type de raccordement, l'ordinateur est connecté en permanence à Internet et peut donc être attaqué à tout moment. La première mesure de protection à prendre est d'équiper l'ordinateur d'un pare-feu.

Antivirus (ou scanner de virus) Programme chargé de protéger l'ordinateur contre les virus, vers et chevaux de Troie.

Attachment (pièce jointe) fichier joint à un courriel. De nombreux programmes malfaisants (malware, crimeware) sont ainsi diffusés. Ils s'activent au moment où l'utilisateur ouvre le message ou le fichier joint. Avant d'ouvrir une pièce jointe, il convient donc de s'assurer que l'expéditeur est bien connu de l'utilisateur et que l'ordinateur est doté d'un antivirus actualisé.

Audit procédure d'évaluation permettant de vérifier le bon fonctionnement des systèmes et processus internes face aux exigences et aux directives de l'entreprise.

ASI (alimentation sans interruption) dispositif intercalé entre le réseau de distribution de l'électricité et l'ordinateur pour servir de batterie de secours en cas de coupure de courant et le protéger des microcoupures ou autres fluctuations électriques.

Backup procédure de stockage des données sur des supports externes. En créant ainsi une copie de sauvegarde, on se protège contre une perte de données éventuelle.

Bluetooth Technologie radio courte distance pouvant être utilisée par les ordinateurs portables et les téléphones mobiles pour échanger des données.

Browser (navigateur) logiciel conçu pour consulter les informations contenues sur le Web (ex. : Internet Explorer, Opera ou Firefox).

Carte à puce carte en plastique portant un circuit intégré (la puce) permettant de stocker des données qui ne seront débloquées qu'après avoir tapé un code confidentiel.

Clé USB support de stockage qui se branche sur le port USB de l'ordinateur. Du fait de sa petite taille et de sa capacité de stockage élevée, elle est notamment utilisée pour le vol de données.

Client ordinateur relié à un réseau et connecté à d'autres ordinateurs.

Cheval de Troie dangereux logiciel malveillant qui s'introduit et s'exécute subrepticement sur l'ordinateur d'un utilisateur De cette manière, un cybercriminel (cracker) peut prendre, à distance, le contrôle total de l'ordinateur. La première mesure de protection à prendre est d'équiper l'ordinateur d'un scanner de virus.

Cracker un pirate informatique qui profite de ses connaissances et de son expérience pour nuire à autrui.

Crimeware terme général pour désigner des programmes utilisés par des cybercriminels pour nuire à des utilisateurs informatiques. Ces programmes servent les plus souvent à voler de l'argent ou des informations précieuses (par ex. des numéros de cartes de crédit). Les spyware appartiennent également à cette catégorie de logiciels mais présentent une forme moins agressive.

Download (téléchargement) processus permettant à un utilisateur de recevoir sur son ordinateur des données et des programmes provenant d'un ordinateur distant (par ex. sur Internet).

Firewall (pare-feu) appareil ou logiciel chargé de protéger un ordinateur ou un réseau contre des attaques venant de l'extérieur (par ex. d'un cracker).

Hacker spécialiste informatique dont les connaissances techniques faramineuses lui permettent de reconnaître des failles dans les ordinateurs ou les réseaux et de les exploiter. Contrairement à un cracker, le hacker n'a pas d'intentions illégales.

Hub appareil permettant d'interconnecter plusieurs ordinateurs pour former un petit réseau.

Instant Messenger (messagerie instantanée) programme permettant d'échanger de brefs messages textuels en temps réel.

ISDN réseau de télécommunication numérique permettant de transmettre des voix et des données à une vitesse supérieure et avec une sécurité accrue par rapport à la technologie analogique traditionnelle.

Junk-Mail (pourriel) courrier électronique indésirable, le plus souvent publicitaire, également désigné sous le terme de spam.

Login (authentification) processus d'identification auprès d'un système faisant intervenir généralement un nom d'utilisateur et un mot de passe.

Malware également connu sous le terme de maliciel. Terme générique pour désigner des logiciels malveillants et nuisibles, comme par exemple les virus, les vers ou les chevaux de Troie.

Modem périphérique servant à convertir des signaux électriques en données analogiques et inversement. Il est utilisé pour établir la connexion entre des lignes téléphoniques analogiques et des réseaux numériques (Internet par ex.). On parle aussi de modem ADSL ou modem câble.
Modem câble type de modem permettant de se connecter à Internet par le biais du réseau de télévision par câble.
Nom d'utilisateur (Username) il est la plupart du temps lié à un mot de passe dans les procédures d'authentification (login) sur un site Internet ou pour l'accès à un programme.
Patch (correctif) mise à jour d'un programme dans lequel on a découvert des erreurs. Voir aussi update.
PGP (Pretty Good Privacy) en anglais, « plutôt bonne intimité ») . Programme de cryptage des données.
Pharming attaque informatique plus redoutable que le phishing, où l'ordinateur de la victime est détourné complètement à l'insu de son utilisateur, au point que seuls des professionnels de la sécurité et des réseaux sont à même de la déceler. Face à ce type de menace, il est vivement recommandé d'utiliser un antivirus, un pare-feu et d'effectuer quotidiennement les mises à jour de l'ordinateur.
Phishing dans ce type d'attaque, la victime est amenée à communiquer ses identifiants (login) à des services financiers en ligne (par ex. e-banking), soit par courrier électronique, soit par la visite d'un site leurre dont le graphisme imite parfaitement le site original.
Port donnée numérique permettant d'adresser un service à un ordinateur. C'est ainsi que l'on peut identifier clairement des

Sunrinse ou Cablecom.
RM (Risk Management) « gestion du risque » en français. Système de gestion des risques d'une entreprise à travers un processus d'analyse, d'actions et de contrôles).
Routeur périphérique servant à relier des réseaux entre eux. On parle aussi de routeur ADSL.
Scanner de virus programme permettant de détecter et d'éliminer les virus et autres parasites informatiques. Voir également antivirus et malware.
SCI sigle de Système de Contrôle Interne décrit à l'art. 728 a (CO) ; ensemble des mesures de contrôle au sein de l'entreprise pour la réalisation de ses objectifs.
Serveur dans un réseau informatique, le serveur est l'ordinateur qui met des services à la disposition d'autres ordinateurs (Clients), comme par exemple le serveur de messagerie électronique.
Signature numérique signature permettant d'authentifier irrévocablement l'auteur d'un document électronique.
Spam courrier électronique non sollicité envoyé en masse sous forme de lettre-chaîne ou de publicité pour des produits ou services douteux. Pour se protéger, il existe des filtres antispam qui permettent de bloquer les courriers indésirables.
Spyware sorte de malware dont la fonction est d'espionner l'utilisateur d'un ordinateur. Grâce à ce logiciel espion, les cybercriminels peuvent observer en particulier son comportement sur Internet, voire même lire les touches qu'il tape sur le clavier (attention au vol de mot de passe !). Pour se protéger, il convient d'utiliser régulièrement un scanner de spyware.

faire fonctionner l'ordinateur et les applications (comme le traitement de texte ou le tableur).

Switch appareil servant à relier des ordinateurs ou des réseaux entre eux. Il est notamment utilisé dans les réseaux locaux (LAN).

Update (mise à jour) action qui permet de réparer des outils informatiques ou des programmes défectueux (comme le système d'exploitation par exemple). Voir aussi patch.

URL adresse d'une page Internet, par ex. www.isss.ch.

Virus programme le plus souvent malveillant (malware) qui détruit les données ou empêche le fonctionnement de l'ordinateur. Les virus se répandent à travers toutes les formes de transfert de données (Internet, disquette, CD-Rom, clé USB, courriel, etc.) et s'activent par une simple action de l'utilisateur. Pour se protéger, l'utilisateur doit installer un scanner de virus qu'il devra régulièrement mettre à jour.

VPN (Virtual Private Network) cette technologie de « réseau privé virtuel » permet de sécuriser, par le biais de clés de cryptage et de mots de passe, l'utilisation de réseaux publics (Internet par ex.) à des fins privées.

Ver programme malveillant (malware) qui se reproduit de façon autonome dans les réseaux informatiques en exploitant les failles des programmes. Cet hôte se manifeste généralement par le ralentissement des capacités de l'ordinateur. Mais les vers peuvent également détruire les données stockées sur l'ordinateur. La première mesure de protection à prendre est d'équiper l'ordinateur d'un scanner de virus.

Zombie ordinateur contrôlé à l'insu de son utilisateur (par un

ISSS Information Security Society Switzerland
Bollwerk 21
CH-3001 Bern
T +41 31 311 5300
sekretariat@isss.ch
www.isss.ch