Roger Hangartner
directeur, Hangartner & Partner AG, Freienbach
www.hangartner-partner.ch

Thomas Scheibmayr
Senior Security Consultant, Hangartner & Partner AG, Freienbach
www.hangartner-partner.ch

La sécurité IT dans l'entreprise est l'affaire du chef!

Les entreprises fiduciaires ne gèrent pas seulement les finances de leurs clients mais forcément aussi les données sensibles de leur clientèle.

Les dirigeants ne sont souvent pas conscients des risques que comportent le traitement et le stockage des données de clients pour l'entreprise. La divulgation par mégarde, la perte ou le vol d'informations de clients peuvent entraîner une perte de confiance, qui risque de compromettre l'entreprise. Les créances réclamées dans le cadre d'une action civile accélèrent en outre la ruine imminente. Les entreprises fiduciaires et d'autres PME n'accordent souvent pas suffisamment d'attention à la sécurité IT. Elles se fient en général à l'installateur de PC et présument qu'il a tout «réglé» correctement. La responsabilité pour l'entreprise n'est cependant pas assumée par le spécialiste IT, mais la devise qui s'applique est plutôt: la sécurité est l'affaire du chef!

Une fausse estimation largement répandue concerne le besoin de sécurité de l'entreprise. On entend souvent les affirmations suivantes:

«Nous n'avons encore jamais eu de problèmes.»
Cette affirmation est audacieuse. Peut-être n'a-t-on rien remarqué lors d'incidents de sécurité antérieurs!

«Il n'y a pas grand-chose à trouver chez nous, nos données ne sont pas si confidentielles.»
Cette estimation est dans la plupart des cas trop superficielle. Une analyse soigneuse des scénarios de sinistres possibles fait apparaître rapidement que l'entreprise traite également des données qui se prêtent à des abus de toutes sortes, si elles tombent entre de mauvaises mains. On ne tient en outre pas compte du fait que les données relatives aux clients de même que celles concernant les collaborateurs sont extrêmement sensibles et doivent, par conséquent, être hautement protégées!

«Notre réseau est sûr.»
Les aptitudes d'agresseurs potentiels sont souvent sous-estimées. S'y ajoute encore que même les spécialistes expérimentés en matière de réseaux et de sécurité ne savent pas tout et commettent parfois des erreurs. Les vérifications externes révèlent presque toujours les graves faiblesses et constituent une bonne protection contre «l'aveuglement professionnel».

«Nos collaborateurs sont dignes de confiance.»
Diverses statistiques révèlent cependant qu'il en est tout autrement: la plupart des violations de la sécurité sont commises par les collaborateurs internes ou externes. Ces derniers n'agissent souvent pas intentionnellement. Des dommages importants sont parfois également provoqués par mégarde, excès de zèle ou curiosité alliés à un manque de conscience des problèmes.
Vous devriez vous rendre compte que la sécurité n'est pas un état statique mais un processus permanent, qui est poussé en avant par l'apparition constante de nouvelles technologies ou des exigences changées. C'est pourquoi, vous devriez sans cesse vous poser les questions suivantes:

- Quelles sont les incidences sur votre entreprise, si l'un de vos collaborateurs passe à la concurrence avec votre fichier des clients fixes?
- Quelles sont les conséquences pour vous si des informations importantes sur des transactions financières de vos clients paraissent tout à coup dans la presse?
- Qu'arriverait-il si des ordinateurs ou d'autres composants IT importants de votre organisation devaient soudain tomber en panne et être inutilisables pendant une certaine durée (jours, semaines, etc.)? Pourriez-vous continuer à travailler? Quel serait le dommage éventuel?
- Qu'est-ce que cela signifierait pour vous si vous deviez constater lors des comptes annuels que beaucoup de données ont été mal traitées ou modifiées après coup par le système de comptabilité?

On pense couramment que les mesures de sécurité IT provoquent nécessairement des investissements élevés dans la technique de sécurité et le recrutement de personnel hautement qualifié. Cela n'est pourtant pas le cas. Les facteurs clés du succès sont cependant le bon sens, des réglementations organisationnelles bien pensées ainsi que des collaborateurs fiables et bien informés, qui respectent volontiers les exigences de sécurité de manière disciplinée et routinière. L'élaboration et l'application d'un concept de sécurité IT efficace et efficient ne doivent pas forcément être impayables. Les mesures les plus efficaces sont étonnamment simples et en outre souvent gratuites!

Les manquements les plus fréquents

Si l'on analyse les erreurs et les manquements typiques, on ne constate que de légères dépendances de la taille de l'entreprise et de la branche. A l'aide de la liste suivante, vous pouvez facilement vérifier quels manquements spécifiques jouent un rôle dans votre entourage et comment ces faits doivent être interprétés.

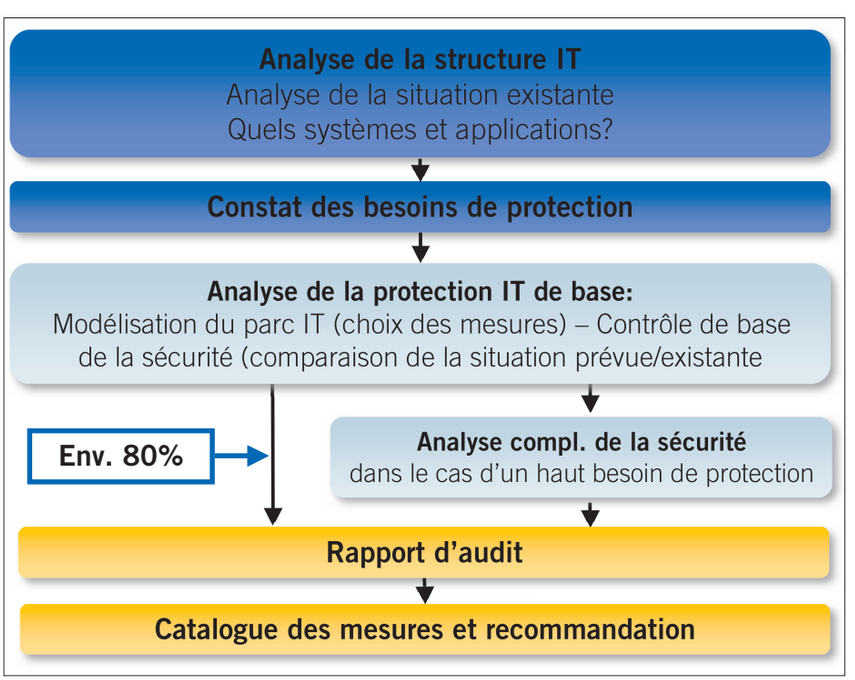
La sécurité revêt une faible importance
La sécurité IT revêt souvent une trop faible importance par comparaison à d'autres exigences (coûts, paresse, haute fonctionnalité, etc.). On considère au contraire la sécurité IT comme un facteur de coûts et un handicap. Notamment lors de nouvelles acquisitions, on néglige ou ignore souvent les caractéristiques de sécurité d'une application ou d'un système. Un exemple à ce sujet est le nombre augmentant à toute vitesse des réseaux sans fil non sécurisés, depuis que des cartes WLAN correspondantes bon marché sont à la disposition de tout un chacun. L'enthousiasme pour une nouvelle technique et la possibilité de renoncer à un câblage gênant font oublier les aspects de sécurité. D'innombrables entreprises «publient» ainsi involontairement leurs données confidentielles et proposent en partie à tous les intéressés des accès gratuits à Internet.

Les mesures de sécurité ne sont pas prises au sérieux par négligence
Les meilleures directives et fonctions de sécurité ne servent à rien, si elles ne sont pas observées ou utilisées. Les documents ou les e-mails confidentiels ne sont souvent pas chiffrés, bien que l'on dispose de mécanismes appropriés. Les utilisateurs trouvent les mots de passe sûrs, modifiés régulièrement tout aussi gênants que les économiseurs d'écran avec mot de passe. Un collaborateur quelconque, qui prétend être un nouveau collaborateur du département IT, se voit révéler des mots de passe, s'il les demande «gentiment».
Les données, notamment celles de notebooks, sont sauvegardées seulement rarement ou même jamais, quoique les utilisateurs connaissent parfaitement les hauts risques d'une perte de données. Même si l'on effectue régulièrement des sauvegardes de données, celles-ci sont souvent incomplètes ou incorrectes. Un contrôle par échantillons de la sauvegarde des données permettrait de supprimer ce gros risque! Lors de sauvegardes automatisées, les collaborateurs ne savent souvent pas quelles données doivent être sauvegardées à quels intervalles et quelle est la durée de conservation des médias de sauvegarde. Il y a beaucoup d'autres exemples similaires qui prouvent que même les mesures de sécurité simples sont vouées à l'échec, si leur application n'est pas acceptée ou ne peut être imposée sur le plan technique. Cela ne vaut malheureusement pas seulement pour les utilisateurs mais aussi pour les administrateurs.

Les mises à jour de sécurité disponibles ne sont pas installées
Beaucoup de dommages causés par des virus ou des vers n'apparaissent qu'au bout d'un certain temps après la découverte du virus. A ce moment, il existe en général déjà des correctifs de sécurité des constructeurs respectifs. Entre-temps, la plupart des produits disposent de correctifs de sécurité qui sont publiés à des intervalles très courts. La sélection et le test des correctifs effectivement pertinents dans le contexte de l'entreprise en question demandent du temps supplémentaire. C'est pourquoi, beaucoup d'administrateurs préfèrent attendre jusqu'à la disponibilité de la prochaine mise à jour ordinaire des logiciels et n'installent les correctifs de sécurité donc pas à temps. Un tel comportement n'est pas négligent mais plutôt gravement négligent.

Utilisation insoucieuse de mots de passe et d'informations d'accès
La plupart des procédés de protection d'accès sont réalisés sur la base de mots de passe. Cela provoque des problèmes si les utilisateurs choisissent des mots de passe peu sûrs (p. ex. trop courts ou faciles à deviner). Des infractions aux systèmes IT sont commises chaque jour, parce qu'un agresseur parvient à déchiffrer un mot de passe – par des essais systématiques, en devinant ou en espionnant. Le fait que les mots de passe sont souvent conservés sous le clavier ou dans le tiroir supérieur d'un bureau aide fortement les criminels ayant accès aux bureaux à s'emparer d'informations sensibles!

Protection insuffisante contre le vol ou les dommages causés par les éléments naturels pour les locaux et les systèmes IT
Les cambrioleurs et les voleurs n'ont que trop souvent beau jeu. Les fenêtres inclinées pendant la nuit, les locaux IT non fermés à clé, les visiteurs non surveillés ou les notebooks abandonnés dans une voiture offrent aux intrus des possibilités variées. La perte des données enregistrées est cependant généralement plus grave que la perte de matériel par vol ou vandalisme. Celles-ci ne peuvent être récupérées – si jamais – qu'au prix de gros efforts. L'entreprise court en outre le risque que le voleur abuse de données confidentielles. Des catastrophes comme des incendies ou des inondations sont certes des événements fort rares, mais si elles surviennent, les conséquences sont en général fatales. Les mesures anti-incendie, la protection contre les dégâts d'eau et la garantie de l'alimentation électrique devraient donc être considérées comme un élément clé de la sécurité IT.



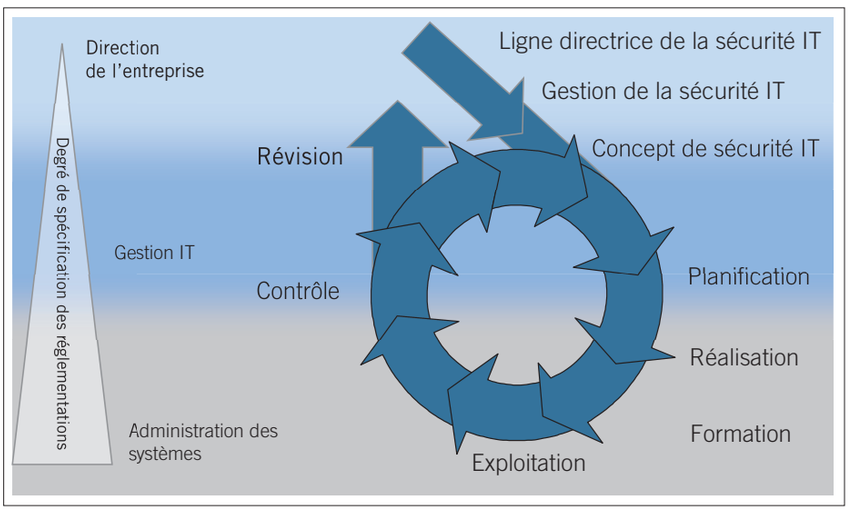
Le déroulement standardisé de l'audit de la sécurité permet une action structurée et rapide.

L'audit de sécurité comme situation de départ de l'amélioration de la sécurité IT

Les pires risques sont ceux qui ne sont pas reconnus comme tels, parce que des mesures de sécurité adéquates font défaut. Ces risques peuvent de ce fait causer de graves dommages à l'entreprise. Comme disait le capitaine du Titanic: «Il n'y a rien qui puisse causer un naufrage de ce navire. Je ne puis imaginer aucune catastrophe qui pourrait frapper ce navire.»
Tout comme les entreprises fiduciaires proposent des révisions à leur clientèle pour assurer l'observation des directives et des lois ainsi que pour garantir l'intégrité de la comptabilité, un contrôle de la sécurité IT passe l'entreprise au crible afin de détecter les faiblesses du traitement d'informations.
L'audit analyse tous les domaines du traitement d'informations tels que l'organisation, le personnel, les processus, la sauvegarde des données, la protection antivirus, l'infrastructure des bâtiments et de l'informatique, les télécommunications, les réseaux et bien plus. Le résultat des audits est un rapport d'audit composé d'une analyse détaillée de la situation ainsi qu'une liste de tous les manquements et des mesures correspondantes. Le catalogue des mesures priorisées en fonction des besoins spécifiques à l'entreprise permet l'application immédiate et durable des mesures de sécurité. La mise en pratique peut être effectuée par le partenaire IT favori, de préférence sous la direction d'un spécialiste en sécurité IT.

La sécurité IT en tant que processus constant

La plupart des entrepreneurs disposent d'une ligne directrice qui sert à définir la stratégie et les objectifs de l'entreprise. Ils doivent également définir une stratégie de sécurité IT sur la base de cette stratégie d'entreprise. Celle-ci décrit grossièrement quelles parties de l'entreprise revêtent une importance commerciale critique dans le domaine IT et nécessitent donc une protection particulière. En partant de cette ligne directrice en matière de sécurité, on peut définir les mesures de sécurité IT, les évaluer (esprit de risque) et finalement les appliquer en fonction de leur priorité.
Pour garantir le niveau de sécurité visé à long terme, les mesures de sécurité IT implémentées doivent sans cesse être actualisées. Il n'existe guère d'autre domaine caractérisé par une «obsolescence» aussi rapide du niveau de sécurité établi que l'environnement IT dynamique. Les enseignements tirés d'incidents de sécurité, de changements techniques ou organisationnels ainsi que les modifications des exigences posées à la sécurité ou de nouvelles menaces exigent des adaptations des mesures de sécurité IT existantes. Il faut en outre proposer aux collaborateurs des cours de sensibilisation à la sécurité IT ainsi que des formations pour l'utilisation de l'IT.
Seuls des audits réguliers de la sécurité sont en mesure de garantir que ces adaptations requises seront effectivement accomplies!



Le processus de sécurité IT doit être lancé par la direction de l'entreprise et contrôlé régulièrement.

L'utilité commerciale de la sécurité IT

Tout bon entrepreneur connaît ses risques, les évalue et prend des mesures adéquates. Le portefeuille des risques d'une entreprise ne comporte cependant pas seulement des risques, qui résultent de l'activité commerciale, mais aussi des risques dans le domaine IT. La valeur commerciale de la sécurité IT peut donc être mesurée à l'importance qu'un décideur accorde à la mise en pratique des mesures.
Il ne faut par ailleurs pas non plus ignorer les effets suivants résultant d'un concept de sécurité IT bien pensé et «vécu» dans la pratique:

- Si l'on aborde les clients avec des directives de sécurité claires – par exemple avec des directives concernant l'échange électronique de données – cette approche engendrera dans la plupart des cas un surplus de confiance et consolidera ainsi le partenariat. On peut dire en général qu'une sécurité IT confirmée inspire confiance aux clients et aux partenaires commerciaux et est aussi réclamée dans une mesure croissante par ceux-ci.
- Si une entreprise est concernée par l'accord Bâle II, sa solvabilité peut éventuellement s'améliorer, si les risques internes – qui comprennent aussi les risques IT – sont considérés comme étant très faibles.
- Les systèmes IT sont bien documentés, ce qui facilite sensiblement le travail quotidien des administrateurs système. Dans le cas d'un sinistre, les données peuvent être rapidement récupérées et mises à la disposition de l'utilisateur, ce qui maintient le surcoût dans des limites raisonnables. Les administrateurs et les utilisateurs connaissent en outre mieux leurs systèmes et travaillent donc plus efficacement.
- Last but not least: la qualité du travail augmente. La sécurité IT vécue favorise une culture d'entreprise où une action responsable, l'orientation vers les clients et l'identification avec les objectifs de l'entreprise sont solidement ancrées.

Conclusion

La sécurité IT est un thème qu'aucun entrepreneur ne doit ignorer. Il faut notamment accorder une attention particulière à ce thème dans des branches qui utilisent chaque jour des données sensibles de tiers. Il importe moins de faire tout ce qui est possible mais plutôt de courir délibérément certains risques. Un audit de sécurité révèle les risques IT spécifiques d'une entreprise et constitue ainsi la base d'une gestion solide des risques à faible coût. ■

La sécurité IT dans l'entreprise est l'affaire du chef! Agissez avant qu'il ne soit trop tard!