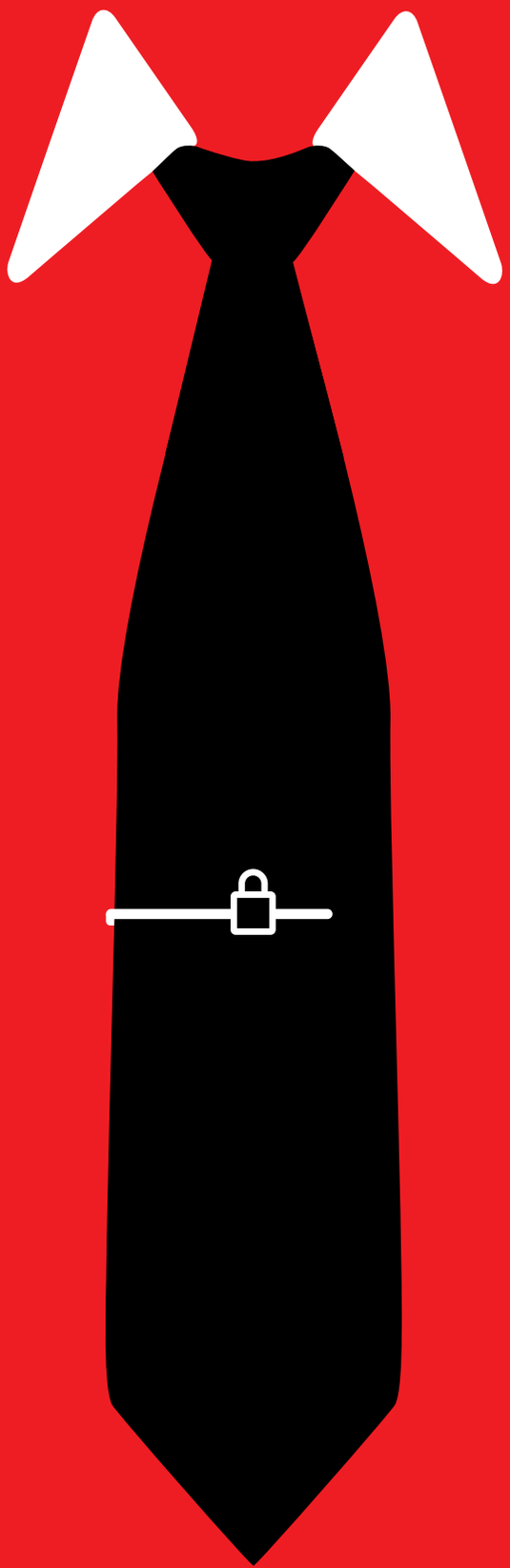


Sécurité informatique

une tâche de gestion

La révolution numérique a bouleversé non seulement la vie privée, mais aussi le monde de l'entreprise. Les autorités, institutions et organisations ne peuvent plus travailler sans soutien technique, voire sont totalement tributaires de ces technologies pour leurs activités. En conséquence, la sécurité informatique prend une place centrale parmi les tâches de gestion. Car si la technique ne fonctionne pas, l'entreprise n'a plus d'autre choix que de mettre la clé sous la porte. Pire encore, elle est exposée à des dangers qui vont au-delà du risque commercial normal.

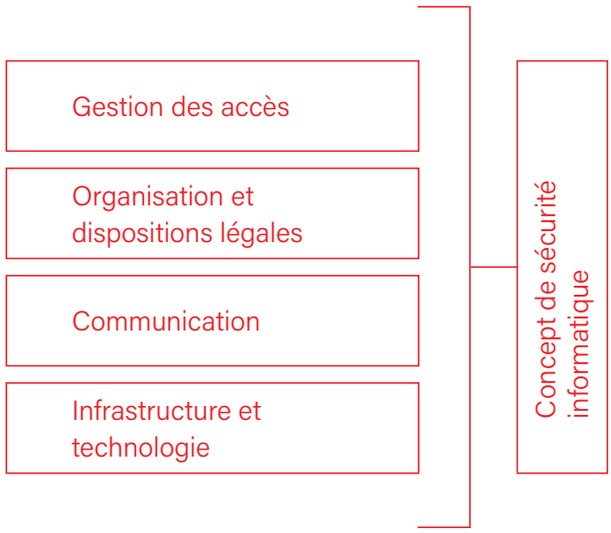
Selon une vaste étude menée par la Haute école d'économie de la Haute école spécialisée du nord-ouest de la Suisse (FHNW), 61 % des entreprises suisses considèrent la sécurité informatique et la protection des données comme le plus grand risque de la transformation numérique. Un tiers des entreprises interrogées ont même déclaré avoir été victimes, au cours des deux dernières années, d'un incident de type attaque contre l'infrastructure et les données informatiques. La plupart des attaques contre les données d'entreprise proviennent d'organisations criminelles ou financées par l'État, mais un nombre étonnamment élevé d'entre elles sont également le fait de collaborateurs (30 %).

L'opérateur du site «10 Guards» compile régulièrement les prix des données et prestations de services volées qui se négocient sur le darknet. Une sélection:
– carte de crédit avec code PIN: de 15 à 35 USD
– login pour opérations bancaires en ligne: de 35 à 65 USD
– compte PayPal: 200 USD
– carte d'identité européenne: 75 USD
– compte Facebook piraté: 75 USD
– compte Instagram piraté: 55 USD
– compte Gmail piraté: 156 USD
– logiciel malveillant: de 70 jusqu'à 6000 USD
– attaque DDoS sur un objectif quelconque: de 10 à 800 USD

Champs thématiques relatifs au propre concept de sécurité informatique

Concernant le propre concept de sécurité informatique, la discussion, la planification et l'implémentation de mesures mènent à quatre champs thématiques principaux (cf. illustration):

1. Le domaine Infrastructure et technologie comprend toutes les mesures techniques, les équipements utilisés, la manière dont ces derniers doivent être configurés et peuvent être protégés.



Champs thématiques de la sécurité informatique (N. Mayencourt & M.K. Peter)

2. La Communication couvre tous les aspects de l'interaction humaine – avec et sur les machines. Il s'agit là de savoir comment sensibiliser davantage le personnel et la direction aux problèmes de sécurité et aux comportements essentiels pour la sécurité.

3. Le champ Organisation et dispositions légales comprend les réglementations et prescriptions qui décrivent la façon dont les collaborateurs devraient se comporter et comment les processus au sein de l'organisation doivent être aménagés pour garantir la sécurité informatique. L'organisation doit également être conçue de manière à être en conformité avec les lois et normes internationales.

4. Quant à la Gestion des accès, toutes les mesures de sécurité reposent sur une série de contrôles: il s'agit ici de régler, contrôler et consigner l'accès aux systèmes et l'utilisation de ceux-ci. Les contrôles d'utilisation comprennent des mots de passe, des contrôles d'accès ainsi que l'authentification, l'autorisation et le décompte des demandes dans le périmètre du système informatique.

Ensemble, ces domaines composent au final le concept de sécurité informatique. Ils définissent les préparatifs nécessaires pour l'entreprise ainsi que leur mise en œuvre, et vérifient en permanence (cf. chapitre «IT-Sicherheitsaudit») si le concept correspond aux types d'attaques actuels, à l'infrastructure informatique actuelle et à l'acceptation des risques.

→

Télétravail à domicile

Avec l'apparition du COVID-19, les entreprises ont presque toutes dû s'intéresser à la question du télétravail et des défis spécifiques qui en découlent. Dans le cadre du home office également, les problèmes de sécurité informatique doivent être pris au sérieux. Ces problèmes sont en principe les mêmes que sur le lieu de travail. Toutefois, lorsque de nombreux collaborateurs travaillent depuis la maison, l'entreprise devient encore plus vulnérable aux attaques: les appareils et connexions privés deviennent partie intégrante du réseau de l'entreprise, et les espaces privés partie intégrante des locaux de l'entreprise. Partant, une intrusion dans les appareils privés ou au domicile des collaborateurs permet d'accéder aux données et à l'infrastructure de l'entreprise. Aussi les espaces et appareils privés ainsi que le comportement des collaborateurs en télétravail doivent-ils de même faire l'objet du concept de sécurité informatique de l'entreprise – chose qu'il n'est pas facile de mettre en œuvre ni de contrôler.

De premiers conseils importants sont énumérés dans l'encadré. Il est recommandé aux entreprises de sensibiliser et de former spécifiquement leurs collaborateurs œuvrant à domicile (et en travail mobile en général) à la sécurité informatique. Il est par ailleurs conseillé de mener un audit de sécurité informatique qui tienne également compte des aspects liés au télétravail.

RÈGLES IMPORTANTES DE COMPORTEMENT EN MATIÈRE DE TÉLÉTRAVAIL À DOMICILE

- Utilisez une connexion VPN, de sorte que les données transférées au système informatique de l'entreprise soient cryptées.
- Communiquez exclusivement via les comptes de l'entreprise et non via des comptes de messagerie privés ou des services de messagerie tels que WhatsApp.
- Verrouillez votre ordinateur, même si vous ne vous absentez que brièvement de la place de travail.
- Ne laissez traîner aucun imprimé ou document confidentiel.
- Ne téléphonez pas sur le balcon pour parler de sujets confidentiels.
- Cryptez les systèmes informatiques, les courriers électroniques et les supports de données (p. ex. clés USB).
- N'installez aucun logiciel / aucune application pour votre famille à des fins privées.
- Tenez à jour les logiciels et les antivirus de votre ordinateur portable.

Audit de sécurité informatique

Le terme «audit» désigne l'examen indépendant ainsi que l'implémentation des processus, exigences et lignes directrices. Un audit de sécurité informatique examine par conséquent l'existence, la qualité et le respect des mécanismes de sécurité informatique dans une entreprise. Dans les grandes entreprises, les audits sont généralement menés par des auditeurs indépendants, spécialement formés, et constituent une part de processus de gestion de la qualité souvent lourds.

Lors de la préparation d'un audit de sécurité informatique, il importe de ne pas perdre de vue l'objectif à atteindre. Un audit ne doit jamais devenir une fin en soi. Au contraire, il faut dès le départ bien réfléchir au but visé. Un objectif type peut être, par exemple, de prouver le respect des exigences légales ou réglementaires, ou encore d'obtenir ou de conserver des certifications. On parle ici souvent de «compliance», autrement dit de conformité. Une fois prise, la décision d'effectuer un audit de sécurité informatique pour augmenter la résilience et protéger la chaîne de création de valeur doit être consignée et communiquée. L'intention déclarée de l'audit devient dès lors le point central de toutes les discussions et décisions à venir. Il s'accompagne en outre d'attentes réalistes: il n'existe pas de protection absolue contre tous les dangers – seul qui ne fait rien ne risque rien. Or comme ne rien faire ne saurait être une option viable, il convient de trouver un équilibre en protégeant la chaîne de valeur du mieux possible et en minimisant les risques voire, idéalement, en les éliminant totalement moyennant des mesures efficientes en termes de coûts. La règle qui fait foi: autant que nécessaire, aussi peu que possible.

Hormis certaines pratiques de sécurité universelles, le choix des mesures de sécurité informatique appropriées dépend fortement de la situation propre à chaque entreprise. La bonne nouvelle est que le moyen d'identifier ces mesures reste plus ou moins identique pour toutes les entreprises. Dans un premier temps, il faut déterminer où et comment sont générés les chiffres d'affaires, à quels risques ils sont exposés au niveau de l'informatique et quelles mesures prendre pour se prémunir là-contre. Pour l'analyse des risques et la planification de mesures, il sera nécessaire, le cas échéant, de faire appel à des experts.

Les audits de sécurité informatique revêtent de nombreuses formes. On peut citer, entre autres, les modèles suivants:
– Pour un test de pénétration, les experts en sécurité se placent dans la perspective d'un cambrioleur. Ils cherchent des moyens de pénétrer dans les domaines protégés du réseau afin, par exemple, d'en extraire des données confidentielles.
– Dans un audit ciblé, le test de sécurité porte sur un domaine du réseau, une certaine composante, un logiciel ou une application.
– Dans le cadre d'un audit complet, l'ensemble de l'infrastructure est intégralement examiné ou analysé, aux fins de détecter les vulnérabilités et faiblesses.
– Lors d'un travail d'équipes rouge/bleue, l'équipe rouge attaque l'infrastructure informatique d'une entreprise, tandis que l'équipe bleue tente de repousser l'attaque. Cette simulation révèle tant les points faibles que la résilience des mesures de sécurité informatique.

Pour plus d'informations:
www.it-sicherheit-kmu.ch
www.dreamlab.net

Marc K. Peter, professeur à la Haute école d'économie de la FHNW, Olten, et Nicolas Mayencourt, fondateur et directeur général de Dreamlab Technologies

MANUEL PRATIQUE DE SÉCURITÉ INFORMATIQUE

Le manuel pratique «IT-Sicherheit für KMU» (Sécurité informatique pour les PME), paru aux éditions Beobachter & Handelszeitung, s'adresse spécifiquement aux petites et moyennes entreprises suisses et leur montre comment se prémunir contre les attaques informatiques. Trois études de cas fictives, dont l'une appliquée à un bureau d'ingénierie, aident à présenter de manière simplifiée les contenus techniques, concepts et applications du manuel pratique et à les rendre plus compréhensibles.

Seules une discussion et une planification actives permettent aux entreprises de faire de la sécurité informatique un avantage concurrentiel; la sécurité informatique devient ainsi une tâche de gestion.

«IT-Sicherheit für KMU – So navigieren Sie Ihr Unternehmen sicher durch Cyber-Turbulenzen», Nicolas Mayencourt & Marc K. Peter, ISBN 978-3-03875-343-8, 1re édition 2021, 176 pages, 48.– CHF