swissVR

Guide swissVR III/2020
Août 2020

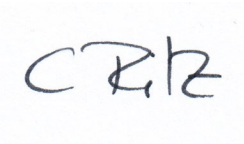
Conseils aux CA des PME: cyber-résilience

Préambule

Ces derniers mois ont montré que de plus en plus d'entreprises suisses sont dans le collimateur de cybercriminels et subissent des dommages dus à des fraudes en ligne ou à des attaques par des rançongiciels. La taille de l'entreprise ne joue ici aucun rôle déterminant.

Comment pouvez-vous renforcer la capacité de résistance aux cyber-risques dans votre entreprise et quel rôle l'administrateur/l'administratrice devrait endosser en la matière?

Le présent swissVR Impuls doit vous aider à trouver la réponse à ces questions. Nous vous souhaitons une bonne mise en œuvre des mesures décrites et espérons que vous serez épargné par les attaques.



Cornelia Ritz Bossicard
Présidente de swissVR

Matthias Bossardt
Responsable Cyber Security and Technology Risk Consulting KPMG

Ce swissVR Impuls a été élaboré par swissVR en collaboration avec KPMG.

Auteurs:

Cornelia Ritz Bossicard, administratrice indépendante, présidente de swissVR (cornelia.ritz@swissvr.ch) et

Matthias Bossardt, responsable Cyber Security et Technology Risk Consulting, KPMG (mbossardt@kpmg.com)

Page titre: pixabay.com/Gerd Altmann

swissVR est une association suisse regroupant des membres de conseils d'administration, créée par des administrateurs/administratrices pour les administrateurs/administratrices – attractive – indépendante – spécialisée. À travers son offre, elle contribue à la professionnalisation des conseils d'administration suisses. swissVR promeut l'échange d'expériences entre les membres de conseils d'administration d'entreprises opérant dans tous les secteurs, et propose à ses plus de 900 membres une offre d'informations et de formations adaptée à leurs besoins. swissVR s'adresse uniquement aux personnes assumant un mandat actif d'administrateur/administratrice.

Pour plus d'informations sur swissVR et l'adhésion à l'association: www.swissvr.ch

swissVR, Suurstoffi 1, 6343 Rotkreuz
info@swissvr.ch, +41 41 757 67 11

(Version du 12 août 2020)

Conseils aux CA des PME concernant la cyber-résilience

Ces dernières années, les cyber-risques ont pris une place à part dans les listes des points à l'ordre du jour de nombreux conseils d'administration. A juste titre: les récents cyber-incidents ont eu de lourdes conséquences sur les entreprises concernées. Ces dernières ont subi des interruptions dans leurs activités, des violations dans la protection des données ainsi que des pertes financières. Elles ont également connu des problèmes de réputation et de confiance. Dans quelques cas, les incidents ont eu un impact considérable sur la valeur des entreprises ciblées, pouvant les mener même jusqu'à la faillite. Comme le montre l'importante couverture médiatique, tant les grandes entreprises que les petites peuvent être victimes dans la même ampleur de cyber-attaques.

En plus des risques opérationnels évidents, les entreprises plus avancées considèrent que la cyber-résilience est une opportunité stratégique pour se démarquer par rapport à la concurrence. Une gestion responsable des cyber-risques et même un cyber-incident bien maîtrisé peuvent renforcer la confiance des parties prenantes d'une entreprise, qu'il s'agisse des clients, des investisseurs, des fournisseurs ou des autorités de surveillance. Par ailleurs, une entreprise cyber-résiliente peut utiliser de façon durable et avec assurance des technologies numériques telles que l'analyse des données, l'intelligence artificielle et le Cloud Computing afin d'améliorer sa position par rapport à la concurrence.

1. Les cyber-risques ne sont pas techniques. Ce sont des risques opérationnels.

Les cyber-risques sont souvent considérés par les entreprises comme une menace non palpable, presque irréelle. Cela s'explique notamment par le fait que de telles attaques exploitent souvent des failles techniques hautement complexes. En conclure que les cyber-risques sont donc des risques techniques que l'organisation informatique doit gérer est une idée fausse.

Si on prend en considération les conséquences possibles d'une cyber-attaque, il devient évident qu'il s'agit de risques opérationnels avec lesquels les conseils d'administration et les directions doivent se familiariser:

Fuites de données
- Violations de la protection des données
- Divulgation de la propriété intellectuelle et des informations confidentielles de l'entreprise

Sorties d'actifs
- Paiements non autorisés ou frauduleux
- Versements de rançons

Interruption de l'activité
- Arrêt de la production
- Défaillance de la logistique

Dysfonctionnement au niveau des produits et services défectueux

Organisation propre en tant que porte ouverte pour les cyber-attaques contre les clients

Ces conséquences directes des cyber-attaques peuvent aboutir à des dommages tels que:

- Perte au niveau de la réputation et de la confiance des clients
- Baisse du chiffre d'affaires
- Frais administratifs liés au remplacement et à la restauration des systèmes
- Frais de justice et amendes
- Responsabilité, dommages-intérêts, indemnisations en cas de retards
- Perte de temps, lancement tardif sur le marché

2. Le rôle du conseil d'administration

Les quatre principales tâches du conseil d'administration se rapportent à la stratégie, aux systèmes, aux collaborateurs et collaboratrices ainsi qu'à la surveillance[1]. Il en découle directement des missions en lien avec la cyber-résilience de l'entreprise.

Stratégie: intégration d'une cyber-stratégie en tant que partie intégrante de la stratégie d'entreprise
- Moteur de l'activité
- Modèle opérationnel
- Produits/Prestations de services

Systèmes: structuration de la gestion de crise et des risques
- Identification et traitement des cyber-risques dans le contexte de l'entreprise
- Gestion de crise qui s'applique également en cas de cyber-crises

Collaborateurs et collaboratrices: désignation de la direction
- Lors de la désignation des personnes chargées de

[1] Best Practice dans les PME, www.ccg.ifpm.unisg.ch

la direction, le conseil d'administration s'assure que ces dernières disposent d'une compréhension suffisante des risques opérationnels afin de pouvoir maîtriser les cyber-risques de façon appropriée.

Surveillance: haute surveillance par le biais de la direction et respect des lois et des directives
- Respect des réglementations sur la protection des données, la sécurité de l'information, la sécurité des produits, les directives internes, etc.
- Cyber-reporting

Pour pouvoir s'acquitter de ces tâches en lien avec la cyber-résilience, il faut établir une gouvernance au sein de l'entreprise qui mette en œuvre des cyber-mesures conformément aux risques.

3. Mise en œuvre rigoureuse des cyber-mesures de protection de base

Alors que, par le passé, on se focalisait, comme au Moyen Age avec les fortifications des villes, sur les mesures techniques visant à empêcher les agresseurs de pénétrer dans l'entreprise (mot-clé: pare-feu), une cyber-stratégie moderne possède une base plus large. En effet, il faut partir du principe qu'avec la mise en réseau et l'intégration croissantes entre les entreprises, les fournisseurs et les clients, un agresseur peut pénétrer et pénétrera dans des domaines protégés.

Une stratégie moderne se doit donc d'identifier rapidement les intrus, de les empêcher de causer des dommages et ainsi d'augmenter la résistance de l'entreprise concernée face aux cyber-attaques.

C'est pour cela que dans le contexte de la gestion des cyber-risques, on utilise de plus en plus le terme de cyber-résilience.

En conséquence, le NIST Cyber-Framework[2] répandu dans le monde entier divise les cyber-mesures en cinq «fonctions»: Identify, Protect, Detect, React et Recover.

Dans l'entreprise, il s'agit de trouver avec des cyber-mesures un bon équilibre entre ces cinq fonctions. Il faut également veiller à ce que la cyber-résilience ne soit pas obtenue uniquement grâce à des mesures techniques mais seulement en ajoutant des mesures organisationnelles / orientées sur les processus (p. ex. principe du double contrôle) et des mesures concernant les personnes (p. ex. sensibilisation et formation).

Le conseil d'administration devrait vérifier que les mesures de protection de base suivantes soient mises en œuvre de façon rigoureuse:

Identifier («Identify»)
- Attribution des tâches, des compétences et des responsabilités
- Connaissance des données critiques de l'entreprise ET des processus commerciaux
- Inventaire des systèmes informatiques et des logiciels (aussi Internet des objets)

Protéger («Protect»)
- Sensibilisation et entraînement des collaborateurs et collaboratrices
- Gestion des identités et des accès, y compris les enregistrements
- «Patching» régulier de tous les systèmes informatiques
- Application de mesures de sécurité dans le cadre de la collaboration avec des tiers

Découvrir («Detect»)
- Identification des malwares
- Segmentation et surveillance du réseau
- Tests techniques de sécurité périodiques/continuels, également dans le cadre du développement de logiciels et de produits

Réagir («React»)
- Développement et test/mise en œuvre des cyber-plans d'urgence

Restaurer («Recover»)
- Back-up (sauvegarde)

4. Questions pour le conseil d'administration

La compréhension de la cyber-menace par le conseil d'administration et sa participation à l'élaboration de la réaction adéquate sont cruciales tant au niveau du rôle de stratège du conseil d'administration au sein de l'entreprise qu'au niveau de sa fonction de surveillance. Le conseil d'administration devrait obtenir des éclaircissements sur les thèmes suivants.

1. Quels sont les nouvelles **cyber-menaces et les nouveaux cyber-risques**? Dans quelle mesure ceux-ci ont-ils un impact sur notre organisation?
2. Notre **programme de cyber-résilience** répond-il aux défis posés par les cyber-menaces d'aujourd'hui et de demain?
3. Comprenons-nous nos **points faibles actuels** (également en ce qui concerne nos fournisseurs et prestataires) et de quels **processus** disposons-nous pour aborder les cyber-risques identifiés?
4. Notre organisation est-elle suffisamment préparée pour pouvoir **réagir correctement à une attaque**?
5. Quels **indicateurs de risques clés** (Key Risk Indicators) et **de performance** (Key Performance Indicators) devons-nous analyser au niveau du conseil de fondation pour pouvoir remplir notre fonction de surveillance?
6. Notre organisation remplit-elle ses **obligations légales et réglementaires** en matière de sécurisation des données (p.ex. protection des données)?
7. La cyber-résilience est-elle **abordée dans les discussions stratégiques du conseil d'administration** et quand nous sommes-nous penchés pour la dernière fois sur la cyber-menace?
8. Comment faire évoluer notre organisation en passant d'une approche **réactive à une approche anticipative** de la cyber-menace?
9. La **concurrence** nous devance-t-elle? Si tel est

[2] https://www.nist.gov/cyberframework

le cas, est-ce là un **avantage concurrentiel** pour elle?

5. Cyber-reporting pour le conseil d'administration

De nombreux conseils d'administration ont des difficultés à obtenir de leurs équipes de direction des rapports appropriés sur les cyber-risques et le stade de cyber-résilience de l'entreprise. Souvent, il s'agit de rapports qui fournissent des aperçus techniques détaillés et truffés de jargon sur l'état des contrôles sans qu'un lien clair puisse être établi avec des cyber-risques opérationnels et les impacts possibles sur les activités. Par conséquent, le conseil d'administration ne peut remplir que difficilement ses obligations en lien avec les cyber-risques.

Un bon rapport permet au conseil d'administration

1) de comprendre la manière dont les cyber-risques affectent les capacités de l'entreprise, de mettre en œuvre sa stratégie commerciale et
2) de positionner les cyber-risques par rapport aux autres risques opérationnels et stratégiques ainsi que de prioriser les ressources en conséquence.

En tant que point de départ, les cyber-rapports réguliers adressés au conseil d'administration devraient aborder les thèmes suivants.

Situation de menace stratégique
- Vecteurs d'attaques, agresseurs
- Tendances (des différentes branches)

Cyber-incidents au sein de l'entreprise
- Constatations et besoin d'agir

Aperçu des principaux cyber-risques
- Potentiel de dommages (en particulier en ce qui concerne les processus et données critiques pour les entreprises)
- Tendances

Mesures de cyber-résilience
- Couverture et efficacité en ce qui concerne les principaux cyber-risques
- Couverture et efficacité des mesures de protection de base à appliquer à toute l'entreprise
- Respect des exigences réglementaires, standards de l'industrie, directives internes

Cyber-stratégie/cyber-programme
- Stade de la mise en pratique
- Impact sur les principaux risques

Besoin d'action/d'investissement

6. Résumé

Les cyber-risques sont des risques opérationnels qui mettent en danger la pérennité d'une entreprise et que le conseil d'administration doit traiter dans le cadre de ses tâches légales. Le conseil d'administration devrait s'assurer que l'entreprise oriente sa cyber-stratégie sur la résilience. Pour cela, les cyber-mesures de base doivent être mises en œuvre de manière rigoureuse.

Afin de clarifier l'état des cyber-risques et de la cyber-résilience de l'entreprise, un cyber-reporting adéquat est nécessaire.

Outre la gestion des cyber-risques, le conseil d'administration devrait, en concertation avec la direction, également analyser dans quelle mesure la cyber-résilience peut être utilisée en tant qu'élément distinctif et avantage concurrentiel.

Liens complémentaires

- National Cyber Security Center
  https://www.ncsc.admin.ch/melani/fr/home.html
- Outils pour les PME
  https://gcatoolkit.org/fr/petites-entreprises/
- NIST Cyber Framework
  https://www.nist.gov/cyberframework
- Password Breaches
  https://haveibeenpwned.com/
- KPMG
  https://home.kpmg/xx/en/home/services/advisory/risk-consulting/cyber-security-services.html

  https://www.kpmg.ch/cyber