swiss BoardForum
sharing experience

Gestion des cyberrisques: la sensibilisation ne suffit pas

La numérisation facilite notre quotidien, tant privé que professionnel. Mais la cybercriminalité augmente. Les entreprises qui ne gèrent pas les cyberrisques de manière systématique compromettent leur exploitation et leur réputation. Sept recommandations pour bien gérer les cyberrisques.

En raison de la numérisation, les modèles d'affaires sont de plus en plus interconnectés. Chaînes de création de valeur fragmentées, services dans le cloud de plus en plus nombreux: des données sont reçues, lues, traitées et transmises. Ces processus d'information et de communication accroissent la dépendance vis-à-vis des fournisseurs. Les cyberrisques deviennent un risque entrepreneurial, mais aussi systémique, auquel la priorité absolue est accordée. En effet, si l'informatique ne fonctionne pas, l'exploitation se retrouve à l'arrêt.

Les cyberattaques visent toutes les entreprises

Il ne s'agit pas de savoir si, mais quand une entreprise sera ciblée. Les cyberattaques se multiplient et la cybercriminalité est de plus en plus lucrative. Les cas qui sont rendus publics ne constituent que la partie émergée de l'iceberg, car les chiffres réels sont élevés. Beaucoup d'entreprises ne souhaitent pas divulguer les faiblesses de leur infrastructure IT ou de leurs processus d'information et de communication et ne révèlent donc pas ces attaques au public. Les attaques qui réussissent, appelées cyberincidents dans le langage des assurances, ciblent les systèmes informatiques. Les conséquences négatives en sont toutefois ressenties au niveau de tous les processus opérationnels, jusqu'au cœur de métier de l'entreprise concernée. Elles menacent la continuité de son activité ainsi que sa réputation et peuvent donner lieu à des prétentions en responsabilité civile en matière de protection des données.

Les stratégies des hackers

Pour s'introduire dans les systèmes informatiques, les pirates utilisent des e-mails d'hameçonnage qui trompent le personnel de l'entreprise visée (ingénierie sociale), par le biais de ports ouverts ou de calculateurs commandés à distance (Botnet). Des maliciels infectent alors les systèmes en exploitant ces failles de sécurité. Les données font souvent l'objet d'un chiffrement et une double rançon est réclamée. Dans un premier temps, les données ne sont restituées, le cas échéant, que lorsqu'une somme élevée en bitcoins a été payée. Un second paiement permet à l'entreprise d'éviter que les données confidentielles qui lui ont été volées soient publiées sur le Darknet ou sur Internet. Le recours à des techniques de fraude telles que la manipulation de factures (attaque de type « homme du milieu », arnaque au CEO) est aussi en hausse.

Des incidents angoissants et coûteux

Une cyberattaque coûte beaucoup de temps et met les nerfs à rude épreuve. Il faut réinitialiser les systèmes informatiques, récupérer et rétablir les données, restaurer les sauvegardes et activer une organisation d'urgence et de crise.

SwissBoardForum
Kapellenstrasse 14 | Postfach | 3001 Bern | T: +41 (0)58 796 98 80 | F: +41 (0)58 796 99 03 | sekretariat@swissboardforum.ch
Route de Lac 2 | 1094 Paudex | Case Postale 1215 | 1001 Lausanne | T: +41 (0)58 796 33 00 | F: +41 (0)58 796 33 82 | secretariat@swissboardforum.ch

www.swissboardforum.ch

En outre, les pertes financières dues à l'interruption de l'exploitation, les coûts de remise en service de l'infrastructure et les dommages économiques en cas de fraude bancaire en ligne sont généralement élevés. Sans oublier les atteintes à la réputation résultant d'une gestion de crise souvent défaillante.

La proactivité est de mise

Pour se prémunir contre ce danger invisible et dynamique, une entreprise doit commencer par bien comprendre ce nouveau phénomène que constituent les cyberrisques. À cette fin, les parties prenantes participent à un échange interne et une réponse commune est apportée à la question de savoir jusqu'à quel point l'entreprise est dépendante du bon fonctionnement du système informatique et de la sécurité des données. Il s'agit également de déterminer la manière dont les cyberrisques doivent être gérés et, comme pour tous les risques, il existe quatre options. Premièrement, le risque peut être accepté. Deuxièmement, l'entreprise peut éviter le risque en prenant des mesures telles que la mise en place d'un logiciel antimaliciel. Troisièmement, elle peut atténuer le risque en se prémunissant contre la réussite d'une attaque, par exemple grâce au Business Continuity Management. Quatrièmement, elle peut transférer le risque à sa société d'assurance. Une cyberassurance fournit un soutien en cas de cyberincident et prend en charge les frais correspondants.

Sept recommandations pour gérer les cyberrisques

Qu'est-ce que cela signifie pour le travail du conseil d'administration ? Quels processus doivent être mis en œuvre pour protéger efficacement une entreprise contre la cybercriminalité ? Les sept recommandations concrètes et non exhaustives qui suivent contribuent à donner au thème de la cybersécurité toute l'importance qu'il mérite :

1. **Ancrer le thème de la cybersécurité dans la politique de risque :** les organes de contrôle et de surveillance doivent intégrer les cyberrisques dans la gouvernance d'entreprise et la politique de risque en définissant des objectifs et des principes. Si ceux-ci sont également communiqués de manière claire et compréhensible au niveau opérationnel, ils permettent de sensibiliser le personnel et de renforcer son sens des responsabilités en matière de cyberrisques. Une véritable culture des cyberrisques est ainsi vécue par les personnes qui prennent des décisions et une chose est claire : les cyberrisques sont l'affaire du management. Ils relèvent de la gestion stratégique des risques au niveau de l'entreprise et ne peuvent pas simplement être délégués par la direction au secteur informatique.

2. **Attribuer clairement les responsabilités :** en cas de cyberattaque, souvent susceptible de mettre en danger l'entreprise, des personnes de contact compétentes doivent être disponibles : le management, la ou le CFO, la ou le gestionnaire des risques et la ou le responsable de la protection des données assument la responsabilité organisationnelle. La ou le prestataire de sécurité informatique, ou Chief Information Security Officer (CISO), connaît les forces et les faiblesses de la sécurité de l'information de l'IT, du réseau et de la télécommunication et endosse la responsabilité technique. La société d'assurance peut apporter un soutien spécifique en précisant la menace et en émettant des recommandations en matière de prévention et de cyberrésilience après avoir évalué les risques.

3. De plus, elle peut accompagner l'entreprise en lui fournissant une couverture d'assurance adéquate et des prestations d'assistance en cas de sinistre (réponse aux incidents, continuité de l'exploitation, gestion de crise et de la réputation), éventuellement avec l'aide d'une courtière ou d'un courtier. Toutes ces responsabilités doivent être clairement définies.

4. **Renforcer la cybersécurité grâce au dialogue sur les risques :** ensuite, ces différents responsables doivent mener une discussion interdisciplinaire sur les cyberrisques en partageant leurs connaissances spécifiques. Ce dialogue constitue un facteur de succès critique dans la mesure où il permet d'analyser, de piloter et de contrôler les cyberrisques dans leur ensemble. À l'interne, les secteurs IT et Business ainsi que la ou le CISO et la ou le gestionnaire des risques doivent se concerter. S'y ajoutent des partenaires externes compétents tels que des prestataires de sécurité informatique, des assureurs et des courtières ou courtiers.

5. **Favoriser l'intégration des cyberrisques dans la gestion des risques à l'échelle de l'entreprise :** la collaboration étroite entre la ou le CISO (cybersécurité technique au niveau des systèmes) et la gestion des risques opérationnels dans l'entreprise permet d'instaurer une gouvernance et une culture réelles des risques. Un processus structuré contribue à identifier les actifs numériques, à évaluer, piloter et contrôler les cyberrisques et ainsi à introduire des mesures d'amélioration. Une telle gestion proactive et globale des risques tenant compte des cyberrisques nécessite une structure de gouvernance clairement définie.

6. **Sans responsabilité individuelle au sein de l'entreprise, pas de cyberprotection :** la mise en œuvre ciblée et continue de mesures techniques, organisationnelles, physiques et en matière de personnel afin d'atténuer les risques favorise la prévention de la cybercriminalité et renforce la cyberrésilience de l'entreprise. L'entreprise est ainsi préparée en cas de cyberattaque. De plus, elle est plus efficace et compétitive en tant qu'organisation. La sensibilisation régulière du personnel fait notamment partie de ces mesures. Il s'agit d'un investissement payant dans la cybersécurité. En effet, l'efficacité de la gestion des cyberrisques est souvent déterminée par le facteur humain et les mesures organisationnelles. En définitive, les diverses mesures prises par l'entreprise dépendent de la compréhension et de l'acceptation des cyberrisques. Étant donné qu'il subsiste toujours un risque résiduel, la mise en place d'une solution de cyberassurance adéquate fait aussi partie de la gestion active des cyberrisques, qu'elle complète. En mettant suffisamment l'accent sur la responsabilité individuelle, les entreprises peuvent ainsi maîtriser leurs cyberrisques dans leur globalité.

7. **Le cloud, élément à part entière de la gestion des cyberrisques :** si des services cloud font partie de l'infrastructure IT ou doivent y être intégrés, une stratégie cloud avec une gestion correspondante des risques doit aussi être élaborée. S'agissant du fonctionnement des applications critiques, des solutions sur site sont privilégiées. En ce qui concerne la cybersécurité, le stockage des données en Suisse, l'établissement d'une classification des données, l'utilisation d'une technologie de chiffrement et la gestion consciente de la dépendance au prestataire cloud jouent un rôle important.

8. **Se préparer aux situations d'urgence grâce à la planification et aux exercices :** dans le cadre d'une gestion efficace de la continuité de l'exploitation, un concept d'urgence tenant compte des services cloud externalisés assure la poursuite de l'activité en cas d'attaque. Son efficacité doit être vérifiée lors d'exercices d'urgence réguliers basés sur des scénarios. À cet égard, la société d'assurance peut servir de « sparring partner » pour l'élaboration de scénarios de sinistre et d'urgence réalistes et faire office d'intermédiaire auprès de prestataires spécialisés.

Source :
Étude sur le cybermarché 2022 ; la Mobilière, Haute école de Lucerne, economiesuisse: «Gestion des cyberrisques dans les grandes entreprises suisses» (disponible en allemand uniquement)

Auteur :
Christoph Clavadetscher travaille depuis plus de trois ans au sein du centre de compétences Cyberrisques à la Mobilière. Fort de 22 ans d'expérience dans le secteur de l'assurance (développement de produits et souscription), il suit actuellement une formation continue dans le domaine de l'information et de la cybersécurité à la Haute école de Lucerne.