La confiance numérique comme facteur de réussite

Les TIC s'imposant toujours davantage, les entreprises du monde numérique sont de plus en plus dépendantes de la disponibilité de leurs systèmes d'information. Parallèlement, la simplicité de l'accès via l'Internet augmente la vulnérabilité de ces systèmes. En observant les entreprises, nous avons toutefois l'impression que nombre d'entre elles sous-estiment les risques en matière de sécurité de l'information et ne les maîtrisent souvent pas suffisamment.

L'intérêt du public pour la protection et la sécurité des données augmente continuellement. À quoi les entreprises qui s'adaptent à des technologies disruptives doivent-elles réfléchir ?

Dr Adrian Marti

L'industrialisation et la digitalisation ont aussi occupé les pages de la rubrique criminelle. Depuis toujours, les criminels sont souvent des pionniers des nouvelles technologies, afin d'avoir une longueur d'avance dans la course aux armements entre l'attaquant et le défenseur. Ces dernières années, les escroqueries basées sur Internet et la criminalité économique ont considérablement augmenté. Il est particulièrement intéressant de constater que le degré d'implication du crime organisé a fortement augmenté dans ce secteur.

Les cyberattaques se développent en un modèle d'affaires profitable. Des bandes criminelles suréquipées, disposant de modèles d'organisation et d'outils modernes, remplacent les cyber-délinquants agissant seuls. La professionnalisation de la cybercriminalité créé de nouveaux services, comme l'*Access as a Service*, des cibles attrayantes, puisque l'accès aux cibles déjà piratées est mis aux enchères et vendu au plus offrant.

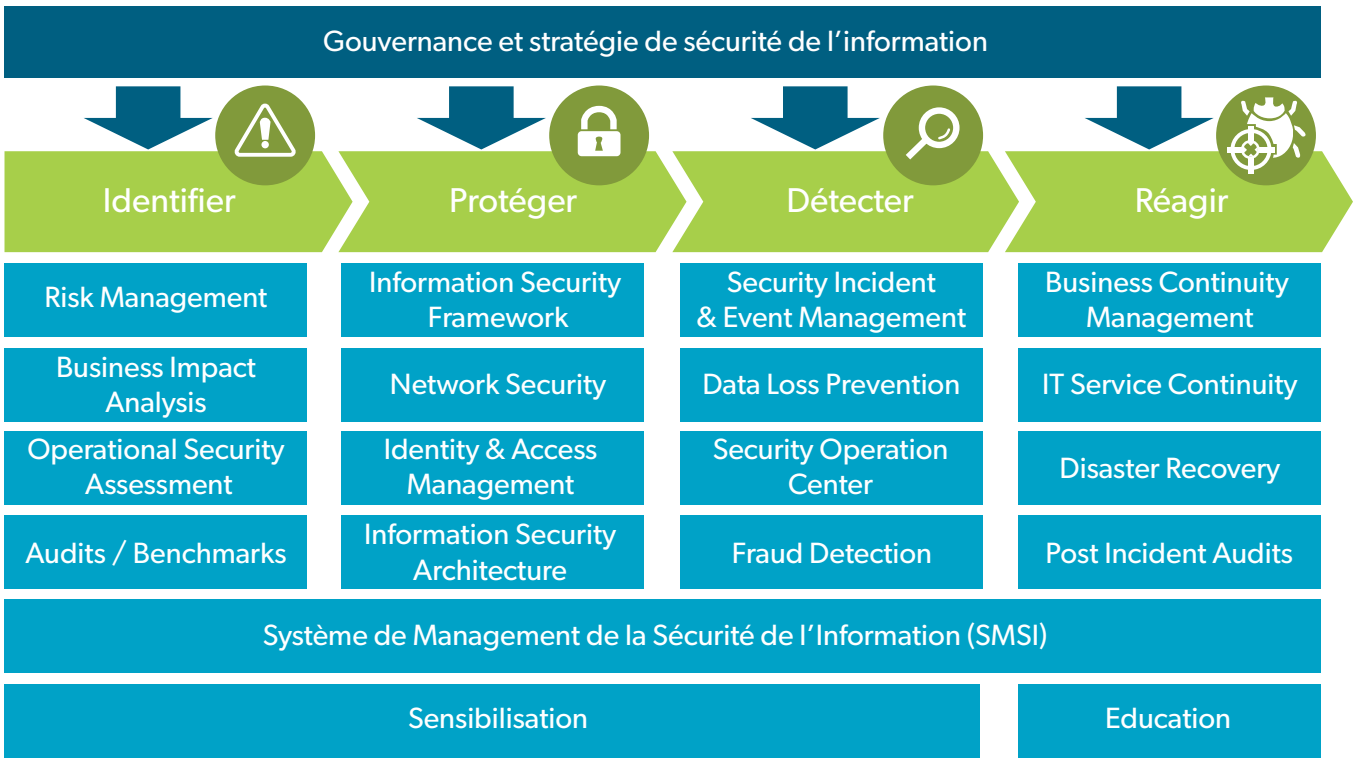
La diffusion croissante des technologies de l'information et la progression de la mise en réseau augmentent la menace. Alors qu'il a suffi durant longtemps de se protéger contre les programmes malveillants, en particulier les virus, les défis en matière de sécurité se sont aujourd'hui multipliés.

Avec la digitalisation, des TIC stables et sécurisées deviennent une ressource commerciale critique. Les incidents de sécurité liés aux TIC ne sont donc plus pour la majorité des entreprises de simples inconvénients, mais des événements qui peuvent mettre en danger leur activité. Si l'on considère l'importance croissante du traitement de données personnelles dans l'économie numérique, la sécurité et la protection des données deviennent essentielles. Des problèmes dans ce domaine peuvent être la cause d'une importante perte de confiance des clients et des partenaires commerciaux, ce qui peut entraîner des conséquences économiques critiques pour l'entreprise.

Une sécurité de l'information moderne doit, d'une part, prévenir activement les risques potentiels pour la sécurité de l'information et réduire le plus possible la vraisemblance de leur concrétisation. D'autre part, en cas de dommage, elle doit permettre la poursuite de l'activité de l'entreprise. Les principes suivants peuvent être appliqués :

- **Prise de décision basée sur les risques**
  Les responsables de la sécurité doivent opter pour une prise de décision basée sur les risques. La mise en œuvre de cette vieille idée bien connue est aujourd'hui plus urgente que jamais. La réflexion basée sur les risques suppose une compréhension de ceux-ci par l'entreprise et constitue la base de l'établissement des priorités en matière de contrôles et d'investissements dans la prévention des risques et la sécurité des TIC. Vu la complexité croissante de la technologie, les ressources disponibles doivent être focalisées sur la gestion des risques majeurs. La réflexion basée sur les risques permet de concentrer les investissements de cybersécurité sur ces derniers. Le moteur de l'analyse des risques doit être la ligne hiérarchique et non pas l'informatique.

- **Protection des joyaux de la couronne numérique**
  Les responsables informatiques et de la sécurité doivent recentrer leur attention de la protection de l'infrastructure à la protection des informations critiques pour l'entreprise. Par le passé, les décisions d'investissements étaient concentrées sur la protection de l'in-



Ill. 1 : Compétences pour garantir la confiance numérique

frastructure TIC. Des ordinateurs centraux aux terminaux, en passant par les serveurs : une technologie était gage de sécurité pour l'entreprise. Nous considérons que cette approche est dépassée. Aujourd'hui plus que jamais, nous avons besoin d'une approche « security by design » : dès les phases de conception et de développement, les *hardware* et les logiciels doivent être conçus de manière à être autant que possible insensibles aux attaques. D'après notre expérience, ceci est certes délicat à intégrer aux méthodes de développement agile, mais peut néanmoins être mis en œuvre avec succès.

Pour la protection des revenus d'entreprise critiques – c'est-à-dire les processus centraux et la rentabilité pour une entreprise ou l'exécution des tâches d'intérêt général pour les pouvoirs publics, la ligne hiérarchique doit disposer d'une stratégie en termes de risques et de sécurité.

Les dirigeants qui ne sont pas impliqués dans les TIC se plaisent à affirmer que les risques et la sécurité des TIC sont des problématiques techniques et délèguent alors leur gestion au département de l'informatique. Or, la sécurité de l'information ne peut être atteinte qu'en étroite collaboration avec le métier.

- **Détection et réaction plutôt que protection à 100 %**
  Protéger ses propres actifs numériques devient plus difficile : les attaques deviennent de plus en plus sophistiquées, alors que le nombre d'interfaces et de terminaux de l'infrastructure TIC de l'entreprise augmente. L'objectif consiste donc à détecter le plus rapidement possible les attaques et à réagir. Il faut des capacités de détection des attaques, mais aussi des moyens pour empêcher leur propagation et la fuite de données.

- **La gestion de la continuité des affaires et de l'informatique est plus importante que jamais**
  En plus des analyses de sécurité classiques (focalisées sur la protection et la sécurité des données) et des analyses d'incidents et de dépendances (focalisées sur la poursuite de l'activité), il s'agira à l'avenir de protéger les individus, les organisations et la société contre des systèmes autonomes victimes de défaillances de toutes natures. À cet effet, dans le contexte de leur analyse de risques, les entreprises doivent recenser tous les processus critiques et mettre en place la gestion de crise correspondante.

- **L'homme est au centre de la sécurité, pas la technique**
  Des études montrent que la plupart des risques pour la sécurité de l'information proviennent de l'intérieur, soit des collaborateurs eux-mêmes. C'est uniquement si la sécurité de l'information est reconnue comme tâche stratégique de l'entreprise que les collaborateurs peuvent développer une sensibilité suffisante à ce sujet.