economiesuisse

Cyberrisques pour les PME: améliorer l'efficacité

L'utilisation d'outils numériques est cruciale dans le développement du modèle d'affaires de nombreuses entreprises. Cela ne doit pourtant pas faire oublier la cybersécurité. Toute négligence dans ce domaine peut être lourde de conséquences, pour l'entreprise, comme pour ses partenaires commerciaux.

Quiconque associe « numérisation de l'économie » uniquement avec les grandes entreprises technologiques ou les start-ups dynamiques de la Crypto Valley oublie qu'aujourd'hui, pratiquement chaque entreprise utilise les progrès numériques à ses propres fins. Les nombreux allègements offerts grâce aux nouvelles technologies sont devenus indispensables, surtout dans le quotidien de nos PME – de la menuiserie à la fiduciaire en passant par l'atelier de vélos. Cela ne concerne pas que l'ordinateur pour la comptabilité ou le traitement de textes. Les plans de construction sont établis et envoyés par voie électronique, les commerciaux enregistrent les commandes directement sur leur tablette, les matières premières s'achètent sur une plateforme et l'appareil d'analyse au laboratoire télécharge directement les mises à jour depuis Internet. D'autres entrepreneurs misent encore plus sur les outils numériques. Les mots-clés sont ici travail nomade et fabrication additive.

À en croire certains sondages récents, de nombreuses entreprises suisses ont l'impression que la numérisation ne les concerne pas. Lorsqu'on aborde le sujet, elles répondent que la transformation technologique ne les touche pas

directement. Comment expliquer cette apparente contradiction ? Dans de nombreux cas, l'utilisation de la technique moderne est entrée par la petite porte dans le quotidien de nos PME, sans faire partie d'une stratégie ciblée de numérisation. Les transformations ne résultent donc pas toutes de décisions actives et ont souvent été le résultat d'autres mesures comme le passage à un nouveau téléphone ou une gestion numérique des documents, ou l'utilisation régulière d'Internet. Les outils électroniques connectés font tellement partie du quotidien qu'ils ne sont plus perçus, notamment dans les PME, comme tels. Et c'est précisément là que réside le plus grand danger au niveau de la cybersécurité.

Nouvelles possibilités technologiques, nouvelles formes de criminalité

Avec la numérisation et l'interconnexion des systèmes qui en découle (de nombreux outils, caméras de surveillance et appareils ménagers sont d'ores et déjà reliés à Internet), notre vulnérabilité atteint un tout nouveau degré. L'espace numérique abrite en effet des éléments et organisations aux activités criminelles. Les attaques visant nos entreprises peuvent être lancées de n'importe où dans le monde, anonymement et avec peu de moyens. Les cybercriminels se moquent des frontières nationales. Ils frappent là où le butin est facile, c'est-à-dire le gain élevé pour un investissement relativement faible. En toute logique, les criminels spécialisés s'en prennent donc aussi aux PME suisses. Leur attention se concentre alors surtout sur celles qui ne se soucient pas des questions de sécurité et ne prennent pas de mesures de protection appropriées.

La numérisation a donc un revers : de nouvelles formes de criminalité. Via Internet, il est possible de voler ou modifier des données, d'endommager des systèmes et de prendre des entreprises en otage. Autant de dangers qui n'existaient pas encore dans le monde analogique. Bien des attaques criminelles peuvent cependant être contrées. Pour cela, une entreprise doit – comme dans le monde physique – réfléchir à la manière de se protéger contre les visées criminelles de tiers. Si la sécurité est négligée, les allégements techniques peuvent vite virer au danger existentiel pour une PME. De nombreux utilisateurs, entreprises autant que particuliers, n'ont pas conscience des dangers liés à l'emploi des nouvelles technologies. Une étude menée par la Haute école de Lucerne en coopération avec l'Association des PME, le Secrétariat d'État à l'économie (SECO), l'Association suisse des cadres (ASC) et economiesuisse le confirme : les entreprises suisses ne sont pas assez bien préparées aux menaces du cyberespace. 40 % des sociétés sondées ont indiqué avoir fait récemment l'objet d'attaques sous forme de programmes malveillants (malware) ou de courriels hameçons (phishing-mail). Malgré la réalité du danger, les PME n'apportent pas de réponses adéquates aux attaques. Elles manquent, entre autres, de savoir-faire quant à la manière de traiter le thème de la sécurité des informations.

Prise de conscience grandissante des dangers, mais…

L'étude conclut que la sensibilité à l'égard de la cybersécurité s'est fondamentalement améliorée. « Numérisation, robotique et automatisation » sont devenues, pour les équipes dirigeantes, la deuxième priorité juste après l'accroissement de l'efficacité. Quelque 78 % des PME sondées affirment d'ailleurs que la cybersécurité a gagné en importance ces trois dernières années. Mais même si le sujet est discuté plus largement dans les PME, il y a urgence en la matière. L'étude note en effet que moins de la moitié des entreprises consultées réévaluent régulièrement leurs mesures de sécurité. Les guides sur la manière de gérer les cyber-risques restent l'exception. Idem pour les formations continues. Dès lors, il faut des stratégies pour établir les meilleures réponses aux dangers de l'Internet. Il suffit souvent de peu pour améliorer sensiblement la sécurité dans une entreprise. Focaliser l'attention sur la cybersécurité dans les entreprises concernées, mais aussi auprès des partenaires commerciaux, fournisseurs et clients permettrait de réduire sérieusement les cas d'abus.

Un risque de sécurité peut être un obstacle aux échanges et mettre en péril une entreprise toute entière ainsi que ses partenaires commerciaux. Il est donc essentiel que le business case inclue la sécurité et les coûts y relatifs dès le départ. L'objectif doit être que chaque entreprise, quelle que soit sa taille, puisse développer un concept de sécurité adéquat qui lui offre une protection suffisante tout en maintenant son bon fonctionnement opérationnel.

Responsabilité de chacun engagée

Tout comme nous sommes nous-mêmes responsables de protéger notre demeure contre les cambriolages, chaque entreprise est la première responsable de sa protection contre les menaces du cyberespace. La réponse ne se trouve pas dans des obligations de comportement dictées par l'État, bien au contraire.

En matière de cybersécurité, les systèmes décentralisés et hétérogènes sont plus résistants que les systèmes centralisés. Notamment lorsqu'il s'agit de gérer des crises et défis inattendus. Dans les cas où des solutions sectorielles s'imposent, l'économie doit prendre les devants. Les différentes branches peuvent, en émettant des normes minimales, au sens de recommandations, renforcer notablement la cybersécurité. Des guides clairs et compréhensibles peuvent alors servir d'aide. Avec de telles normes minimales, les PME pourraient bénéficier du savoir-faire des grandes entreprises et les asymétries sectorielles face au cyberespace pourraient être compensées. L'État apporte sa contribution en favorisant de pareilles normes de sécurité et en veillant à une application équilibrée au regard de la législation internationale. En cas de crise, c.-à-d. d'attaque à vaste échelle, il est indispensable que les tâches de l'économie privée et de l'État soient clairement réglées et réparties.

Avec des incitations adéquates, l'État doit donc veiller à ce que les incidents en lien avec le cyberespace soient signalés. Cela augmente la transparence, abaisse le niveau de menace et aide à réduire l'impact de telles attaques sur des tiers. La population, les entreprises, l'administration et les milieux politiques doivent être dûment sensibilisés afin d'améliorer la prise de conscience face aux cyberrisques. La sécurité dans le cyberespace est une tâche commune classique. Tout est connecté et les systèmes s'influencent mutuellement. En clair, chacun doit contribuer à augmenter la sécurité. En appeler à une intervention de l'État, tout

comme le fait d'ignorer sa propre vulnérabilité technologique, ne sert à rien.

Article paru en allemand dans le magazine IT business.