Vers plus de sécurité dans le cyberespace

Des criminels opèrent de manière toujours plus professionnelle dans le cyberespace et menacent la durabilité de la mutation numérique. En tant que place scientifique, la Suisse doit se préoccuper de la question. D'autres pays, de même que l'UE, ont d'ores et déjà introduit une obligation d'annoncer et imposé des normes de sécurité. *Arié Malz*

Abrégé Les rapports et les études sur la sécurité des infrastructures numériques concordent pour admettre que le cyberespace perd de sa sécurité. Tandis que la numérisation croissante expose tous les domaines à des attaques, les cybercriminels et les espions agissent de manière toujours plus professionnelle. Il devient de plus en plus difficile d'estimer la menace et de déterminer ce qu'est un niveau de sécurité adéquat. Il y a lieu de penser qu'une majorité d'entreprises n'investissent pas encore assez dans la cybersécurité. C'est ce que montre notamment une étude de l'Information Security Society Switzerland (ISSS). Faut-il des normes pour les infrastructures critiques ou pour les infrastructures numériques, voire pour toutes les infrastructures ? D'autres pays, de même que l'UE, vont plus loin que la Suisse à cet égard. Le débat est lancé et doit être poursuivi d'urgence.

Les rapports et les études sur la sécurité des infrastructures numériques, désormais innombrables, s'accordent sur un point : le cyberespace est de moins en moins sûr[1]. Les divergences portent sur la vitesse du phénomène et sur la pondération des divers modèles de cyberattaque ainsi que sur les modèles d'affaires criminels. Voilà qui est clair : une quantification complète des incidents et de la situation, toute urgente et nécessaire qu'elle soit, n'est manifestement pas réalisable à l'heure actuelle. On prend conscience du fait que nous en savons actuellement trop peu sur ce que nous ne connaissons pas. Le plus grand risque envisageable se situe à ce niveau.

En revanche, nous savons que le nombre de nouveaux maliciels et de réseaux zombies identifiés croît d'heure en heure, tout comme celui des failles inconnues qui circulent dans le réseau. Il n'en est pas moins inquiétant de constater que les attaquants arrivent régulièrement à leurs fins en exploitant des failles déjà connues. D'un point de vue purement statistique, il faut supposer qu'une large majorité d'entreprises et d'organisations ont déjà été victimes, au moins une fois, d'une attaque numérique.

Qu'en est-il de la compréhension des risques et des mesures prises dans les entreprises ? Comment peut-on améliorer la protection de la société, de l'économie et des exploitants d'infrastructures critiques, par exemple dans les domaines de l'énergie et des transports ? Quel est, dans ce cadre, le rôle dévolu à l'État ? Les normes de sécurité, les exigences minimales et les obligations d'annoncer sont déterminantes dans les réponses apportées à ces questions.

Progression des cyberincidents

Dans la mesure où les chiffres sont fiables, ils parlent un langage clair : la criminalité et l'espionnage motivent plus des trois quarts des cyberincidents, la limite entre les acteurs criminels et apparentés aux États s'estompant ainsi. Le reste se répartit entre le cyberactivisme politique et la cyberguerre. Le nombre d'attaques d'origine criminelle est ainsi monté en flèche par rapport à 2015. Celle dirigée contre le trafic de paiements interbancaires géré par la société Swift montre à quel point les cyberattaques criminelles peuvent être professionnelles et lucratives. Le dommage pour la Banque centrale du Bangladesh a sans doute atteint, selon les sources, plus de 80 millions d'USD.

Les attaquants opèrent désormais en se divisant les tâches à un très haut niveau. Même les novices en technique trouvent dans le Web clandestin (« Darknet »), grâce à « Cyber-Attack as a Service », des services sophistiqués et sur mesure leur permettant d'opérer. La variété de l'offre est impressionnante : il est possible de louer des infrastructures performantes dès 20 USD l'heure. Si les menaces avancées et persistantes ou APT (« Advanced Persistent Threats ») étaient auparavant surtout l'apanage de gouvernements, elles sont en bonne voie de devenir des produits de consommation dans le Web clandestin. Les barrières à l'entrée sont de ce fait beaucoup plus basses pour les criminels. La vente de données volées, les modèles d'affaires basés sur le chantage par des logiciels de rançon et, surtout, les attaques de déni de service distribué ou DDoS (« Distributed Denial of Service ») sont potentiellement très lucratifs. Les DDoS sont capables de paralyser un service en surchargeant un serveur par une accumulation de requêtes.

Le professionnalisme des attaques spécifiques devrait encore s'accroître en raison de la diffusion incontrôlée de failles encore inconnues (« zero-day exploits ») et d'instruments d'attaque hautement développés. Autrefois consciencieusement gardées par les armées et les services de renseignement, ces armes délicates de cyberattaque sont parvenues au public au cours des deux dernières années à la faveur de fuites de données survenues dans les services de renseignement. La demande se fait toujours plus pressante envers les organes étatiques concernés pour qu'ils annoncent immédiatement d'éventuels points faibles aux producteurs plutôt que de les exploiter à leurs propres fins d'espionnage.

La vulnérabilité continue d'augmenter

La cybercriminalité progresse aussi parce qu'une mutation numérique est en cours du côté des personnes attaquées. Le degré et la complexité des interconnexions qui en résultent augmentent en raison de la mise sur pied et de l'extension d'écosystèmes numériques dans l'exploitation des entreprises et dans leur système de distri-

1 Le présent article a été rédigé en coopération avec Umberto Annino, président de l'ISSS.

bution. Selon une étude sur la numérisation dans les PME suisses[2], près des trois quarts des entreprises interrogées mènent déjà des projets de numérisation. Cette enquête montre aussi où résident les risques pour l'avenir : une large majorité d'entreprises estiment que le manque de savoir-faire et le financement des importants investissements nécessaires constituent leurs principaux défis.

L'exposition aux attaques et donc la vulnérabilité inhérente à la numérisation continueront d'augmenter. Ce sera d'autant plus vrai si l'industrialisation des solutions dans le domaine des technologies de l'information et de la communication (TIC) progresse rapidement. Les machines, les logiciels et les capacités de calcul seront plus avantageux, interconnectables et supposés plus simples à employer et à entretenir justement parce que l'industrie 4.0 sera en plein essor.

La standardisation et l'industrialisation de la sécurité des TIC n'ont pas suivi le rythme. Lorsque les attaques sont mieux ciblées, les solutions qui ont fait le succès des techniques de sécurité ne sont plus guère utiles. En bref, nous circulons à 200 km/h sur les autoroutes numériques dans un véhicule dont l'équipement de sécurité appartient au passé. Les développeurs ont négligé à ce stade d'incorporer la sécurité dans la conception même des matériels et des logiciels pour minimiser leur vulnérabilité (« security by design »). Les conséquences de cette négligence apparaissent désormais.

La détection des attaques est tardive

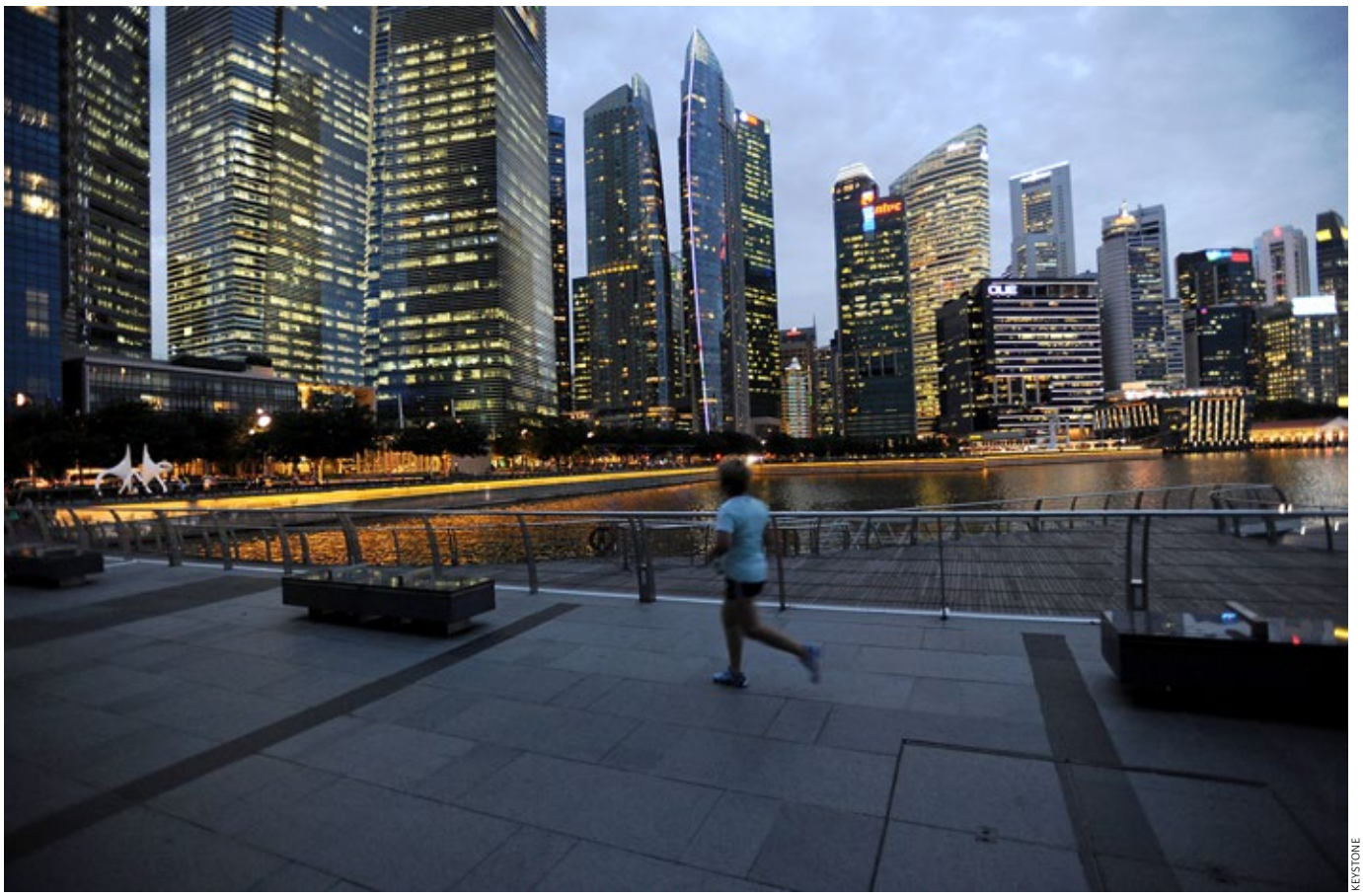
Si l'appel à une gestion des risques liés aux infrastructures numériques se fait toujours plus pressant, la menace concrète, autrement dit la base de l'évaluation classique du risque, ne saurait être qualifiée clairement. Elle échappe a fortiori aux tentatives de la quantifier. De toute évidence, les attaques contre les infrastructures numériques et les données surviennent très rapidement. Il est, toutefois, difficile d'évaluer l'ampleur du risque inhérent aux informations détournées. Celui-ci peut concerner des données sur les clients et les affaires, des informations relevant de la propriété intellectuelle et d'autres permettant d'identifier l'utilisateur. Le délai entre l'infection et la détection d'une attaque réussie est de plus en plus long (environ 300 jours actuellement). En outre – ce point est critique –, la plupart des personnes attaquées doivent être averties par des partenaires extérieurs pour se rendre compte de la situation. Une étude[3] a été menée récemment par l'Information Security Society Switzerland (ISSS) auprès de PME, d'entreprises de grande taille et de groupes suisses. Une majorité de répondants ont estimé que les flux involontaires de données constitueront à l'avenir un risque prédominant et que la résilience dans le domaine des possibilités de détection et de contrôle devient toujours plus urgente.

Selon cette étude, confirmée par d'autres, la sensibilisation aux cyberdangers et leur compréhension ont nettement progressé au cours des deux dernières années, tout comme la compréhension des mesures qu'ils requièrent dans les entreprises. Toutefois, les grandes entreprises internationales continuent d'évaluer les dangers à un degré plus élevé et elles se montrent plus critiques quant à leur sécurité que les petites entreprises ac-

2 Gering Marco et al., *Digitalisierung in Schweizer Klein- und Mittelunternehmen : KMU-Spiegel 2017*, Saint-Gall, 2017.

3 Les résultats reposent sur 110 réponses d'entreprises dans le cadre d'une enquête menée en juillet dernier. L'ISSS présentera une évaluation plus complète de cette étude d'ici à la fin de l'année.

Singapour a introduit des normes et un devoir d'annonce pour les infrastructures critiques comme les banques. La Suisse est loin de ce niveau de cybersécurité.



KEYSTONE

tives sur le plan national. L'étude de l'ISSS montre qu'en dépit de leur niveau de sensibilisation, un cinquième seulement de toutes les entreprises ont investi dans la sécurité une part de leurs ressources informatiques plus élevée en 2017 que l'année précédente. Simultanément, seule une infirme minorité est prête à consacrer davantage de moyens à la sécurité informatique, alors que les budgets informatiques régressent. Cette attitude montre que les entreprises ne sont en général pas disposées, les ressources informatiques faisant défaut, à renoncer à davantage de prestations au profit de la sécurité.

Les choses bougent à l'étranger

Vu l'importance des infrastructures numériques, une discussion s'est ouverte quant aux prestations, aux réglementations et aux mesures dont l'État doit s'acquitter, et ce pas seulement pour les infrastructures critiques. Quelle est la situation à l'étranger de ce point de vue ? Les exploitants d'infrastructures critiques sont-ils soumis à des normes minimales contraignantes ? Les dispositions prises concernent-elles seulement certains secteurs et, au sein de ceux-ci, seulement des exploitants précis ? Ces dispositions couvrent-elles également les exploitants d'infrastructures numériques telles que les solutions de distribution basées sur une plateforme, les services en nuage ou les moteurs de recherche ? Il n'est pas étonnant que des pays dont le gouvernement est autoritaire, comme la Chine ou Singapour, aient imposé des réglementations strictes ces trois dernières années. Ces pays ont adopté des normes de sécurité informatiques et des obligations d'annoncer pour les infrastructures critiques et pour toutes les infrastructures numériques dont l'importance est reconnue. Aux États-Unis, on a introduit, grâce au « Cyber Security Framework » du National Institute of Standards and Technology » (Nist), une quasi-norme relativement détaillée pour les infrastructures critiques. Même si elles ne sont pas explicitement contraignantes, les propositions sécuritaires exercent, avec les différentes lois nationales et en vigueur au niveau des États, une certaine pression. Elles permettent à l'administration d'intervenir régulièrement chez les exploitants privés.

La mise en œuvre de la directive sur la sécurité des réseaux et de l'information (directive SRI), entrée en vigueur en août 2016, devient la norme déterminante pour l'espace européen. Elle doit garantir un niveau de sécurité élevé en ce qui concerne les réseaux et les systèmes d'information de l'Union européenne. Les États membres doivent créer des points de contact nationaux, établir des centres de réponse aux urgences informatiques (Cert) et identifier les entreprises faisant partie des infrastructures numériques critiques. De telles firmes doivent se protéger sur le plan technique et annoncer les incidents concernant la sécurité. Ces exigences s'appliquent aussi aux prestataires de services numériques pertinents. Si des pays comme l'Allemagne ou la France avaient déjà introduit des normes minimales avant l'introduction des dispositions SRI, d'autres pays, tels le Royaume-Uni et la Suède, doivent évoluer à ce niveau.

La réponse de la Suisse est encore hésitante

En Suisse, il n'existe pas de dispositif permettant de protéger complètement des cyberdangers ni d'obligation d'annoncer pour les infrastructures critiques. Lorsqu'elles existent, les règles et les obligations sont sectorielles et spécifiques. Par exemple, on trouve des règles internes liées à des mesures techniques et organisationnelles pour le trafic aérien et ferroviaire, parce que la protection et la sécurité y revêtent la plus haute priorité.

Face aux cybermenaces, l'Autorité fédérale de surveillance des marchés financiers a également accentué les charges qu'elle impose dans ses circulaires pour plus de cybersécurité, mais elle n'a pas introduit d'obligation d'annoncer. Cette dernière n'apparaît que lors d'interruptions spécifiques de l'approvisionnement, par exemple dans le domaine des télécommunications, mais elle ne se focalise pas sur la saisie de la cybermenace. Cette situation complique les tentatives de dépasser le stade d'un tableau fragmenté. Cependant, le message concernant la révision partielle de la loi sur les télécommunications[4] prévoit, au niveau de la loi, des dispositions en matière de protection et l'obligation d'annoncer. Cela montre que le débat sur les normes et l'obligation d'annoncer faite aux exploitants d'infrastructures critiques (et éventuellement de services numériques), selon l'exemple de la directive SRI, est lancé et s'intensifiera.

Il convient de ne pas écarter les entreprises au moment de déterminer par qui et comment la cybersécurité devrait être encouragée, voire réglementée. L'amélioration de la cybersécurité, un fondement de la confiance et d'une mutation numérique durable s'agissant du traitement des données, restera un thème clé pour la place technologique et scientifique suisse. Dans ce contexte, le groupe d'experts « Avenir du traitement et de la sécurité des données », institué par le Conseil fédéral, se penche sur le sujet. Il soumettra des propositions dans le cadre de son rapport final, qui est attendu pour la mi-2018.

4 Le Conseil fédéral a adopté le 6 septembre 2017 le message concernant la révision partielle de la loi sur les télécommunications (LTC).

Arié Malz
Responsable du secrétariat du groupe d'experts « Avenir du traitement et de la sécurité des données », Département fédéral des finances (DFF), Berne