Dépendance et complexité

Cybersécurité: Défis pour la Suisse politique

Etat des lieux

Notre société et notre économie dépendent de manière critique d'un grand nombre d'infrastructures numériques. Nous sommes tributaires de la disponibilité constante de la connectivité et du bon fonctionnement d'innombrables technologies et services que nous ne contrôlons plus directement. Des événements qui ont lieu à distance peuvent avoir des impacts locaux immédiats, durables et graves. Plus que jamais auparavant dans l'histoire, les effets de réseau en cascade représentent aujourd'hui un risque bien plus élevé pour l'économie dans son ensemble.

La crise financière de 2007 a été riche en enseignements sur les risques opaques et sous-estimés des systèmes fortement interconnectés et interdépendants. Depuis lors, nous n'avons fait que renforcer nos dépendances.

La numérisation progressive et la tendance à tout interconnecter augmentent non seulement l'efficacité, mais amplifient aussi les conséquences d'un événement aléatoire, d'un dysfonctionnement, d'une mauvaise configuration, d'attaques malveillantes, de jeux de pouvoir politiques ou de sanctions. Actuellement, la Suisse court le risque de générer des dépendances et des problèmes sensibles par une utilisation prématurée et, dans certains cas, l'acquisition et la fourniture non contrôlées de produits et de services numériques. De tels problèmes ne se manifesteront qu'à long terme (ou en cas de crise) et ne pourront alors être corrigés qu'à grands frais.

Recommandations

1. Saluer la numérisation et, en même temps, investir dans la compréhension des principaux risques et prendre des décisions en toute conscience sur les investissements critiques.
2. Pour les autorités, les organisations et les particuliers, il est impératif d'évaluer scrupuleusement les dépendances critiques de leur cyberinfrastructure et de trouver activement un équilibre entre optimisation (efficacité, gains à court terme), résilience (redondance, survie à long terme) et coûts correspondants.
3. Partir de l'échec et planifier en conséquence. Les fonctions critiques pour la société et l'économie doivent, à un certain niveau, pouvoir résister aux défaillances. Il est impératif de planifier, communiquer, financer, mettre en œuvre et tester les redondances.
4. «Attaque une difficulté dans ses éléments faciles. Accomplis une grande œuvre par de menus actes. La chose la plus difficile au monde se réduit finalement à des éléments faciles.» - Laozi (Lao Tseu), 600 av. J.C.

Défis

La méconnaissance du niveau de sécurité et la dépendance croissante au sein des infrastructures et entre elles génèrent des menaces critiques à mesure que la numérisation progresse[1]. Les liens étroits, la complexité et les dépendances grandissantes entre un faible nombre d'acteurs, de services, de technologies et d'infrastructures dominants entraînent une énorme accumulation de risques critiques dans la société numérique. Les choses deviennent de plus en plus complexes, connectées et interdépendantes, à un rythme superlinéaire.

- **Connectivité et réseau:** les services et les appareils ont besoin d'une communication continue et d'un réseau disponible en permanence. La plupart des infrastructures échappent à notre contrôle direct et les défaillances paralysent des fonctions essentielles.
- **Matériel et logiciels:** quelques produits logiciels et matériels dominants, issus d'un nombre encore plus restreint de fabricants, sont absolument essentiels au fonctionnement intersectoriel. Les points faibles, le bon fonctionnement et l'effet d'enfermement entraînent des problèmes de disponibilité, d'activité, de protection des données et de stabilité du système.
- **Protocoles:** la dépendance à l'égard d'un nombre restreint de protocoles internet et de leur infrastructure de déploiement augmente le risque d'effets en cascade dans différents secteurs[2].
- **Cloud, fournisseurs de cloud et modèles de service**: le nombre croissant de services en ligne ou dans le nuage, combiné à la pression constante pour passer à des modèles d'abonnement, augmente la dépendance à l'égard de la disponibilité des fournisseurs de réseaux et de services. Une partie significative du commerce mondial sur internet dépend de moins de dix fournisseurs de cloud issus de deux pays seulement. Les petites défaillances génèrent toujours plus de dégâts et une accumulation énorme et croissante de risques systémiques[3].
- **Cryptographie**: quelques méthodes cryptographiques dominantes et leurs implémentations supportent pratiquement toutes les garanties de sécurité du monde virtuel. Énorme exposition systémique à des points faibles encore inconnus en mathématiques et dans l'implémentation ou à des avancées soudaines de l'informatique quantique.
- **Héritage**: il n'est plus possible d'exploiter de manière isolée des produits et des services sans connectivité ou assistance continues du fabricant tout au long de leur durée de vie. Risque critique dû à une disparition prématurée du fabricant ou du fournisseur (faillite, obsolescence forcée, sanction).
- **Politique**: forte concentration de fabricants dominants et d'infrastructures dans quelques pays seulement. Le contrôle par les infrastructures numériques remplace le pouvoir politique, car les nations peuvent aisément traverser les frontières pour perturber les systèmes du monde réel. La diffusion de l'internet dans le monde physique entraîne une escalade radicale des préoccupations des gouvernements en matière de vie privée, de discrimination, de sécurité humaine, de démocratie et de sécurité nationale[4].

[1] Reference to Cyber Security "Wake-Up Calls" - https://ctovision.com/reference-cyber-security-wake-calls/

[2] How the Dyn DDoS attack unfolded - https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html

[3] Adobe is cutting off users in Venezuela due to US sanctions - https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions

[4] The Internet in Everything: Freedom and Security in a World with No Off Switch - https://www.amazon.com/Internet-Everything-Freedom-Security-Switch/dp/0300233078

Nécessité d'agir

Tout est interconnecté et devient de plus en plus complexe. Nous ne pouvons plus agir isolément. Les mesures efficaces et durables de protection et de mise à disposition des produits et des infrastructures vont au-delà de la sécurisation des systèmes individuels. Après la crise financière de 2008, les économistes ont inventé l'expression «to big to fail» pour qualifier les entreprises financières dont les conséquences d'une faillite seraient catastrophiques pour l'économie. Autoriser leur insolvabilité serait irresponsable.

Nous devons identifier et évaluer les infrastructures de numérisation **«to critical to fail»** et développer des stratégies pour minimiser les dépendances, protéger ces infrastructures et accroître la résilience de la société et de l'industrie numériques. Nous devrions le faire avant qu'une crise ne survienne.

Comprendre et maîtriser la complexité

La complexité des systèmes et des infrastructures entraîne une vulnérabilité accrue, des défaillances, des erreurs, une confusion humaine et des difficultés à se remettre d'un problème[5]. Nous devons privilégier des architectures, des conceptions et des implémentations simples et cohérentes afin d'éviter toute complexité et dépendance inutiles. Il n'est pas possible de prévoir, de tester et de modéliser complètement toutes les conditions avec de tels systèmes. C'est pourquoi nous devons accepter les défaillances et les compromis, les prendre en compte et concevoir des systèmes qui ne présentent aucun danger. La seule chose qui ait jamais apporté de réels gains en matière de sécurité a été la maîtrise de la complexité[6].

[5] Flash Crash - https://en.wikipedia.org/wiki/Flash_crash

[66] Security, Moore's law, and the anomaly of cheap complexity, Thomas Dullien - https://rule11.tech/papers/2018-complexitysecuritysec-dullien.pdf

Références

- Systemic Risk in the Broad Economy - www.rand.org/t/RR4185
- Globally networked risks and how to respond, Dirk Helbing - http://adaptation.ei.columbia.edu/files/2018/09/nature12047.pdf
- The Precautionary Principle - https://www.fooledbyrandomness.com/PrecautionaryPrinciple.html
- Whitepapger Supply Chain Security, ICT Switzerland - https://ictswitzerland.ch/en/white-paper-supply-chain-security

Contact

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
Septembre 2020