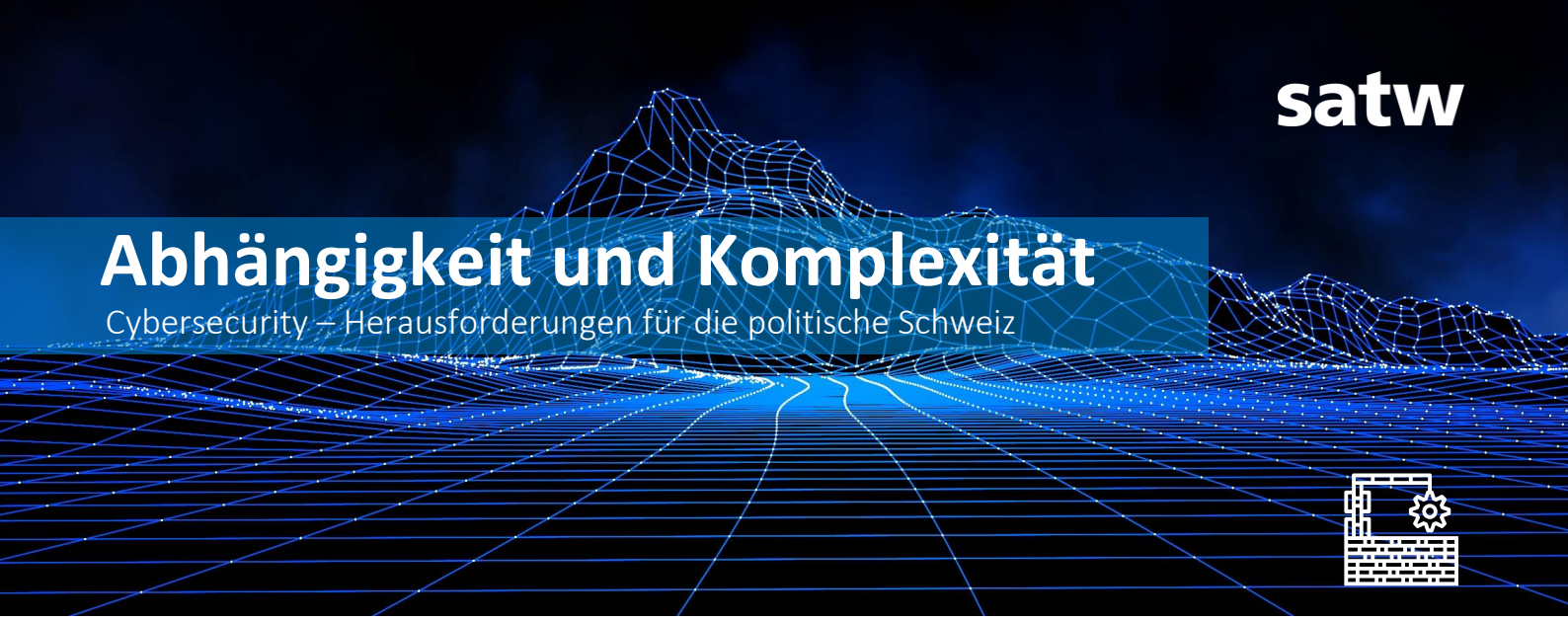

Abhängigkeit und Komplexität

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Unsere Gesellschaft und Wirtschaft sind in kritischer Weise von einer Vielzahl digitaler Infrastrukturen abhängig geworden. Wir sind auf die ständige Verfügbarkeit von Konnektivität und das korrekte Funktionieren unzähliger Technologien und Dienste angewiesen, die wir nicht mehr direkt kontrollieren. Ereignisse, die in der Ferne stattfinden, können sofortige, langanhaltende und schwerwiegende lokale Auswirkungen haben. Für die gesamte Wirtschaft stellen kaskadenartige Netzwerkeffekte heute ein viel grösseres Risiko dar als jemals zuvor in der Geschichte.

Die Finanzkrise von 2007 hat uns viel über die undurchsichtigen und unterschätzten Risiken hochgradig vernetzter und voneinander abhängiger Systeme gelehrt. Seitdem haben wir unsere Abhängigkeiten nur noch verstärkt.

Die fortschreitende Digitalisierung und die Tendenz, alles miteinander zu verbinden, erhöht nicht nur die Effizienz, sondern verstärkt auch die Folgen eines zufälligen Ereignisses, einer Fehlfunktion, einer Fehlkonfigurationen, böswilliger Angriffe, politischer Machtspiele oder Sanktionen. Gegenwärtig läuft die Schweiz Gefahr, durch die verfrühte Nutzung und in einigen Fällen durch die unkontrollierte Beschaffung und Bereitstellung digitaler Produkte und Dienstleistungen kritische Abhängigkeiten und Probleme zu schaffen. Solche Probleme werden sich erst langfristig (oder im Krisenfall) zeigen und können dann nur mit grossem Aufwand korrigiert werden.

Empfehlungen

1. Nehmen Sie die Digitalisierung an, aber investieren Sie in das Verständnis der Hauptrisiken und treffen Sie bewusste Entscheidungen über kritische Investitionen.
2. Die Regierung, Organisationen und Einzelpersonen müssen kritische Abhängigkeiten in ihrer Cyberinfrastruktur bewusst bewerten und aktiv ein Gleichgewicht zwischen Optimierung (Effizienz, kurzfristige Gewinne) und Belastbarkeit (Redundanz, langfristiges Überleben) und den entsprechenden Kosten finden.
3. Gehen Sie von einem Scheitern aus und planen Sie entsprechend. Kritische Funktionen für Gesellschaft und Wirtschaft müssen bis zu einem bestimmten Grad Ausfällen standhalten. Redundanzen müssen geplant, kommuniziert, finanziert, durchgeführt und getestet werden.
4. «Greife eine Schwierigkeit bei ihren leichten Elementen an. Vollende ein grosses Werk mit kleinen Akten. Die schwierigste Sache der Welt beginnt stets als Leichtes» - Laozi (Laotse), 600 v. Chr.

Herausforderungen

Mangelndes Bewusstsein für das Sicherheitsniveau und die zunehmende Abhängigkeit innerhalb und zwischen den Infrastrukturen führen mit fortschreitender Digitalisierung zu kritischen Bedrohungen[1]. Die engen Verbindungen, die Komplexität und die zunehmende Abhängigkeiten von wenigen und dominanten Akteuren, Diensten, Technologien und Infrastrukturen führen zu einer enormen Anhäufung kritischer Risiken in der digitalen Gesellschaft. Die Dinge werden in superlinearem Tempo immer komplexer, häufiger miteinander verbunden und voneinander abhängig.

- **Konnektivität & Netzwerk**: Dienste und Geräte benötigen eine kontinuierliche Kommunikation und ein ständig verfügbares Netzwerk. Die meisten Infrastrukturen entziehen sich unserer direkten Kontrolle, Ausfälle lähmen kritische Funktionen.
- **Hard- und Software**: Einige wenige dominante Hard- und Softwareprodukte von einer noch geringeren Anzahl von Herstellern sind für ein sektorübergreifendes Funktionieren absolut notwendig. Schwachstellen, Fehlfunktionen und der Lock-in-Effekt führen zu Problemen bei Verfügbarkeit, Geschäftstätigkeit, Datensicherheit und Systemstabilität.
- **Protokolle**: Die Abhängigkeit von einer kleinen Anzahl von Internet-Protokollen und ihrer Bereitstellungsinfrastruktur erhöht das Risiko von Kaskadeneffekten über verschiedene Sektoren hinweg[2].
- **Cloud, Cloud-Provider und Servicemodelle**: Die zunehmende Anzahl von Online- oder Cloud-basierten Diensten, verbunden mit dem ständigen Druck, zu Abonnement-Modelle überzugehen, erhöht die Abhängigkeit von der Verfügbarkeit von Netz- und Serviceanbietern.

Ein bedeutender Teil des globalen Internet-Geschäfts hängt von weniger als zehn Cloud-Providern aus nur zwei Ländern ab. Kleine Ausfälle verursachen immer mehr Schaden und eine riesige und wachsende Häufung von systemischen Risiken[3].

- **Kryptographie**: Einige dominante kryptographische Methoden und ihre Implementierungen unterstützen fast alle Sicherheitsgarantien in der digitalen Welt. Es ergibt sich eine enorme systemische Exposition gegenüber noch unbekannten Schwachstellen in der Mathematik, der Implementierung oder dem plötzlichen Fortschritt im Quanten Computing.
- **Vermächtnis**: Produkte und Dienstleistungen können nicht mehr isoliert betrieben werden, ohne dass während ihrer gesamten Lebensdauer eine kontinuierliche Konnektivität oder Unterstützung durch den Hersteller gewährleistet ist. Es besteht ein kritisches Risiko durch vorzeitiges Verschwinden des Herstellers oder Lieferanten (Konkurs, erzwungene Stilllegung, Sanktion).
- **Politisch**: Es gibt eine hohe Konzentration dominanter Hersteller und Infrastrukturen in nur wenigen Ländern. Die Kontrolle über die digitale Infrastruktur ersetzt die politische Macht, da Nationen leicht Grenzen überschreiten können, um Systeme der realen Welt zu stören. Die Ausbreitung des Internets in die physische Welt führt zu einer radikalen Eskalation der Bedenken der Regierung in Bezug auf Privatsphäre, Diskriminierung, menschliche Sicherheit, Demokratie und nationale Sicherheit.[4]

[11] Reference to Cyber Security «Wake-Up Calls» - https://ctovision.com/reference-cyber-security-wake-calls/
[22] 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

Handlungsbedarf

Alles ist miteinander verbunden und wird immer komplexer. Wir können nicht länger isoliert handeln. Wirksame und nachhaltige Massnahmen zum Schutz und zur Bereitstellung von Produkten und Infrastruktur gehen über die Sicherung einzelner Systeme hinaus. Nach der Finanzkrise von 2008 entwickelten Ökonomen den Begriff «too big to fail», um Finanzunternehmen zu beschreiben, deren Scheitern katastrophale Folgen für die Wirtschaft hätte. Ihre Zahlungsunfähigkeit zuzulassen wäre unverantwortlich.

Wir müssen die «to critical to fail» digitalen Infrastrukturen identifizieren und bewerten und Strategien entwickeln, um Abhängigkeiten zu minimieren, diese Infrastrukturen zu schützen und die Belastbarkeit der digitalen Gesellschaft sowie der Industrie zu erhöhen. Wir sollten dies tun, bevor es zu einer Krise kommt.

Komplexität verstehen und beherrschen

Die Komplexität von Systemen und Infrastrukturen führt zu erhöhter Verwundbarkeit, Ausfällen, Fehlern, menschlicher Verwirrung und Schwierigkeiten bei der Bewältigung eines Problems[5]. Wir müssen einfache und konsistente Architekturen, Entwürfe und Implementierungen bevorzugen, um unnötige Komplexität und Abhängigkeiten zu vermeiden. Es ist nicht möglich, mit solchen Systemen alle Bedingungen vollständig vorherzusagen, zu testen und zu modellieren. Deshalb müssen wir Ausfälle und Kompromisse akzeptieren, sie berücksichtigen und Systeme entwerfen, die sicher sind. Das Einzige, was jemals echte Sicherheitsgewinne gebracht hat, war die Beherrschung der Komplexität.[6]

[5] Flash Crash - https://en.wikipedia.org/wiki/Flash_crash
[6] Security, Moore's law, and the anomaly of cheap complexity, Thomas Dullien - https://rule11.tech/papers/2018-complexitysecuritysec-dullien.pdf

Referenzen

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

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

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

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
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
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020