

Was geht (nicht) ohne Internet?

Das Forschungsprojekt ISIDOR hat sich in den vergangenen zwei Jahren mit der Frage beschäftigt, was passiert, wenn das Internet in Österreich großflächig und für einen längeren Zeitraum ausfällt. Dabei wurden verschiedene Szenarien betrachtet, von Ausfällen bestimmter Internetdienste, bis hin zu einem Totalausfall. Dem "All Hazards"-Ansatz des Austrian Programme for Critical Infrastructure Protection (APCIP) folgend, standen nicht die Ursachen eines derartigen Ausfalls und deren Vermeidung im Fokus des Projekts, sondern das Augenmerk wurde auf den Bereich Cyber-Resilience gerichtet.

Dabei galt es, herauszufinden, wie sich die Lage nach einem Schadensfall entwickeln könnte, und wie die dadurch ausgelöste Krise bestmöglich aufgelöst wird.

Anstoß für das Projekt war der entsprechende Arbeitsschwerpunkt im Staatlichen Krisen- und Katastrophenschutzmanagement. Es war klar, dass eine große Abhängigkeit von dieser Infrastruktur und Technik besteht. Es wurde aber bisher nicht im Detail untersucht, wie die Lage nach einem Ausfall in den verschiedenen Sektoren aussehen könnte, und welche sektorübergreifenden Fragestellungen sich daraus ergeben. Ziel des Projekts war es einerseits, Antworten auf diese Fragen zu finden und auszuloten, welche Maßnahmen in der Vorbereitung auf so eine Krise die Handlungsfähigkeit verbessern und den Impact im Ernstfall reduzieren würden. Andererseits wurde auch das generelle Verständnis für den Umgang mit vernetzten Krisen verbessert.

Das Projekt wurde gefördert bzw. finanziert im Rahmen des FTI-Programms KIRAS durch das Bundesministerium für Finanzen und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt. Die Projektleitung lag beim Institut für Produktionswirtschaft und Logistik der Universität für Bodenkultur Wien. Weitere Projektpartner waren das Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften, das Bundesministerium für Inneres, das Bundesministerium für

Digitalisierung und Wirtschaftsstandort, sowie die Firmen Infraprotect, Mar Adentro und Repuco.

Ergebnisse

Wie sehr sind nun unterschiedliche Sektoren kritischer Infrastrukturen von einem Ausfall des Internets betroffen? Was voraussichtlich weiterhin funktionieren sollte, ist die Versorgung mit Trinkwasser und die Entsorgung des Abwassers. Es ist auch zu erwarten, dass die Stromversorgung in Österreich dadurch nicht eingeschränkt wird, wie wohl es eine Ausnahmesituation für das Management der Netze darstellen würde, das

eventuell weitere krisenhafte Ereignisse nicht ohne weiteres ausgleichen könnte.

Große Schwierigkeiten sind dort zu befürchten, wo IT-Prozesse und -Ressourcen im Normalbetrieb ausgelagert wurden. Das ist beispielsweise bei der Nutzung von Cloud-Diensten oder

dem Outsourcing von IT-Personal der Fall. Ähnlich verhält es sich mit dezentralen, mobilen IT-Systemen, wie bspw. Patientendokumentation im Rettungswesen. Stark betroffen wäre auch der Banken- und Finanzsektor, wo viele Geschäftsprozesse ohne die Möglichkeit zur Datenkommunikation undenkbar sind.

Ein sektorübergreifendes Problem ergäbe sich aus der Betroffenheit des Transportwesens. Ohne Schnittstellen zur Datenkommunikation wäre der Transport von Gütern nur mit Einschränkungen möglich. Die Daten- und Dokumentationsverarbeitung, sowie das Transportmanagement (z.B. Sendungsverfolgung, Aviso, Einlagerung, Wiederauffinden, Zustellung etc.) sind in hohem Maße von miteinander vernetzten IT-Systemen abhängig. Gleichzeitig verlassen sich viele Organisationen darauf, dass z.T. mehrmals täglich – just in time – zugestellt wird, um das jeweils dringend Benötigte zu erhalten, ohne ein großes Lager mit differenziertem Bestand erhalten zu müssen.

Durch die zu erwartenden Einschränkungen in der Mobilkommunikation, entweder weil – je nach Ursache – das Mobilfunknetz selbst ausfällt, oder weil es aufgrund der Verlagerung eines großen Anteils des Datenverkehrs überlastet sein kann, ist davon auszugehen, dass die meiste Sicherheitstechnik nicht funktionieren wird: Alarmanlagen und Brandmelder, die direkt an Polizei oder Feuerwehr melden, wären ebenso



wenig funktionsfähig wie Alarmierungen (z.B. von Krisenstäben) über Apps oder SMS.

Manches davon kann durch die Umstellung auf analoge Prozesse und den erhöhten Personaleinsatz ausgeglichen werden, wenn das zuvor geübt wurde, und die notwendigen Ressourcen im Krisenfall zur Verfügung stehen.

Vernetzte Krisen

Der Trend zur Konvergenz in der Infrastruktur und Effizienz in den Geschäftsprozessen führte in den vergangenen Jahrzehnten zu einer starken Reduktion von „Puffern“ im Gesamtsystem. Dadurch steigt nicht nur allgemein die Abhängigkeit durch die voranschreitenden Vernetzung, sondern es sinkt zugleich die Fehler-toleranz des Systems.

Durch die gegenseitigen Abhängigkeiten über sektorale Grenzen hinweg wird es kaum einen Bereich geben, der durch einen Ausfall internetbasierter Dienste nicht beeinträchtigt wäre. Ähnlich wie bei einem großflächigen Stromausfall spricht man auch hier von einer sog. vernetzten Krise. Es ist eine sehr komplexe Situation mit hoher Dynamik und vielen Unsicherheiten erwartbar. Letztendlich ist es auch mit viel Aufwand nicht möglich, genau vorherzusagen, wie die Lage nach so einem Schadensfall aussähe. Zielführender ist es, die Kräfte für das Krisenmanagement zu stärken und die First Responders in Trainings auf eine solche Situation vorzubereiten. Dadurch ließe sich die Handlungsfähigkeit im Ernstfall besser erhalten oder sogar erhöhen, als durch den Versuch genauerer Prognosen.

Was ist zu tun?

Der Situation während eines großflächigen und langandauernden Internetausfalls kann man auf verschiedenen Ebenen begegnen.

Der langfristige Ausfall kritischer, internetbasierter Dienste ist in Österreich noch nicht vorgekommen. Dementsprechend fehlt es an Erfahrungswissen. Übungen für alle Organisationen, die in der Krisenbewältigung arbeiten, helfen dabei, die erforderlichen Kompetenzen für so einen Fall zu vermitteln und die Abläufe, die sich stark vom Regelbetrieb unterscheiden können, zu trainieren.

Organisationsintern könnten KI-Betreiber strategische Überlegungen dazu anstellen, welche Prozesse sich im Ernstfall auch offline erledigen lassen.

In einigen Bereichen, z.B. Bargeld und Lebensmittel-logistik, bedarf es weiterer Arbeit aller Stakeholder:innen, um einer robusten Lösung näher zu kommen.

Speziell im Gesundheitswesen könnte es notwendig werden, krisenrelevante Versorgungsgüter in großem Umfang dezentral zu bevorraten.

Kommunikationswege, die von der fürs Internet genutzten Infrastruktur unabhängig sind, sollten bewahrt und ausgebaut werden, um in der Krise eine Kommunikation zwischen allen Beteiligten zu ermöglichen. Es gibt in Österreich schon einige Netze, die autark funktionieren können. Statt eines oft geforderten neu errichteten Staatsgrundnetzes wäre es leichter und günstiger, eine Ausfallslösung zu realisieren, die diese potentiellen „Inseln“ miteinander verbindet (Dazu gab es auch einen Austausch zwischen dem ISIDOR- und dem Hammondorgel-Projektteam). Ebenso muss gewährleistet werden, dass der Kommunikationsaustausch mit europäischen Institutionen während einer solchen Krise erhalten bleibt.

Auf dem Gebiet der gemeinsamen Vorbereitung aller Akteur:innen ist, nicht zuletzt im Rahmen des Projekts, in den vergangenen Jahren viel passiert. Eine weitere Vertiefung ist sinnvoll und wird von den Betreibern kritischer Infrastrukturen gewünscht. Auch weitere Forschung ist, aufbauend auf den Ergebnissen aus ISIDOR, erforderlich, um zu sehen, wo die Implementierung zukünftiger Technologien die Abhängigkeit vom Internet weiter erhöhen wird; bspw. im Feld autonomer Systeme. Fest steht, dass ein langandauernder und großflächiger Ausfall internetbasierter Dienste mit anderen vernetzten Krisen wie Blackout, Gasversorgungsengpässen gleichzusetzen ist.

Eine ausführliche Darstellung der Projektarbeit, inklusive aller Ergebnisse und Empfehlungen, findet sich im Abschlussbericht, der ab Ende November unter: <https://short.boku.ac.at/isidor> verfügbar sein wird.

Projektkonsortium



 Bundesministerium Inneres

 Bundesministerium Digitalisierung und Wirtschaftsstandort

Das Projekt ISIDOR wurde gefördert bzw. finanziert im Rahmen des FTI-Programms KIRAS durch das Bundesministerium für Finanzen und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt.

 Bundesministerium Finanzen



Autor:innen:

Krieger-Lamina, Jaro jaro.krieger-lamina@oeaw.ac.at

Schachenhofer, Larissa larissa.schachenhofer@boku.ac.at