

WAS GEHT OHNE INTERNET?

IN KÜRZE

- In so gut wie allen Branchen sind wir bei wesentlichen Arbeitsvorgängen auf das Internet, und auf eine funktionierende IT-Infrastruktur, angewiesen.
- Die Betreiber Kritischer Infrastrukturen müssen darauf vorbereitet sein, dass ihre Dienste auch ohne Internet erbracht werden können. Das schließt Kommunikation innerhalb der Organisation sowie mit dem Staatlichen Krisen- und Katastrophenschutzmanagement ein.
- Kommt es bei der Kritischen Infrastruktur zu einem Schadensfall spricht man von einer vernetzte Krise. Sie zeichnet sich u.a. durch eine hohe Dynamik aus, die es erschwert, seriöse Aussagen über den weiteren Verlauf der Krise zu treffen. Wichtiger als starre Checklisten sind in diesem Fall eindeutig Kommunikationsfähigkeit und Krisenmanagement.

WORUM GEHT ES?

Was passiert mit Kritischen Infrastrukturen, wie z.B. dem Stromnetz oder der Versorgung von Krankenhäusern, wenn das Internet in Österreich großflächig und für einen längeren Zeitraum ausfällt? Die im Projekt ISIDOR analysierten Szenarien reichen von Ausfällen bestimmter Internetdienste bis hin zu einem Totalausfall. Der „All Hazards“-Ansatz des Austrian Programme for Critical Infrastructure Protection (APCIP) konzentriert sich bei der Analyse weniger die Ursachen eines derartigen Ausfalls und deren Vermeidung, sondern auf Cyber-Resilienz, also das Erkennen von Problemen, ohne dass Abläufe unterbrochen werden. Wie sieht die Lage nach einem Ausfall in den verschiedenen Sektoren aus und welche sektorübergreifenden Herausforderungen ergeben sich daraus? Durch eine sektorübergreifende Betrachtungsweise und die Erfahrungen aus den

Vorbereitungen auf einen Blackout konnte auch das generelle Verständnis für den Umgang mit vernetzten Krisen verbessert werden. Denn – durch die gegenseitigen Abhängigkeiten über sektorale Grenzen hinweg wird es kaum einen Bereich geben, der durch einen Ausfall Internet-basierter Dienste nicht betroffen ist. So würde eine Beeinträchtigung von Logistikprozessen jedenfalls in den Gesundheitssektor und andere Versorgungsgebiete wirken. Ähnlich wie bei einem großflächigen Stromausfall spricht man auch hier von einer sogenannten vernetzten Krise.



Was geht nicht, wenn das Internet ausfällt?

Ein möglicher Internetausfall ist eine sehr komplexe Situation mit hoher Dynamik und vielen Unsicherheiten. Der Trend zur Zusammenfassung von Infrastruktur in der Verwaltung von Rechenzentren und Effizienzsteigerung in Geschäftsprozessen hat verstärkt „Puffer“ im Gesamtsystem abgebaut. Damit steigt nicht nur allgemein die Abhängigkeit durch die voranschreitende Vernetzung, sondern es sinkt gleichzeitig auch die Fehlertoleranz des Systems. Auch ist es wichtig, bereits vor der Einführung neuer Technologien abzuklären, ob sich dadurch die Abhängigkeit vom Internet weiter erhöht. Ein Beispiel dafür ist der Einsatz autonomer Fahrzeuge. Bereits jetzt läuft die gemeinsame Vorbereitung aller Akteure im Bereich der Kritischen Infrastruktur intensiv, eine weitere Vertiefung ist sinnvoll und wird von den Betreiber:innen der Infrastrukturen gewünscht.

ECKDATEN

- Projekttitlel:** ISIDOR – Folgen einer langandauernden und großflächigen Einschränkung der Internet-basierten Dienste
- Projektteam:** Krieger-Lamina, J., Konicar, G., Peissl, W. (in einem nat. Konsortium)
- Laufzeit:** 09/2020 – 08/2022
- Auftraggeber:** FFG/KIRAS

WESENTLICHE ERGEBNISSE

Die Versorgung mit Trinkwasser und die Entsorgung des Abwassers wird wohl weiterhin funktionieren. Es ist auch zu erwarten, dass die Stromversorgung bei einem Totalausfall des Internets weiter funktioniert, obwohl dies eine Ausnahmesituation für das Management der Netze wäre. Eventuell zusätzlich auftretende, krisenhafte Ereignisse könnten eventuell nicht ohne weiteres ausgeglichen werden. Große Schwierigkeiten sind dort zu befürchten, wo IT-Prozesse und -Ressourcen im Normalbetrieb ausgelagert sind., etwa bei der Nutzung von Cloud-Diensten oder dem Outsourcing von IT-Personal. Ähnlich verhält es sich mit dezentralen, mobilen IT-Systemen, wie der Patient:innendokumentation im Rettungswesen, die aber zentral gemanagt oder mit Daten versorgt werden.



Credits: Alexandros Giannakis (Unsplash)

Stark betroffen wäre der Banken- und Finanzsektor, viele Geschäftsprozesse sind hier ohne die Möglichkeit zur Datenkommunikation undenkbar.

Ein sektorübergreifendes Problem ergäbe sich aus der Betroffenheit des Transportwesens. Die Daten- und Dokumentationsverarbeitung sowie das Transportmanagement (Sendungsverfolgung, Aviso, Einlagerung, Wiederauffinden, Zustellung etc.) sind in hohem Maße von miteinander vernetzten IT-Systemen abhängig. Dabei verlassen sich viele Organisationen darauf, dass z.T. mehrmals täglich zugestellt wird, um das jeweils dringend Benötigte zu erhalten, ohne ein großes Lager mit differenziertem Bestand führen zu müssen. Durch die zu erwartenden Einschränkungen in der Mobilkommunikation wird die meiste Sicherheitstechnik nicht funktionieren: Alarmanlagen und Brandmelder, die direkt an Polizei oder Feuerwehr melden, oder Alarmierungen von Krisenstäben über Apps oder SMS. Manches kann durch Umstellung auf analoge Prozesse und erhöhten Personaleinsatz ausgeglichen werden, wenn das zuvor geübt wurde und die notwendigen Ressourcen im Krisenfall zur Verfügung stehen.

WAS TUN?

Der Ausfall des Internets oder wichtiger Internet-basierter Dienste für einen langen Zeitraum ist in Österreich noch nicht vorgekommen. Dementsprechend fehlt es an Erfahrungswissen. Folgende Empfehlungen lassen sich aus der ISIDOR-Studie ableiten:

- 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 Betreiber Kritischer Infrastrukturen strategische Überlegungen dazu anstellen, welche Prozesse sich im Ernstfall auch offline erledigen ließen.
- In einigen Bereichen (z.B. Bargeld, Lebensmittellogistik) bedarf es weiterer Arbeit aller Stakeholder:innen, um einer robusten Lösung näher zu kommen.
- Speziell im Gesundheitswesen könnte es notwendig werden, krisenrelevante Versorgungsgüter in größerem Umfang dezentral zu bevorraten.
- Kommunikationswege, die von der für das Internet genutzten Infrastruktur unabhängig sind, sollten bewahrt und ausgebaut werden. Es gibt in Österreich schon einige Netze, die autark funktionieren können (z.B. Helix in Wien; das staatliche Netz der Verwaltung (GovIX); betriebsinterne Netze; Amateurfunk). Statt eines oft geforderten neu errichteten Staatsgrundnetzes, wäre es leichter und günstiger, diese „Inseln“ miteinander zu verbinden.
- Ebenso sollte gewährleistet werden, dass der Austausch mit europäischen Institutionen auch während einer solchen Krise erhalten bleibt.

ZUM WEITERLESEN

Schachenhofer, L., Gronalt, M., Krieger-Lamina, J., Pisecky, H., Konicar, G., Hartwig, L. -H., et al. (2022). ISIDOR – Folgen einer langandauernden und großflächigen Einschränkung der internetbasierten Dienste und Infrastrukturen (Endbericht) (p. 144). Wien. doi.org/10.1553/ITA-pb-2022-02

KONTAKT

Gregor Konicar
E-Mail: tamail@oeaw.ac.at
Telefon: +43 1 51581-6582

