RISIKEN & CHANCEN *der vernetzten Welt*

Die Digitalisierung schreitet voran und damit unsere Abhängigkeit von diesen Technologien wie auch von den dahinterstehenden Unternehmen. Das bringt große Herausforderungen, aber auch Chancen für die lokale Wirtschaft mit sich.

VON PIA MOIK

Egal ob Berufs- oder Privatleben, wir alle sind im Alltag darauf angewiesen, dass die digitale Infrastruktur rund um uns herum funktioniert. Würde diese zusammenbrechen, stünde auch unser Alltag still. Wir sind abhängig von einer reibungslos funktionierenden digitalen Welt und damit auch von Unternehmen, die die Komponenten dieser digitalen Infrastrukturen her- oder bereitstellen. Dazu zählen Anbieter von Hard- oder Software oder Cloudlösungen genauso wie beispielsweise Betreiber von Social Media-Plattformen. Das Gros dieser Unternehmen sitzt außerhalb Europas, vorwiegend in den USA oder den asiatischen Ländern. Genau das ist jedoch auch die Krux an der Sache, denn damit entsteht auch eine Abhängigkeit von diesen Ländern. „Europa hat seine digitale Wirtschaft verloren. Es gibt nichts mehr, das in der EU hergestellt wird", führt Joe Pichlmayr, Geschäftsführer von Ikarus Security Software, aus. Das Wiener Unternehmen agiert global und ist im Softwarebereich etwa auf Antivirus- und Content-Security spezialisiert.

Man habe es verabsäumt, sich mit der zunehmenden Abhängigkeit von außereuropäischen Playern ernsthaft auseinanderzusetzen, die Auswirkungen abzuschätzen und sich Gegenstrategien zu überlegen, bemängelt Pichlmayr. Durch die verschiedenen Krisen der letzten Jahre - allen voran die Corona-Pandemie - folgt nun ein Aufwachen. Denn damit wurde sichtbar, welche Auswirkungen es für die regionale Bevölkerung mit sich bringt, wenn die globalen Versorgungsketten ins Stocken geraten.

Warum diese Firmen praktisch nur mehr außerhalb Europas zu finden sind, führt Pichlmayr auf die besseren Skalierungsmöglichkeiten in großen Staaten zurück: „Diese Unternehmen können in großen Märkten ihre Lösungen viel billiger realisieren als das in kleinen Ländern der Fall ist."

Selektiver Informationsaustausch

Nachteile dieser Abhängigkeit findet man auch abseits solcher Extremsituationen wie Pandemien. Ein heikles Beispiel stammt aus dem IT-Sicherheitsbereich, wie Pichlmayr aus seiner Unternehmenspraxis erzählt: „Wir müssen Wissen aus den USA zukaufen, weil es das in Europa nicht mehr gibt - zum Beispiel über Hacker aus anderen Ländern. Das Wissen darüber ist in Europa nur da, weil wir es aus den USA erhalten." Allerdings geben die US-Firmen ihren Informationsstand nur bedingt weiter. „Infos über Hacker der ‚bösen' Staaten erhalten wir, es fehlt aber das über die der ‚guten'", beschreibt der Sicherheitsexperte. Wissen über Spionagetätigkeiten etwa aus China oder Russ-

land wird also übermittelt, während sich die US-Firmen zu jenen über westliche Staaten bedeckt halten - allen voran über die aus den USA selbst. „Damit fehlt uns wichtiges Wissen und Informationen können verschleiert werden", so Pichlmayr. Aktuell löst sein Unternehmen dies durch das Einbeziehen zusätzlicher Angaben aus weiteren Staaten. Allerdings wären innerhalb der EU erhobene Daten wünschenswert.

Doch um auf EU-Ebene gemeinsam im Sinne der Cybersicherheit und digitalen Souveränität gegenzusteuern, braucht es ein Umdenken, ist Pichlmayr überzeugt: „Europa braucht ein digitales Bewusstsein. Ein Bewusstsein darüber, dass das Leben, das wir kennen, mit dem digitalen verschmilzt. Das ist die Chance zu verstehen, wohin die Richtung geht", so der IT-Security-Spezialist.

Chancen für lokale Betriebe

Auch wenn Europa hier nicht die Nase vorne hat, handelt es sich bei allen IT-Lösungen um ein globales Zusammenspiel. Viel Expertise kommt dabei aus Europa, denn hier liegen auch Chancen, die gerade kleinere Betriebe gut für sich nutzen können. Gerade im Nischenbereich, auf den es sich in der aktuellen Situation zu fokussieren auszahlt. „Es gibt extrem viele Nischen. Die muss man halt finden", so Pichlmayr: „Die Großen skalieren so schnell, dass sie gewisse Dinge gar nicht angreifen. Es mag sich zwar für die Großen nicht mehr rentieren, für kleinere Betriebe lässt sich trotzdem damit gutes Geld verdienen." Außerdem profitieren kleine Betriebe von ihrer Agilität. Denn auch die großen Anbieter brauchen kleine, agile Lösungseinheiten, die flexibel sind und schneller reagieren können.

Weiteres wirtschaftliches Potenzial schlummert in Innovationen wie Technologie-Konvergenzen, also dem Verschmelzen von neuen Verfahren oder Lösungen mit etwas Bestehendem. Ein Beispiel ist die Sensor-Technologie, die in Zusammenarbeit mit KI-Tools tolle Dienste für die Menschen - etwa in der Medizin - leisten kann, wenn man die möglichen Nutzungsbereiche erkennt. „Es gibt hier riesige Anwendungsmöglichkeiten - daraus entstehen neue Märkte und damit neue Möglichkeiten", so der Experte.

© Ikarus Security Software GmbH

„Das Wissen über Hacker ist nur da, weil wir es von den USA erhalten."

Joe Pichlmayr, Geschäftsführer Ikarus Security Software GmbH

Cybersicherheit

Welche große Rolle der Sicherheitsaspekt spielt, zeigt eine aktuelle Studie „Cybersicherheit in Österreich" des Beratungsunternehmens KPMG. Diese stellt erneut das Anwachsen von Cyberkriminalität fest. So hat sich die Anzahl der Deep Fakes österreichweit von 2023 auf 2024 verdoppelt (+ 119 Prozent). In Wien erlebte Social Engineering den größten Zuwachs mit 23 Prozent. Hier wird ein Kontakt zu einer Person im Unternehmen aufgebaut, um diese danach zur Informationsherausgabe zu bewegen, etwa durch das Schüren von Ängsten wie den Verlust des Arbeitsplatzes. Bedroht sind zunehmend Klein- und Mittelunternehmen, die in den seltensten Fällen einen auf IT-Security spezialisierten Mitarbeiter haben. „Cybercrime ist eine ernsthafte Bedrohung für KMU - das Herz des Wirtschaftsstandorts Österreich", betont Martin Heimhilcher, Obmann der Sparte Information und Consulting der WK Wien, und rät: „Wenden Sie sich an den IT-Dienstleister Ihres Vertrauens, damit das Internet nicht zu einem Sicherheitsproblem für Ihr Unternehmen werden kann." Denn im Falle eines solchen Cyberangriffs ist mit Betriebsunterbrechungen zu rechnen. Bei 44 Prozent der Befragten dauerte diese ein bis zwei Wochen, bis der Vorfall komplett aufgearbeitet werden konnte. „Ein derartiger Stillstand kann die Existenz des Unternehmens gefährden", gibt Heimhilcher zu bedenken.

© Florian Wieser

„Cybercrime ist eine ernsthafte Bedrohung für KMU."

Martin Heimhilcher, WK Wien Spartenobmann Information und Consulting

Hilfestellungen seitens der WK Wien gibt es über die Cyberhotline sowie auch über ein Cyberversicherungsprodukt mit besonderen Bedingungen für Mitgliedsbetriebe, in das die Erfahrungswerte der WK Wien eingeflossen sind (siehe Kasten unten).

CYBERSICHERHEIT

WK CYBERSECURITY-HOTLINE

- Täglich rund um die Uhr besetzt: 0800 / 888 133
- Erstinformation und Notfallhilfe im Falle eines Cyberangriffs
- Auf Wunsch erfolgt die Kontaktherstellung zu einem auf IT-Security und Cyberkriminalität spezialisierten Unternehmen vor Ort

CYBERVERSICHERUNG

- Cyberversicherungsprodukt, entwickelt von der WK Wien gemeinsam mit Infinico
- Halbierter Selbstbehalt für Mitglieder der WK Wien
- Drei-Schritte-Sicherheitsplan und weitere Infos: cybersecurity-versicherung.at

MEHR INFOS & SELBSTCHECK

- Prävention & Strategieentwicklung sowie Links zu Förderungen, wichtigen Webseiten und Handbüchern: www.it-safe.at
- Kostenfreies Online-Tool zum Check der IT-Sicherheit für KMU und EPU mit Umsetzungsvorschlägen: ratgeber.wko.at/itsafe