Nachhaltige Cybersecurity?

Die Zivilgesellschaft wird seit einiger Zeit durch Katastrophenszenarien systematisch verunsichert. Die Medien spielen dabei eine prägende Rolle, indem sie Vorkommnisse oder Entwicklungen so lange Wiederkauen bis am Ende der Eindruck eines menschengemachten Untergangs der Zivilisation beschworen wird. Beispiele gibt es viele:

- Die Covid-Pandemie und ihre Folgen für Lieferketten und Arbeitsteilung,
- Die globale Bewertung der Erderwärmung und auf ihrer Grundlage die Klimakrise mit ihren Folgen für die Lebensbedingungen großer Teile der Gesellschaft,
- Die Energiekrise infolge des russischen Angriffs auf die Ukraine und die risikovolle Reaktion des Westens,
- und die fragwürdigen Prämissen für die Wirtschaft – Gewinn erzielen und Abwälzung der Risiken auf die Gesellschaft.

Vor diesen Hintergründen ist zu klären, welche Rolle die IT-Sicherheit in der Rangfolge der Bedrohungsszenarien aktuell spielt und ob die Argumente zu ihrer Bewertung noch die erforderliche Wirkung entfalten können. Durch die allgemeine Digitalisierungseuphorie steigt die Komplexität von IT-Systemen schneller als ihre Transparenz oder systematische Analyse. Die Folge ist eine zunehmende Hysterie bei der Bewertung der IT-Sicherheit, die sich verbal ebenfalls dem Krisenmodus nähert.

Beispiele finden sich im BSI-Lagebericht 2022: „Gefährdungslage im Cyber-Raum hoch wie nie". Wer fühlt sich durch diese Feststellung angesprochen und welche Konsequenzen ergeben sich für die kleinteilige Anbieterlandschaft?

Anschauungsunterricht gab es auf der it-sa 2022 in Nürnberg. Auf dieser Messe waren die Anbieter von IT-Security-Lösungen unter sich. Gefühlt 2/3 der fast 700 Aussteller warben auf Ihren Ständen mit der Losung des BSI-Lageberichts 2022 für ihre Angebote zur Abwendung der aktuellen Gefahren. Die Angebote sind differenziert und jeweils mit Leistungsversprechen verbunden, die nicht exakt nachprüfbar sind, aber die Überwindung von bestimmten Gefährdungen – vermeintlich sicher – garantieren. In den meisten Fällen handelt es sich um Updates zu ‚Standardprodukten', die den Anwendern als Abonnenten angeboten werden. Dieses Geschäftsmodell garantiert einen stabilen Absatz und reduziert das wirtschaftliche Risiko der Anbieter.

Offen bleibt aber, wie und wann die Sicherheitsupdates in die Anwenderlösungen integriert werden, mit welchen Qualifizierungsmaßnahmen die IT-Experten auf neue Qualitäten und Infrastrukturerfordernisse vorbereitet werden und ob nachweislich Gefährdungen der IT-Sicherheit in der Anwendungsumgebung des Anwenders reduziert werden.

Ganz allgemein muss man davon ausgehen, dass bei Updates auch neue Sicherheitslücken und Softwareschwachstellen entstehen, die erst während der Anwendung entdeckt werden und so einen weiteren Update-Zyklus wahrscheinlich machen. Dieser Kreislauf begleitet das Bemühen um sichere und datenschutzgerechte Lösungen seit den Anfängen der Digitalisierung, ohne dass nachhaltige Ergebnisse erreicht werden konnten. Ebenso lange weiß man, dass überzeugende und nachhaltige Leistungen für die IT-Sicherheit nur gemeinsam von Anwendern und Anbietern erreicht werden können.

Mit IoT und der zunehmenden Akzeptanz von Cloud-Diensten hat sich die Komplexität der IT-Landschaft bei vielen Anwendern signifikant verändert, ohne dass die damit verbundenen Gefahren für die IT-Sicherheit hinreichend beachtet werden. Die Folge sind neue – und teilweise erfolgreiche – Angriffsstrategien auf die IT-Systeme in Unternehmen, der Verwaltung und bei kritischen Infrastrukturen. Beispielhaft sei hier auf die zunehmende Bedrohung durch Ransomware verwiesen.

Die im BSI-Lageberichts 2022 beobachtete Ausweitung von Methoden der Erpressung im Cyber-Raum setzt sich weiter fort. Insbesondere das sogenannte Big Game Hunting, also die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer, deren Daten etwa wegen ausbleibender Zahlungen auf Leak-Seiten veröffentlicht wurden, sind weiter gestiegen. Der finanzielle Schaden durch Ransom-Angriffe beläuft sich in diesem Jahr allein in Deutschland bereits auf 24 Mrd. €.

Die Tendenz ist steigend und es bleibt bei den Eindrücken der Hilflosigkeit der Anbieter von Cybersicherheitslösungen und der bisher fehlenden Nachhaltigkeit vieler ihrer Leistungen.

Helmut Reimer