Telekom CR-Wissen

Neue "Emerging Risks"

Für jedes Unternehmen besteht die Notwendigkeit, langfristige Risiken, die in der Zukunft auftreten könnten, vorherzusehen und sich darauf vorzubereiten. Obwohl diese Risiken schwer zu identifizieren sind, können sie einen erheblichen Einfluss haben. Daher ist es notwendig, solche negativen Ereignisse frühzeitig und effektiv zu erkennen, zu bewerten und Strategien zur Risikominderung zu entwickeln, um unser Unternehmen und unsere Kunden vor solchen Risiken zu schützen. Die umfassende Berücksichtigung von sogenannten „Emerging Risks“ der Deutschen Telekom ist Teil unseres Risikomanagementsystems, das relevante Risiken systematisch identifiziert, bewertet und steuert.

Diese „Emerging Risks“ werden in die Kategorien politische, wirtschaftliche, soziale, technologische, ökologische und regulatorische/rechtliche Ereignisse eingeteilt. Als Bewertungsfaktoren werden die Änderungsgeschwindigkeit und Neuartigkeit des Risikos sowie die Relevanz für unsere Branche und unser Geschäft in den kommenden Jahren berücksichtigt.

Die folgenden aufkommenden Risiken sind auf dem Vormarsch:

Technologische Risiken:
Die Cyberkriminalität nimmt drastisch zu. Die digitale Transformation, die zunehmende Verwendung von Geräten (wie Computer oder Smartphones), maschinelles Lernen und andere Anwendungen mit exponentiell steigender Rechenleistung entwickeln sich weiterhin schneller als der aktuelle Sicherheitsschutz. Da die Zahl der möglichen Angriffspunkte in Unternehmen wächst und Cyberkriminalität immer lukrativer wird, wird die Zahl der

Cyberangriffe weiter steigen.

Zu den Risiken gehört, dass Hacker Ransomware einsetzen, die den Zugriff auf Daten und wichtige Systeme blockieren kann (entweder durch das Ausnutzen von Sicherheitslücken in den Netzwerken von Unternehmen oder durch Phishing-E-Mails, um Anmeldedaten abzugreifen und sich Zugang zu verschaffen). KI-gestützte Cyberangriffe werden immer autonomer und selbstverbreitend, da sie die Netzwerkumgebung des Ziels auskundschaften, anstatt sich auf bekannte oder allgemeine Schwachstellen zu verlassen.

Zu den aktuellen Abhilfemaßnahmen gehören die Etablierung einer robusteren IT-Kontrollumgebung, um die Prävention gegen häufigen Angriffe zu erhöhen; der Einsatz von maschinellen Lerntechniken (künstlicher Intelligenz zur Erkennung des Eindringens in Netzwerke und starke, effektive Reaktionsfähigkeiten zur Abwehr erkannter Angriffe; die Verbesserung der Malware-Erkennung und die sichere Benutzerauthentifizierung sowie die Schärfung des Cyber-Bewusstseins, um potenzielle Cyberverletzungen zu reduzieren.

Wirtschaftliche Risiken:
Eine Pandemie lässt sich nicht vorhersagen, aber historische Daten zeigen, dass in den letzten Jahrzehnten regionale und globale Pandemien immer häufiger aufgetreten sind. Eine neue Pandemie kann das Wirtschaftswachstum weltweit drastisch reduzieren und sich auf mehrere Branchen, Lieferketten und die Art und Weise, wie wir leben und arbeiten, auswirken.

Damit verbundene Risiken könnten höhere Zahlungsverzögerungen und Zahlungsausfälle unserer Geschäfts- und Privatkunden sein, die unsere Forderungsausfälle erhöhen. Mögliche öffentliche Beschränkungen würden Geschäfte zur Schließung zwingen und Reisebeschränkungen würden unser Kundenwachstum und das Volumen des Roaming-Verkehrs verringern. Zusätzlich könnten Unternehmen ihre IT-Bestellungen reduzieren. Die Beschränkung sozialer Kontakte und Distanzunterricht könnten die Gesamteffizienz senken oder im Falle einer schweren Pandemie unsere Belegschaft vorübergehend oder sogar dauerhaft reduzieren. All dies könnte wiederum zu einem Umsatzrückgang führen.

Unser Konzernlagezentrum überwacht jegliche Entwicklungen einer eventuell auftretenden Pandemie. Als Teil unseres Krisenmanagements kommuniziert es Pandemierichtlinien und stellt Hygiene- und Sicherheitsausstattungen für alle Geschäfte, Büros und Infrastrukturstandorte bereit, um Kunden und Mitarbeiter zu schützen. Zu den weiteren konzernweiten Maßnahmen zur Eindämmung einer Pandemie gehören das Hochfahren und die Stabilisierung unserer Netzwerke,um sicherzustellen, dass unser Netzwerk zusätzliche Spitzen im Sprach- und Datenverkehr bewältigen kann. Um die Ausbreitung eines möglichen Ausbruchs zu minimieren, können Mitarbeiter von zu Hause arbeiten und unsere Vertriebs- und Serviceteams können umdisponieren, um veränderten Anforderungen gerecht zu werden.

Umweltrisiken:
Naturkatastrophen wie Überschwemmungen, schwere Stürme, Hagel, Hitzewellen, Waldbrände, Wirbelstürme und Erdbeben treten immer häufiger auf. Die physikalischen Auswirkungen unseres sich verändernden Klimas führen zu einer Erwärmung der Ozeane, einer Zunahme von Hitze und Feuchtigkeit und einem Anstieg der durchschnittlichen Temperaturen und Luftfeuchtigkeit. Daher werden sich diese extremen Wetterszenarien in Zukunft wahrscheinlich verstärken.

Wenn mehr Naturkatastrophen auftreten, werden bestimmte Gebiete anfälliger für Überschwemmungen, Stürme oder Hitze und könnte sich die Anzahl der Netzausfälle unserer Netzinfrastruktur (direkte Schäden) erhöhen oder die entsprechende Versorgung mit Strom oder Wasser (indirekte Schäden) beeinträchtigen. Dies wiederum könnte zu Umsatzeinbußen oder geringerer Kundenzufriedenheit führen.

Zu den Maßnahmen zur Reduzierung solcher Netzausfälle gehört die Analyse vergangener und die Vorhersage möglicher zukünftiger Katastrophen, um Schwachstellen in Bereichen zu identifizieren, die anfälliger für stärkere und häufigere Katastrophen sind. Identifizierte Schwachstelle in unseren Netzwerken würde aufgerüstet werden, um die Robustheit gegen solche Katastrophen zu erhöhen. Darüber hinaus gibt es detaillierte Business-Continuity- und Disaster-Recovery-Pläne für den Fall, dass solche Ereignisse eintreten sollten.