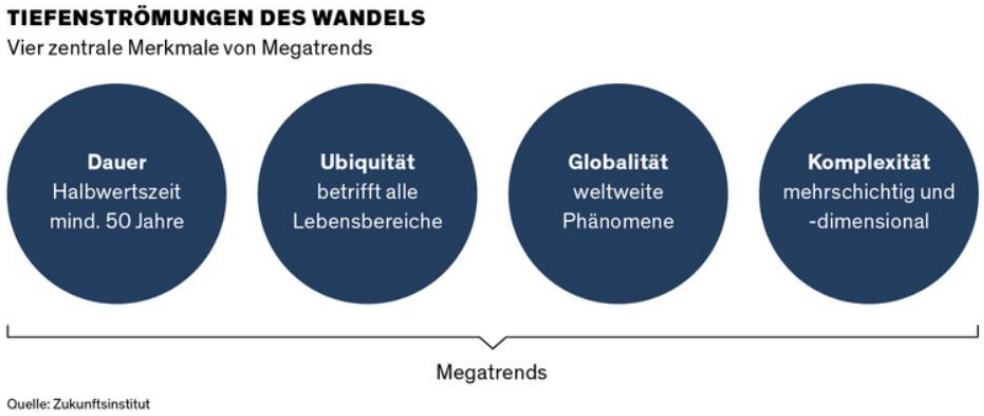
Zukunftstrend Sicherheit – Erkenntnisse für die Aufstellung einer modernen Unternehmenssicherheit

von Franziska Englert
25. Oktober 2022

Wie stellen Sie Ihre Unternehmenssicherheit zukunftssicher auf?
Die Ausrichtung der Unternehmenssicherheit erfolgt grundsätzlich entlang der Unternehmensstrategie. Auf Basis der geplanten Unternehmensentwicklung, die beispielsweise Wachstum und Aktivitäten auf neuen Märkten bedeuten kann, werden mögliche Risikofelder antizipiert.
Dafür ist ein Verständnis der gesellschaftspolitischen und wirtschaftlichen Entwicklungen der Unternehmensumwelt in Gänze erforderlich. Einen wesentlichen Baustein dafür stellen die Megatrends des Zukunftsinstituts dar, sie heben tiefgreifende globale Veränderungen und Subtrends hervor.



Was nicht verwundert ist, dass Sicherheit einer der 12 identifizierten Megatrends ist. Neue Erkenntnisse lassen sich jedoch aus den in diesem Artikel beschriebenen Subtrends ziehen. Dies gilt sowohl für die

Ausrichtung der Unternehmenssicherheit und künftige Sicherheitsmaßnahmen selbst, als auch die begleitenden notwendigen bereichs- und prozessübergreifenden Anpassungen im Unternehmen.

Ausgangslage
Seit 1993 ist die Anzahl der Straftaten (gemäß Polizeilicher Kriminalstatistik PKS) in Deutschland kontinuierlich zurückgegangen. Dem entgegen steht das, in Studien des BKA ermittelte, gestiegene Unsicherheitsgefühl der Bürger.
Das Sicherheitsparadoxon beschreibt die steigende Sensibilität für Risiken und Gefahren durch zunehmend sichere Umfelder.
Daraus resultieren künftig noch weiter steigende Anforderungen an die Sicherheit. Aufgrund gestiegener Erwartungen von Mitarbeitern an Reisesicherheit, durch neue Gesetze, die zum Risiko- und Krisenmanagement verpflichten, und zunehmenden Vorgaben von Geschäftspartnern an die Fortführung von Geschäftsprozessen, sind Unternehmen gezwungen, den Fokus verstärkt auf bestehende Risiken und mögliche Handlungsoptionen zu richten.

Widerstandsfähigkeit liegt im Unternehmensinteresse, um bei aller Volatilität, Unsicherheiten und Ambiguitäten wettbewerbsfähig zu sein und zu bleiben.

Subtrend Digitale Reputation
Die Informationen über ein Unternehmen im Internet und sein Ruf in sozialen Netzwerken bestimmen künftig stärker die Bewertung von Unternehmen und Marken.

1. Vollständigen Überblick verschaffen
   Voraussetzung für die Ermittlung eines realistischen Bildes der eigenen aktuellen Reputation**,** ist ein kontinuierliches, umfassendes Screening aller Medien, insbesondere auch derer in denen sich Ihr Unternehmen selbst nicht präsentiert. Beziehen Sie die Kommunikation der Mitarbeiter im Intranet und die Äußerungen ehemaliger Mitarbeiter, z.B. auf Plattformen wie Kununu, mit ein.

2. Risiken identifizieren
   Die Gefahr einer existenzgefährdenden, sich mitunter schleichend entwickelnden Reputationskrise, nicht als Folge eines Vorfalls, sondern als originäres Ereignis, steigt. Gerüchte, Fake News oder Shitstorms beinhalten das Potential, die Reputation eines Unternehmens nachhaltig zu gefährden. Das gilt beispielsweise auch für veröffentlichte interne Mitteilungen wie Mails von Führungskräften oder Informationsschreiben zu internen Entscheidungen, aber auch für Mitarbeiterpostings mit Unternehmensbezug. Es gilt der Grundsatz: Interne Kommunikation ist automatisch externe Kommunikation. Steuern Sie beide.

3. Interdisziplinäre Zusammenarbeit
   Unternehmenskommunikation, Sicherheitsverantwortliche und Juristen können gemeinsam Maßnahmen festlegen und auf (drohende) Reputationsschäden abgestimmt reagieren.
   Richten Sie zudem eine Schnittstelle zum Beschwerde- und Bedrohungsmanagement, so vorhanden, ein. Die Information, welchen Stand Ihr Unternehmen bei einzelnen Personen(gruppen) hat, kann Ausgangspunkt für Präventions- und Sicherheitsmaßnahmen sein. Im Gegenzug nutzen Erkenntnisse über (Be-)drohungen und laufende Erpressungen oder Kampagnen bei der gezielten Suche nach Gerüchten und Fake News.

4. Prozesse und Dokumente anpassen
   Jede offizielle Kommunikation, unabhängig vom Kanal, muss auf die Übereinstimmung mit anderen Veröffentlichungen und ihre Wirkung auf verschiedene gesellschaftliche Gruppen und Interessensvertreter geprüft werden. Ziel muss es sein, „Fettnäpfchen“ zu erkennen und zu bewerten.

Reaktionen der Öffentlichkeit können so besser kalkuliert und ihnen somit adäquat begegnet werden. Krisenkommunikationspläne müssen so angepasst werden, dass das Unternehmen der medialen Öffentlichkeit bei Notfällen mit gelungener statt misslungener Krisenkommunikation auf allen Kanälen auffällt. Denkbar wäre hier die Vorplanung von virtuellen Pressekonferenzen sowie eigens betriebenen und administrierten Diskussionsplattformen.

Subtrend Resilienz
Die Widerstandsfähigkeit von Unternehmen rückt zunehmend in den Vordergrund und löst damit die Effizienz-Maxime ab.

Resilienz ist die Fähigkeit eines Unternehmens sich negativ auswirkenden Veränderungen so zu begegnen, dass das bisherige Leistungsniveau trotz widriger Umstände gehalten, beziehungsweise schnell wieder erreicht wird.
Es stellen sich aus Sicht der Unternehmens-sicherheit zwei Fragen: Was trägt die Abteilung zur Resilienz des Unternehmens bei und wie kann die eigene Organisation resilient aufgestellt werden?

<u>Der Beitrag der Unternehmenssicherheit zu organisationaler Resilienz</u>
Resilienz-Kultur bezeichnet das Verständnis bezüglich der Notwendigkeit und Möglichkeit mit der eigenen Tätigkeit zur Resilienz des Unternehmens beizutragen.

Mit dieser Haltung lassen sich entsprechende Maßnahmen und Lösungen entwickeln:

- Unternehmenssicherheit in der Hierarchie direkt der Unternehmensleitung zuordnen
- Bei international tätigen Unternehmen: Etablierung geeigneter Länder-Sicherheitsverantwortlicher
- Planung der Sicherheitsstrategie auf Basis der Unternehmensstrategie
- Unternehmensrisiken ganzheitlich und kontinuierlich erfassen
  inkl. Antizipation künftiger Risiken (Analyse und Abgleich künftiger globaler Entwicklungen und Unternehmensziele)
- Interdisziplinäre Zusammenarbeit in- und extern zunehmend auf Projektbasis sowie mit relevanten Schnittstellen im Unternehmen (RM, Compliance, Justiziariat, Unternehmensleitung) und bei Behörden.
- Awareness für Risiken und Sicherheitsmaßnahmen im Unternehmen schaffen
- Krisenbewältigungskompetenzen stärken (Stäbe und Personal trainieren)
- Bearbeitung aller relevanten Unternehmenssicherheitsfelder

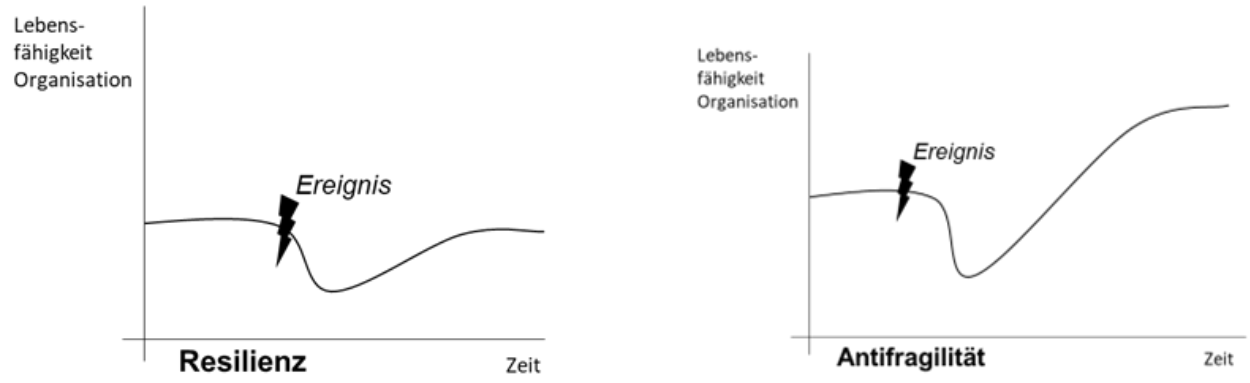
<u>Die resiliente Unternehmenssicherheit</u>
Die Widerstandsfähigkeit der Unternehmenssicherheit bzw. ihrer Leistungen hängt von folgenden Faktoren ab

- Struktur
  - Interne Prozesse (24/7 Bereitschaft, Vertretungsregelungen)

- Personal
  - Recrutingkriterien für Sicherheitsexperten: Erfahrung, Charakter, Talent/Potenzial, Haltung
  - Gezielte Stärkung der Lösungskompetenz
  - Wissensmanagement
  - Einbindung spezialisierter Dienstleister

- Organisation
  - Sicherheitsmaßnahmen zur Vermeidung von Informationsabflüssen (Freistellungen nach Kündigung usw.)
  - Budget

Über Resilienz hinaus geht Antifragilität. Sie lässt sich mit dem Prinzip der Hyperkompensation im Sport vergleichen. Nach einem Trainingsreiz, einer ungewohnt belastenden Herausforderung, passt sich der Organismus nach gewisser Zeit an. Die Leistungsfähigkeit liegt nach der Herausforderung über dem ursprünglichen Niveau. Dieser Mechanismus sorgt dafür künftige Belastungen und Herausforderungen dieser und höherer Intensität besser bewältigen zu können. In Unternehmen resultiert die entsprechende Performancesteigerung, beispielsweise nach einer Krise, auf der Identifikation und Nutzung bisher nicht wahrgenommener Chancen, noch während der Bewältigung der aktuellen Herausforderung. Wer die neuen Anforderungen von Arbeitnehmern flexibel zu arbeiten während der Corona-Krise nicht nur früh erkannt sondern auch proaktiv ermöglicht und beworben hatte, konnte nicht nur eigene Talente halten, sondern zusätzlich Talente der Mitbewerber für sich gewinnen. So zu handeln verschafft einen Wettbewerbsvorteil.



Quelle: Corsecon

Subtrend Cybercrime
Der Begriff bezeichnet die Art von Kriminalität, die mithilfe von Informations- und Kommunikationstechnik (IKT) verübt wird. Unter Cybercrime fallen Verbrechensarten wie digitale Industriespionage, Identitätsmissbrauch, Diebstahl geistigen Eigentums oder digitale Fälschung.

Für die erforderliche Prävention im Vorfeld und das Notfallmanagement im Fall eines Cyberangriffs, ist die Zusammenarbeit der Bereiche Informationstechnik (IT), Informationssicherheit und Unternehmenssicherheit erforderlich. Heute besitzt jedes Unternehmen neben physischen Werten wie Liegenschaften und Prototypen, die geschützt werden müssen, auch eine große „digitale (Angriffs-)Fläche“. Hier sind ebenso Zugangsbeschränkungen und –kontrollen durchzuführen und eine „virtuelle“ Hausordnung für Mitnutzer des eigenen Netzwerks sowie Schnittstellenpartner festzulegen.
Wirksamer Schutz eines Unternehmens beginnt heute mit der Erkenntnis, dass Unternehmen mit vielen Daten und Informationen heute an zwei „Standorten“, in der realen Welt und virtuell, präsent sind. Daraus folgt, dass in beiden Fällen in Technik, Prozessorganisation und personelle Maßnahmen zum Schutz investiert werden muss.

1. Integration IT-Sicherheit
   Bei den heutigen Anforderungen an die Sicherheit des Unternehmens, die „Standorte“ in der realen und virtuellen Welt und den zahlreichen Risiken, lassen sich die bisher zur Unternehmenssicherheit gehörenden Bereiche und die IT-Sicherheit nicht mehr länger trennen.
   Eine konsequente Integration der IT-Sicherheit und Informationssicherheit in die Unternehmenssicherheitsstruktur ist anzustreben.
   Die wesentlichen Vorteile sind: Zentrale Steuerung und Planung der Sicherheit eines Unternehmens, Zusammenführen der Expertise und Erkenntnisse der einzelnen Disziplinen für bessere und schnellere Maßnahmen im Bereich Risikoanalyse, Prävention und Notfallmanagement, Vermeidung von Sicherheitslücken an Schnittstellen zwischen IT- und Unternehmenssicherheit, Kostenreduktion durch Nutzung von Synergien und Vermeidung von Doppelarbeit.

Gemeinsam mit dem IT-Verantwortlichen (CISO) sollte eine gemeinsame Organisation des Zuständigkeitsbereichs vorgenommen werden.

2. Härtung der (Sicherheits-)systeme
   Für sensible Unternehmensbereiche und kritische Infrastruktur kann die Installation von Sicherheitstechnik wie beispielsweise Videoüberwachungssysteme als geschlossenes System sinnvoll sein. Es wird auch von Härtung der Systeme gesprochen. Hierfür werden unter anderem systemeigene Datenleitungen (Glasfaserkabel) verlegt und Schnittstellen z.B. für Fernwartung vermieden.
   Wartung oder das Einspielen von Softwareupdates vor Ort sind weiterhin Angriffsvektoren, die bedacht werden müssen.

Cybercrime im engeren Sinne sind Taten, die mithilfe von Informations- und Kommunikationstechnologie (IKT) auf IKT verübt werden. Im weiteren Sinn werden darunter auch andere Straftaten, die mithilfe von IKT und entsprechenden Komponenten wie Malware (Schadsoftware) begangen werden, verstanden.

Ein detaillierter Blick auf aktuelle Erkenntnisse, Regelungen, zukünftige Entwicklungen und deren Bedeutung für die Arbeit der Unternehmenssicherheit lohnt sich.

Sicherheitslücke Technik

Durch die zunehmende Digitalisierung existieren neue Angriffsvektoren. Über mehr Schnittstellen (Industrie 4.0 – Smart Factory), den vermehrten Einsatz von Software (digitale Lieferketten) und mehr Geräte sowie Anlagen, die durch Internetanbindung Bestandteil eines Netzwerkes sind (Internet of Things-IoT), können bei Angriffen Daten abgegriffen und Vorgänge manipuliert werden.
Aufgrund der Netzwerkstrukturen und Schnittstellen zu weiteren Systemen ist es Tätern, die unter Ausnutzung einer Schwachstelle in ein System eindringen, möglich, auf weitere Daten im Netzwerk zuzugreifen, die nicht ausreichend gesichert sind. Erfolgt der ursprüngliche Angriff auf ein Lieferantensystem, kann dies bspw. unmittelbare die Zugriffsmöglichkeit der Täter auf, durch das eigene Unternehmen verwaltete, Daten bedeuten.

Sicherheitslücke Mensch

Phishing und Social Engineering zählten 2021 zu den häufigsten Angriffsformen (Quelle Bitkom).
Bei Phishing wird vorrangig versucht an Passwörter zu gelangen, beispielsweise indem u.a. per Mail zum Anklicken eines Links und der Eingabe von Daten aufgefordert wird.
Mit Social Engineering versuchen Täter, mithilfe von Identitätsmissbrauch und Verschleierung des eigenen Vorhabens, an vertrauliche Informationen zu gelangen und Handlungen oder Abläufe zu ihren Gunsten manipulieren. CEO-Fraud, die Anweisung von Zahlungen auf Konten durch vermeintliche

Vorgesetzte, mithilfe von Anrufen oder Mails, gilt als Teilphänomen. Riefen Täter bisher selbst an und gaben vor für diese Anweisungen legitimiert zu sein, warnt das BSI heute bereits vor Deepfakes, z.B. manipulierten Videoanrufen, bei denen sowohl der Vorgesetzte sichtbar wird (aus Fotos generiertes Bewegtbild) als auch die tatsächliche Stimme eines Kollegen zu hören ist (mittels Stimmgenerierung –Voice-Cloning).

Ausblick: Künftige Gefahren

Mit Zunahme der Qualität und Verfügbarkeit von Künstlicher Intelligenz (KI), wird diese künftig für automatisierte Angriffe im IKT-Umfeld genutzt. Für Täter sinkt die Zugangsschwelle zu wirksamer Schadsoftware weiter und die Frequenz von Angriffen steigt. Selbstlernende Systeme sind schwerer abzuwehren, weswegen künftig auch Schutzsysteme KI nutzen werden.

CaaS (Cybercrime as a Service) wird vom TüV als Cybersecurity-Trend 2022 aufgeführt. Im Internet können einzelne Leistungen, die für einen Cyberangriff notwendig sind als Service gebucht werden. Die Komponenten werden von voneinander unabhängigen Akteuren bereitgestellt. Der Einzelne hat keine

Kenntnis vom oder direkten Einfluss auf den geplanten Angriff, was das Risiko für alle kriminellen Beteiligen verringert, die Verhandlungen mit Tätern sowie etwaige Strafverfolgung erschwert.

Aktuelle und weiterführende Informationen zu den Schlagwörtern des Megatrends Sicherheit finden Sie unter https://www.zukunftsinstitut.de/artikel/megatrend-glossar/sicherheit-glossar/

Quelle für Trends: Zukunftsinstitut

Weitere Fachartikel unserer Experten erhalten Sie mit unserem Sicherheitsbriefing.