Neue KomplexitÃ¤t: Die Evolution der Sicherheitsfunktionen

Ein Gedankenimpuls der Konzern Sicherheit & Resilienz der Volkswagen AG.

Die Welt hat sich in den letzten Jahren grundlegend verÃ¤ndert. Viele Themen, die heute Teil der tÃ¤glichen Lage- und Berichterstattung sind, waren vor einigen Jahren noch nahezu undenkbar und kamen bestenfalls in vagen Prognosen vor. Der russische Angriffskrieg auf die Ukraine und die terroristischen Angriffe der Hamas auf Israel markieren eine neue Dimension der politischen Machtentfaltung. Wir erleben einen spÃ¼rbaren geo- und sicherheitspolitischen Wandel und mÃ¼ssen weiteres Konfliktpotenzial erwarten.

Neben militÃ¤rischen Auseinandersetzungen gewinnt die hybride KriegsfÃ¼hrung an Bedeutung. Was frÃ¼her als Propaganda bezeichnet wurde, hat heute neue Dimensionen erreicht und ist Teil komplexer, oft insbesondere durch kÃ¼nstliche Intelligenz gesteuerte Desinformationskampagnen, die etablierte Strukturen und Demokratien destabilisieren sollen. Neue Formen der gezielten Falschinformation und Manipulation der Ã¶ffentlichen Meinung spielen hierbei eine wesentliche Rolle.

Gleichzeitig entfernt sich die Gesellschaft zunehmend von einer gemÃ¤Ã?igten politischen Mitte und driftet zu extremen politischen RÃ¤ndern ab. Die Gewaltbereitschaft in Teilen der BevÃ¶lkerung hat messbar zugenommen, und die Zahl der Delikte steigt kontinuierlich. Besonders im Internet ist ein dramatischer Anstieg von Hass und Hetze zu verzeichnen. Den Worten folgen immer Ã¶fter auch Taten und auch legitimer Protest eskaliert heute nicht selten.

WomÃ¶glich steht gegenwÃ¤rtig nicht weniger als die Demokratie und die globale Weltordnung auf dem Spiel.

Neue Bedeutung der Sicherheit
Ã?ber die GrÃ¼nde all dessen wird auf sozialwissenschaftlicher Seite, in den Medien und der Politik sowie bei vielen weiteren Akteuren geforscht. Gleichzeitig kommt in der Konfrontation mit diesen Themen und der globalen Lage den Handlungsfeldern der Sicherheit neue Bedeutung zu. Deutschland hat 2023 erstmals in der Geschichte der Bundesrepublik eine Sicherheitsstrategie entwickelt, die das Thema Sicherheit ganzheitlich betrachtet und neben vielen anderen Aspekten auch das Zusammenspiel der verschiedenen staatlichen und nicht-staatlichen Akteure im Kontext der Sicherheit fokussiert. Ã?ffentliche Sicherheit entsteht bisher und auch weiterhin im filigranen und geÃ¼bten Zusammenspiel von Polizei, Justiz, Nachrichtendiensten, Verwaltung, Gesundheitswesen, Ersthelfern und nicht zuletzt durch politischen sowie gesellschaftlichen RÃ¼ckhalt.

Wirtschaft + Sicherheit = Wirtschaftsschutz
Sicherheit in der Gesellschaft wird heute zunehmend durch privatwirtschaftliche Sicherheitsinteressen ergÃ¤nzt. Den BehÃ¶rden ist es heute alleine schon aus KapazitÃ¤tsgrÃ¼nden nicht mÃ¶glich, sich Ã¼ber â??den BÃ¼rgerâ?? hinaus in angemessenem Umfang zusÃ¤tzlich um die Sicherheitsinteressen von Unternehmen zu kÃ¼mmern. Zu komplex, zu individuell und zu ressourcenhungrig sind die Bedarfe, die beispielsweise bei den sogenannten â??Global Playernâ?? konkret vorliegen. Auch der Mittelstand taucht zunehmend tiefer in die speziellen Aufgabenfelder der Sicherheit ein.

FÃ¼r die Konzern Sicherheit & Resilienz der Volkswagen AG und die zu unserem Konzernverbund gehÃ¶renden Marken, Gesellschaften und Regionen sind insbesondere folgende Einflussfaktoren maÃ?geblich:

- Geopolitische Risiken
  Zwischenstaatliche Konflikte, Kriege, handelspolitische Spannungen beeinflussen Standorte, firmenspezifische Lieferketten und Mitarbeitersicherheit weltweit.
- Gesellschaftlicher Wandel & Gewaltzunahme
  Polarisierung, sinkendes Vertrauen in Institutionen und mehr Gewalt im Ã¶ffentlichen Raum erhÃ¶hen das Risiko fÃ¼r Mitarbeitende und Standorte.
- KriminalitÃ¤t (physisch & digital)
  Erfordert flexible und dynamische Schutzkonzepte, die sich schnell an neue Bedrohungen anpassen lassen.
- Digitale Risiken im physischen Raum
  Die Grenze zwischen digitaler und physischer Welt verschwimmt â?? Sicherheitskonzepte mÃ¼ssen beide Dimensionen integrieren.
- Produktbezogene Sicherheit
  Schutz von Fahrzeugen, Software und Daten wird zur Kernaufgabe

Zielkonflikte der Sicherheit
Betriebswirtschaftlich geprÃ¤gt ist das Handeln auf vielen Ebenen von der Frage nach â??Aufwand-Nutzenâ?? â?? mit dem Ziel, Aufwand zu minimieren und aus diesem Handeln den grÃ¶Ã?tmÃ¶glichen Nutzen zu ziehen. Das klassische Aufwand-Nutzen-VerhÃ¤ltnis hat sich in der Sicherheit allerdings Ã¼ber die Jahre um eine vom Kunden gewÃ¼nschten Dimension erweitert: die Frage nach dem Komfort einer LÃ¶sung. Dies umfasst dabei auch zusammenhÃ¤ngende Aspekte wie Nutzerakzeptanz und SimplizitÃ¤t einer LÃ¶sung. Gleichzeitig wurde der Begriff des â??Nutzensâ?? Ã¼berfÃ¼hrt in den prÃ¤ziseren Begriff â??Sicherheitâ??, soll heiÃ?en den Grad an Sicherheit, den man erreichen will. Damit ist ein Zielkonflikt in nunmehr drei Dimensionen entstanden: Kosten â?? Komfort â?? Sicherheit, da hohe Sicherheit mit Komfort teuer ist, wÃ¤hrend gÃ¼nstige LÃ¶sungen oft an Sicherheit und Akzeptanz verlieren.

Da Kosten messbar, Sicherheit aber schwer definierbar ist, kann â??notwendige Sicherheitâ?? von Minimalanforderung bis hin zu â??was ist faktisch notwendigâ?? reichen. ZusÃ¤tzliche Attribute wie â??lageangepasste Sicherheitâ?? oder â??erforderliche Sicherheitâ?? bringen hier ebenfalls keinen argumentativen Mehrwert. Alle potentiellen SicherheitslÃ¶sungen sind daher immer ein Kompromiss. SicherheitslÃ¶sungen umfassen aber zwei Komponenten: objektive Sicherheit und subjektive Sicherheit. Im sprachlichen Alltag wird fast ausnahmslos auf den Aspekt des Subjektiven abgezielt. Damit liegt der Begriff der Sicherheit in seiner Varianz mit dem rein von subjektiven Elementen getragenen Begriff des Komforts im Wesentlichen auf AugenhÃ¶he.

Es gilt also zuvorderst den Mehrwert von SicherheitsmaÃ?nahmen auszudrÃ¼cken, was nur dann gelingen kann, wenn deutlich wird, wie Sicherheit einen (potenziellen) Schaden bspw. verhindert, abwendet, minimiert, aufdeckt, verzÃ¶gert oder in irgendeiner Form akzeptabel macht.

Man kann nur schÃ¼tzen, was auch geschÃ¼tzt werden will
Der Grad des Schutzes eines Unternehmens (und damit die effektive Wirkung der Sicherheit) wird von dessen Willen und FÃ¤higkeit zur Resilienz bestimmt. Allzu oft gilt allerdings: â??Sicherheit ist stets zu viel bis zu dem Augenblick, wo sie fehlt.â??

Der Sicherheitsfunktion eines Unternehmens kommt hier eine wesentliche Rolle zu, in dem sie Risiken und Bedrohungen determiniert und im Dialog mit GeschÃ¤ftsverantwortlichen festlegt. Auch wenn Sicherheitsverantwortliche in aller Regel die Governance-Verantwortung tragen, so sind die Sicherheitsfunktionen auch heute noch leider viel zu selten in die alltÃ¤glichen AblÃ¤ufe der unternehmerischen Prozesse integriert. Hier tun sich fÃ¼r die Zukunft noch viele Chancen im Sinne eines Wertbeitrags auf, die Sicherheitsverantwortliche und Sicherheitsfunktionen leisten kÃ¶nnen, ja sogar mÃ¼ssen. Hierzu bedarf es weniger einer Governance- sondern vielmehr einer Steuerungshoheit, die verstÃ¤ndlich, nachvollziehbar und praxistauglich ist, anstellt antiquierter â??Du darfstâ?? und â??Das darfst Du nichtâ?? Regelwerke.

Erweiterung des Sicherheitsdreiecks
Das bisher beschriebene klassische Sicherheitsdreieck ist heute aber lÃ¤ngst durch ein Vieleck abgelÃ¶st, das die KomplexitÃ¤t des Handelns und der Verantwortung weiter erhÃ¶ht. Neben Kosten, Komfort und Sicherheit spielen heute u.a. gesetzliche Vorschriften und Regularien, (geo-)politische und kulturelle EinflÃ¼sse, Digitalisierung, Risikobewusstsein und Versicherbarkeit, Medienwirkung, Reputation sowie gesellschaftliche Faktoren und letztlich Kaskadeneffekte eine Rolle.

Gelebte Sicherheitsverantwortung = Resilienz
Die Grenzen zwischen Business Continuity Management und strategischer Krisenvorsorge verschwimmen, da keine dieser

beiden Komponenten fÃ¼r sich alleine eine sinnvolle Wirkung entfalten kann. Zudem geht es in der Sicherheitsverantwortung nicht nur um Vorsorge, sondern etwaig auch um MaÃ?nahmen im Schadensfall. Umso mehr wird deutlich, dass ein Sicherheitsdreieck mittelfristig ausgedient hat, da es die gegenwÃ¤rtige KomplexitÃ¤t der Entscheidungsparameter nicht hinreichend abbildet.

Daher ist festzuhalten, dass Sicherheitsfunktionen nach einem Dauerkrisenmodus in den Jahren 2020 bis 2023 erneut vor neuen und ungleich komplexeren Herausforderungen stehen. Es bedarf neuer Konzepte, mit denen Sicherheitsfunktionen ihren Wertbeitrag zum Unternehmenserfolg vermitteln und diesen letztlich auch messbar machen; was im prÃ¤ventiven Bereich oft nur bedingt gelingt. Repressives Handeln hingegen wird in der Regel Ã¼ber HÃ¤ufigkeitszahlen in einzelnen Deliktfeldern und PhÃ¤nomenbereichen abgebildet. Diese greifen im betrieblichen Kontext allerdings nicht selten zu kurz, da sie nur Teilaspekte abbilden und durch externe Faktoren wie auch Dunkelfelder verzerrt werden.

Fazit
Der Begriff der betrieblichen Sicherheit muss daher mittelfristig konsequent weitergedacht werden. Einerseits bleibt Sicherheit ein unverhandelbares menschliches GrundbedÃ¼rfnis, andererseits muss Sicherheit als Funktion operativ flexibel und angemessen reagieren kÃ¶nnen. Dazu gehÃ¶rt auch eine valide Sensorik und das Antizipieren von Kaskadeneffekten und kÃ¼nftiger Sicherheitsrisiken. Gleichzeitig scheint es nÃ¶tig, dass Sicherheit in sich auch digitaler und vernetzter werden muss. Risiken im digitalen Raum haben immer einen Bezug zur realen Welt und vor allem auch digitale KriminalitÃ¤t hat immer einen Bezug zur realen Welt. Damit verschieben sich in einem Sicherheitsvieleck die Perimeter der Sicherheitsverantwortung.

Gleichzeitig ist die Prognose erlaubt, dass es auch absehbar und auf ansteigendem Niveau alle Formen von (schwerer) KriminalitÃ¤t geben wird. Krisenhafte Ereignisse und ihre Kaskadeneffekte beeinflussen zudem die sozialgesellschaftlichen AblÃ¤ufe in nicht unerheblichem MaÃ?e. Daher heiÃ?t es: in der Sicherheit weiterhin vernetzt denken und handeln, um der Gefahrengemeinschaft proaktiv zu begegnen. Kurzum: Sicherheit neu denken. Um genau diesem Anspruch gerecht zu werden, setzt die Volkswagen AG auf Elemente wie modernisierte Security Intelligence, messbare WertschÃ¶pfung, proaktive KritikalitÃ¤tsbemessung oder andere prÃ¤ventiv wirkende MaÃ?nahmen in der physischen oder digitalen Supply Chain des Konzerns.

Als â??Konzern Sicherheit & Resilienzâ?? der Volkswagen AG vereinen wir mit unseren Marken, Regionen und Gesellschaften ein zukunftsorientiertes, sich von Innen heraus modernisierendes und global vernetztes Team, das im Sinne der obigen ErlÃ¤uterungen und auf Basis unserer Sicherheitsstrategie als â??ONE.securityâ?? handelt. Wir haben aktuell eine detaillierte Analyse unseres kompletten Leistungsportfolios durchgefÃ¼hrt, die sich Ã¼ber sieben Handlungsfelder der Sicherheit, ca. 30 Kernprozesse und weit Ã¼ber 100 wesentliche Aufgaben / TÃ¤tigkeiten erstreckt. Diese Portfolio-Analyse wird unter BerÃ¼cksichtigung der Elemente des â??Security-Vieleckâ?? sowie der externen Einflussfaktoren im weiteren das Target Operating Modell sowie die Datenverarbeitungserfordernisse der Konzern Sicherheit & Resilienz beeinflussen.

Quellenangaben
Titelbild von Kaspars Grinvalds â?? stock.adobe.com (generiert mit KI)
Autoren:
Andreas Maack und Theresa HÃ¤rtl

Autor

Andreas Maack fuÌ?hrt seit September 2021 die Konzern Sicherheit der Volkswagen AG. In dieser Funktion vereinen sich Sicherheitsverantwortung sowie strategische und operative Steuerungshoheit der Risikofruì?herkennung, des Krisenmanagements und der Gefahrenabwehr in einem komplexen Gefuì?ge physischer und digitaler Angriffsvektoren, denen der Konzern und seine BeschÃ¤ftigten im Rahmen der WertschÃ¶pfung jeden Tag aufs Neue ausgesetzt sind.

Autorin

Theresa HÃ¤rtl
PersÃ¶nliche Referentin Andreas Maack, Konzern Sicherheit & Resilienz
Seit 2020: Volkswagen Group
2020-2023 Konzern Produktion im Fachbereich Digitale Innovationen
2023-heute: Konzern Sicherheit & Resilienz