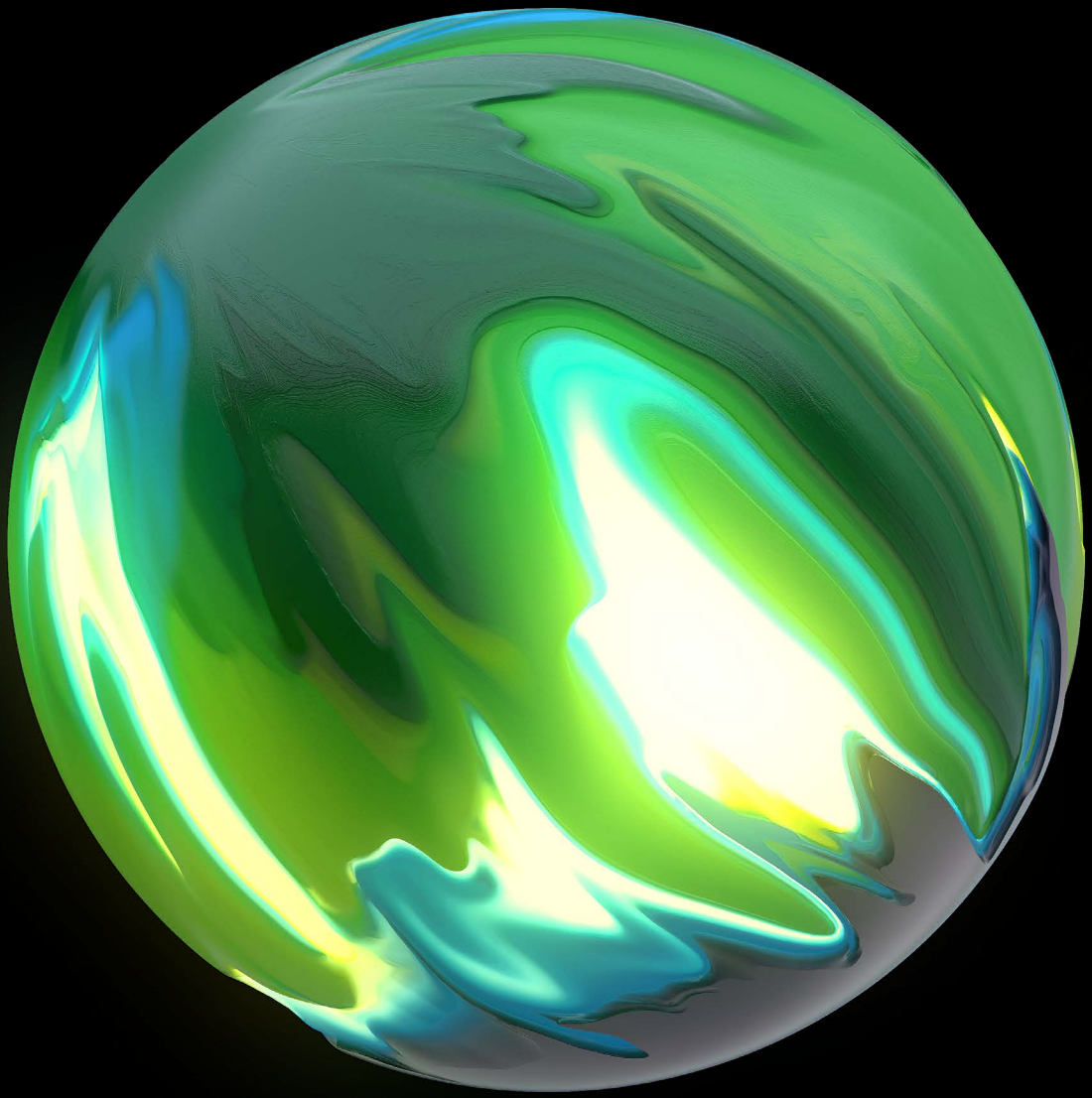
Deloitte.



Cybersecurity

Die Königsdisziplin für agile Organisationen und kybernetische Governance

MAKING AN IMPACT THAT MATTERS since 1845


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
if _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
rror_ob.select= 1
difier_ob.select=1
y.context.scene.objects.active = modifier_ob
int("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0

Vorwort

Fortschreitende Digitalisierung, weltweite Nutzung von Cloud-Lösungen, Web3 oder 5G-Telekommunikation: All diese Technologien eröffnen Menschen, Unternehmen und Gesellschaften immer umfassendere und vielfältigere Möglichkeiten der Kooperation, Interaktion und Kommunikation. Zugleich stellen sie für Cybersecurity-Experten in Unternehmen eine völlig neue Dimension der Komplexität potenzieller Risiken dar. Technologische Aspekte und das relevante IT-Wissen, das für die Bewältigung dieser Komplexität notwendig ist, werden in vielzähligen Publikationen und Fachkongressen intensiv diskutiert.

Die hier vorliegende Zusammenstellung von Fachartikeln konzentriert sich auf jene Aspekte der Cybersecurity, die im aktuellen Diskurs gern übersehen werden. Die Autoren widmen sich der Fragestellung, wie Unternehmen den Umgang mit Cyberrisiken organisatorisch, managementseitig und individuell behandeln sollten.

Wie strukturieren CISOs mit ihren Experten die Teams? Wie sollen Kommunikation und Kooperation gestaltet werden, um ein möglichst reibungsloses Zusammenspiel aller Beteiligten und Betroffenen in der Bekämpfung und der Prävention von Cyberattacken sicherzustellen? Worauf müssen Manager achten? Welches Vorgehen begünstigt, die Experten der CISO-Teams mit der gesamten Organisation in einen produktiven Dialog und eine konstruktive Kooperation zur Cyberdefense zu bringen? Was bedeutet die Auseinandersetzung mit Cybersecurity aus individueller Sicht?

Aus einem Gespräch zwischen Dr. Ralf Schneider (Allianz SE) und Andreas Slogar (Deloitte) für eine Folge des Deloitte-Podcasts „Sprint! New Work – New Mindset" ist die Idee entstanden, diese Perspektiven auf Cybersecurity zu beleuchten und mit einer Reihe namhafter Experten zu vertiefen. Im Zentrum dieser Überlegungen steht die Kybernetik: die Wissenschaft, die Kunst bzw. das Handwerk der Steuerung – und verallgemeinert der Steuerung, Regelung und Lenkung – durch Kommunikation, wie Prof. Dr. Fredmund Malik sie in seinem Beitrag definiert.

Diese Wissenschaft umfasst eine Vielzahl an Modellen, Werkzeugen und Erkenntnissen, die sich in Unternehmen – also hochkomplexen Systemen – immer mehr durchsetzen und es mit ihren Potenzialen ermöglicht, die Chancen und Risiken der eingangs genannten technologischen Entwicklungen zu nutzen und zu bewältigen, anstatt durch Überforderung zu scheitern. Aus dieser Perspektive betrachten die Co-Autoren in ihren Beiträgen die Rolle des Managements in Organisationen. Sie untersuchen die Strukturen der Kooperation in Unternehmen und die Auswirkungen auf die individuelle Perspektive der Mitarbeitenden im Kontext von Cybersecurity und Kybernetik.

Den Auftakt zu den nachfolgenden Überlegungen macht Dr. Karsten Nohl (Autobahn Security GmbH) mit einem Einblick in die aktuelle Situation der Cybersecurity. Er beschreibt die Dynamik des Wettlaufs zwischen Hackern, die Unternehmen attackieren, und den Cybersecurity-Teams, die diese abwehren und Firmen vor Cyberrisiken schützen.

Darauf aufbauend findet sich das Transkript des vorgenannten Podcast-Gesprächs. Ralf Schneider beschreibt aus der weltweiten IT-Praxis der Allianz SE, wie deren Experten, CIOs, CISOs und er vorgegangen sind, um Cybersecurity mit den Möglichkeiten der Kybernetik völlig neu, partizipativ und dezentral zu denken und durchzuführen.

Prof. Dr. Fredmund Malik (Malik International AG) gibt in seinem Beitrag einen fokussierten Einblick in die Kybernetik, die Entwicklung dieser interdisziplinären Wissenschaft und welche Bedeutung ihr vor allem in unserem Jahrhundert der Vernetzung zukommt.

Im vierten Kapitel untersucht Andreas Slogar die Perspektive der Organisations- und Kooperationsstruktur von CISO-Teams und erörtert jene Elemente der Kybernetik, die es Cybersecurity-Experten und den mit ihnen kooperierenden Organisationsbereichen eines Unternehmens ermöglichen, Echtzeitereignissen konstruktiv und proaktiv zu begegnen.

Abschließend legt Yip Thy-Diep Ta den Fokus auf die individuellen Aspekte des Themengebiets und die elementare Rolle der Antifragilität und Achtsamkeit im Kontext der Kybernetik für jeden Mitarbeitenden. Zusätzlich entwickelt Yip Thy-Diep Ta (Unit Network) einen Perspektivwechsel aus der gegenwärtigen Handlungsnotwendigkeit hin zu künftigen Entwicklungen, die aus der Evolution von Web3 und der Token-Ökonomie zu erwarten sind.

Wir von Deloitte möchten als Herausgeber besonders den Autoren danken und hoffen, dass Sie, unsere geschätzten Leserinnen und Leser, aus den nachfolgenden Überlegungen, Erfahrungen und Erkenntnissen nützliche Impulse für sich und Ihre Kollegen gewinnen und so Ihre eigene Arbeit als CIO, CISO oder Cybersecurity-Experte weiterentwickeln sowie gewohnte Pfade überdenken können.

Schutz vor Hacking – ein ewiger Wettlauf im Unternehmen?

Dr. Karsten Nohl | Autobahn Security GmbH

Dr. Karsten Nohl ist Hacking-Experte und Gründer von Autobahn Security in Berlin. Karsten schafft Bewusstsein für Cybersicherheit – durch Hacking-Forschung und -Beratung. Dabei fasziniert ihn besonders der Zielkonflikt zwischen Security und Innovation.

Das Thema Hacking ist ein Garant für spannende Hollywood-Filme. In der echten Welt kommen wir bei der entsprechenden Prävention jedoch kaum voran. Beides aus dem gleichen Grund: Das Vorgehen von Hackern scheint mysteriös, weil die meisten so wenig dazu wissen. Die Gefühle schwanken zwischen Nervenkitzel für die einen und ständiger Furcht für die anderen, das nächste Opfer zu werden.

Letztere schlägt in Firmen oft in Lethargie um: „Die Hacker gewinnen eh immer." Diese Einstellung könnte von den Tatsachen nicht weiter entfernt sein: Firmen verzeichnen jeden Tag Hacking-Versuche und dennoch werden fast alle Firmen an fast allen Tagen nicht gehackt.

Um mit Cyberrisiken souveräner umzugehen, müssen Tatsachen die Strategie bestimmen. Diese Abkehr von irrationalen Ängsten ist in anderen Risikobereichen bereits gelungen, zum Beispiel beim Wettlauf mit biologischen Viren. Obwohl die Forschung biologische Organismen nur im Ansatz versteht, wurde das Risiko vieler Krankheiten durch Diagnostik, Immunisierung und Behandlung erfolgreich verringert.

Technische Systeme und Organisationen sind hoch komplex, aber längst nicht so komplex wie biologische Organismen. Wer eine Chance sieht, das Risiko von Krankheiten aktiv zu beeinflussen, kann beim Thema Cyberabwehr nicht das Handtuch werfen. Der erste Schritt auf diesem Weg: Durch ständiges Messen und dezentral organisierte Verbesserung – also durch Kybernetik – können wir Hacking entmystifizieren und den nötigen Schutz aufbauen.

Hacking ist von Mythen umrankt, weil wir zwar viel darüber reden, selten aber mit den Verursachern. Der wichtigste Schritt zur Aufklärung: Hacker in ihrem Vorgehen verstehen. Große Firmen machen das regelmäßig, indem sie Sicherheitsexperten zu Angriffssimulationen einladen. Diese laufen ähnlich ab wie Militärmanöver in Friedenszeiten: Ein Teil der eigenen Truppe spielt den Feind, um Schwächen in der Verteidigung zu finden. Auch die Bezeichnung der Hacking-Manöver, „Red-Teaming", stammt aus dem Militärischen – sinnbildlich haben die Feinde rote Uniformen an.

Im ersten Schritt erlangen die Red-Teamer Kontrolle über einen Firmencomputer. Das geschieht zum Beispiel über E-Mail-Viren oder Schwachstellen in Webseiten. Das initiale Einfallstor ist in den meisten Fällen kein kritisches System, ermöglicht aber das Ausspionieren des Firmennetzes. Im zweiten Schritt nutzen die Red-Teamer Schwachstellen aus, die sie in internen Applikationen und Servern finden, um ihre Zugriffsmöglichkeiten über Wochen sukzessiv auszubauen. Die Hacking-Reise vom Einfallstor bis zur kompletten Kontrolle der Unternehmens-IT dauert in den meisten Fällen weniger als einen Monat.

Red-Teaming ersetzt den Nervenkitzel durch schnöde Fakten: Wie gehen Hacker vor, um in unsere Systeme einzudringen?

Jede Red-Team-Übung legt das schwächste Glied der Schutzkette offen und zeigt auf, was nötig ist, um echte Hacker vom Durchbruch abzuhalten. Red-Teaming ist dabei nur ein Beispiel, wie Firmen Hacker verstehen können. Ähnliche Einblicke geben Retrospektiven auf echte Sicherheitsvorfälle, allerdings erst wenn der Schaden bereits entstanden ist.

Die Organisation kann sich nun darauf konzentrieren, dem nächsten Hacker das Leben schwerer zu machen. Regelmäßige Red-Team-Übungen – oder echte Sicherheitsvorfälle – ermöglichen es, die jeweils schwächsten Schutzglieder zu verbessern und einen immer besseren Schutz zu erreichen.

Die kontinuierliche Verbesserung wirft die nächste Frage auf: Wann hat die Firma ein ausreichendes Schutzniveau erreicht?
Diese bleibt bislang oft unbeantwortet, da Firmen ihren Hacking-Schutz nicht quantifizieren, also nicht wissen, wie einfach oder schwer es ein Hacker hat, an wichtige Daten zu kommen. Das muss sich hin zu einem berechenbaren Risikomanagement ändern. Was nicht gemessen wird, lässt sich schwer managen. Firmen brauchen eine Messlatte, um voneinander zu lernen und mit den Hackern Schritt zu halten. Sicherheit zu quantifizieren kann regelrecht in eine Hyperaktivität ausufern – oft werden Dutzende technische Kennzahlen gemessen und über die Zeit verglichen. Wie beim Wetterbericht gehen die Zahlen hoch und runter, ohne dass die Firma weiß, wie sie auf diese Einfluss nehmen kann. Messungen, die nicht klar Verbesserungsmöglichkeiten aufzeigen, sind somit nicht zielführend.

Eine sinnvolle Messgröße hat somit folgende Eigenschaften: a) Nachvollziehbarkeit, auch für Security-Laien, b) aus Sicht der Hacker formuliert und c) zielführend, also Verbesserungsmaßnahmen klar aufzeigend.

Hier bietet sich der Hackability Score als normierte Messlatte an, welche diese drei Eigenschaften mitbringt. Er aggregiert eine Vielzahl von Security-Messungen aus regelmäßigen Scans und Tests. Diese Rohdaten sind in aller Regel bei den Unternehmen bereits vorhanden. Sicherheitsscans großer Firmen finden regelmäßig mehrere 100.000 Schwachstellen, von denen die meisten einem Hacker oder Red-Teamer aber nicht weiterhelfen. Dadurch stiften die Scans mehr Verwirrung als Aufklärung und verdammen Sicherheitsteams zu frustrierender Mehrarbeit.

Bei der Zusammenfassung der Scanrohdaten in den Hackability Score wird für jeden Messpunkt die Frage gestellt: Wie sehr stört es einen Hacker, wenn diese Schwachstelle verschwindet? Somit ist klar vorgegeben, welche Handlungsvorschläge durch den Hackability-Score priorisiert werden: Diejenigen Maßnahmen, die den Score am meisten senken, machen auch den Hackern das Leben am schwersten. Das bestätigt spätestens die nächste Red-Team-Übung.

Da der Hackability Score immer gleich berechnet wird – für jede Organisation, jedes Team oder auch jedes Netzwerksegment –, ermöglicht er einen Dialog zwischen Peers, zum Beispiel zwischen Landesgesellschaften eines Konzerns. Der Score zeigt, wer von wem zu welchem Thema das Meiste lernen kann. Er ist im Übrigen nur ein Beispiel für eine normierte Messgröße, die den Dialog über Cyberrisiken ermöglicht – auch zwischen Experten und Laien. Jede Firma braucht eine solche Messlatte und den Dialog zwischen Peers.

Aus der einfach zugänglichen Messgröße entsteht automatisch ein Wettlauf: Wer kann seinen Hackability Score am schnellsten und nachhaltigsten verbessern?
Dieses Rennen läuft dezentral ab: Jede Firma, jedes Team, jede Applikation vergleicht sich mit der eigenen Peer Group. Da grundsätzlich niemand unterdurchschnittlich geschützt sein möchte, die meisten sogar weit überdurchschnittlichen Schutz anstreben, geht der Wettlauf immer weiter – ein positiver Kreislauf der ständigen Verbesserung. Und damit erreicht die Organisation die angestrebte Entmystifizierung des Themas Hacking und macht Fortschritt beim Hacking-Schutz transparent, was den Wetteifer weiter anheizt.

Eine letzte Zutat ist nötig, um den positiven Kreislauf ungestört ablaufen zu lassen: das Vertrauen des Unternehmens, dezentral Verbesserungen vorantreiben zu können. Statt Hacking-Schutz generalstabsmäßig zu steuern – wie es in vielen Firmen noch der Fall ist –, sollte die einzige Aufgabe der „Generäle" sein, dezentralen Teams einen Zielkorridor für deren Hackability Score vorzugeben. Wie ein Team diese Ziele erreicht, wird dort entschieden, oft durch gemeinsames Lernen in der Peer Group.

Hacking-Schutz wird erreicht durch:
1. Vertrauen in dezentrale Selbstorganisation
2. Wettlauf mit der Peer Group (z.B. Hackability Score)
3. Wettlauf mit echten Hackern (Red-Teaming)

Dezentralisierte Verbesserung basierend auf einer gemeinsam Messmethode, das genau ist Kybernetik.

Cybersecurity und Kybernetik

Ein Gespräch zwischen Dr. Ralf Schneider | Allianz SE und Andreas Slogar | Deloitte

Das folgende Interview mit Dr. Ralf Schneider basiert auf einem Gespräch, das als Episode des Podcasts „Sprint! New Work – New Mindset“ veröffentlicht wurde. Die vorliegende Version ist eine redaktionell überarbeitete Transkription.

Dr. Ralf Schneider ist seit 2010 Group CIO der Allianz SE und verantwortet global die IT Governance, Strategy und Security. Davor war er IT-Vorstand der Allianz Managed Operations & Services SE (2010–2016) und CIO der Allianz Deutschland (2006–2010). Nach seinem Studium der Mathematik und einer Promotion in Informatik fing er 1995 bei der Allianz an. Seit über 25 Jahren hat er führende Positionen im IT-Bereich inne, so war er u.a. Abteilungsleiter des Bereichs Informationssysteme Vertrieb und Fachbereichsleiter des Fachbereichs e-Business und Projektcontrolling Deutschland. Zusätzlich ist er Mandatsträger mehrerer Cyber-Security-Organisationen wie des Cyber Security Sharing & Analytics e.V., der Deutschen Cyber Sicherheitsorganisation und des Digital Society Institute an der ESMT.

Andreas Slogar war in über 20 Ländern, den USA, Europa, dem Mittleren Osten und Afrika tätig und hat u.a. als CIO umfassende Erfahrung in strategischer und operativer Managementarbeit aufgebaut. Slogar ist als Experte auf die Transformation ganzer Unternehmen in einen veränderungsfähigen Kollaborationszustand spezialisiert und ist Autor diverser Fachartikel, Podcasts und des Buches „Die agile Organisation“ (Hanser Verlag, 2018, 2020).

Andreas Slogar: Ralf, du hast mit deinem Team die globale Cybersecurity der Allianz Versicherung auf Grundlage der Modelle der Kybernetik komplett neu gedacht und etabliert. Könntest du uns zum Einstieg beschreiben, auf welche Probleme ihr im Bereich Cybersecurity gestoßen seid? Und wie kommt dabei Kybernetik ins Spiel?

Dr. Ralf Schneider: Die Allianz ist ein weltweit tätiges Unternehmen mit vielen Brands und operativen Einheiten. Und jede Einheit hat in der Cybersecurity zwei Key Player, den Chief Information Officer, der die Systeme verändern und sicherer machen kann, und den Chief Information Security Officer. Das sind bei uns 65 CIOs und 65 CISOs! Die große Herausforderung ist nun: Wie bekommt man diese 130 Menschen bei der Umsetzung von Cybersecurity auf eine Linie, ohne dass jeder in eine andere Richtung läuft? Wenn Systeme so komplex sind, gibt es nur eine Antwort: die Kybernetik, also die Wissenschaft der Selbstorganisation, Selbstregulation und Selbststeuerung. Denn die Hauptfrage der Kybernetik ist: Wie schafft man, dass sich das System selbst steuert?

Andreas Slogar: Das heißt, es war weniger ein technisches Problem, das ihr zu lösen hattet, sondern ein organisatorisches? Wie könnt ihr über Selbstorganisation effizienter, schneller, schlagfertiger werden?

Dr. Ralf Schneider: Wir bewegen uns ja in Systemen, die ich mit dem Begriff Socio-Cyber-Physical Systems beschreiben würde. Menschen sind über Software mit anderen Menschen oder Maschinen vernetzt. Und diese Vernetzung ist auch noch rückgekoppelt. Wenn man solche Systeme betrachtet, ist nicht nur entscheidend, wie ihre Prozess- oder Organisationsstruktur aussieht. Sondern auch: Wie funktioniert denn eigentlich die Steuerungsstruktur?

Andreas Slogar: Nun ist Cybersecurity ein immer relevanteres Themengebiet für alle Organisationen, von Firmen bis Regierungen. Was habt ihr mit Kybernetik erreichen können, was traditionelle Vorgehensweisen nicht erlauben?

Dr. Ralf Schneider: Der Ausgangspunkt ist die Frage: Wo will man überhaupt hin? Eines der wichtigsten kybernetischen Prinzipien lautet: Du brauchst eine gemeinsame Sprache, die jede handelnde Person im System gleichermaßen versteht. Wir haben also zunächst eine Policy formuliert, die beschreibt, wie in der Allianz Cybersecurity praktiziert wird. Darin sind auch die Security Controls und ihre Umsetzung definiert. Die Kybernetik kommt nun bei der Implementierung ins Spiel. In jeder unserer 65 Ländergesellschaften haben wir diese Controls implementiert und dann durch ein Effectiveness Testing überprüft. Die Kybernetik liefert dabei ein Modell für die Steuerung. Das Modell macht transparent, was vor Ort hinsichtlich Cybersecurity überhaupt los ist, welche Risiken identifiziert sind, welche Gefahren lauern oder welche Angriffe gerade ablaufen. Wir haben dafür zehn Cybersecurity Health Indicators definiert, die über Sensoren zentral überwacht werden. Durch diese transparente Steuerung der Systeme und durch die Rückkoppelung weiß jeder, was zu tun ist.

> Du musst zwei Dinge geben und zwei Dinge einfordern. Was du geben musst, ist natürlich Vertrauen. Vertrauen, dass die Leute das Richtige tun, aber auch das Richtige können. Das ist ganz wichtig, den Kolleginnen und Kollegen das Vertrauen zu übergeben. Und das zweite ist Autonomie. Mittel an die Hand geben und sie autonom operieren lassen. Ganz wichtig: Autonomie heißt nicht Autarkie.
>
> **Dr. Ralf Schneider, Allianz SE**

Kybernetik

Kybernetik bezeichnet die Wissenschaft von der Steuerung komplexer Systeme. Sie orientiert sich an der Selbstregulierung von natürlichen Organismen und überträgt diese Prinzipien auf Maschinen oder auch auf soziale Systeme. Ein bekanntes Beispiel für kybernetische Steuerung ist ein Thermostat, der mit Mess- und Steuerungselementen ausgestattet ist. Bei der Überschreitung bestimmter Schwellen des Istwerts wird bei der Heizung gegengesteuert, um den Sollwert zu erzielen. Der Begriff Kybernetik geht zurück auf das griechische Wort kybernetes („Steuermann"). Im Lauf seiner Geschichte wurde er von der Steuerungs- und Regelungstechnik u.a. auf die Disziplinen Informationstechnologie, Philosophie, Soziologie, Pädagogik und Managementtheorie übertragen.

Andreas Slogar: Bekommt dann jeder CIO diese Controls in einer Art Dashboard angezeigt? Oder habt ihr Arbeitskreise, in denen ihr euch diese regelmäßig anseht? Wie muss ich mir das operativ vorstellen?

Dr. Ralf Schneider: Das ist genau die richtige Frage, die uns zur Selbststeuerung bringt. In der Cybersecurity, wo sich ein Angriff quasi in Lichtgeschwindigkeit abspielt, kann man natürlich nicht mehr mit Komitees operieren. Wir nutzen hier als Dashboard unser sogenanntes Cybersecurity Cockpit, in dem uns – zentral wie dezentral – alle Informationen der Sensoren in Echtzeit zur Verfügung gestellt werden. Für mich ist die zentralste Methodik der Kybernetik, dass jeder weiß, dass jeder weiß. Das bedeutet nichts anderes, als dass jeder einzelne CIO erkennt, in welcher Situation er sich befindet, aber gleichzeitig auch weiß, wo alle anderen Kollegen stehen. Und er ist sich auch bewusst, dass alle Kollegen wissen, dass alle das gleiche Wissen haben wie er selbst. Und das in Echtzeit. Das ist der Schlüssel. Der springende Punkt ist aber nun: Wenn das Modell der Steuerung nicht ausreichend wirksam ist, um Angriffe abzuwehren, dann muss man das Modell anpassen, bis die notwendige Wirksamkeit (wieder) erreicht ist.

Andreas Slogar: Und das Modell passt ihr über die Rückkopplung der Ereignisse an. Wenn irgendwo eine Attacke läuft und das im Dashboard sichtbar wird, könnt ihr darüber das Modell iterativ weiterentwickeln?

Dr. Ralf Schneider: Genau. Es ist ein in zweierlei Hinsicht dynamisches Modell. Erstens werden die Cybersecurity-Health-Indikatoren entsprechend der Attack-Vektoren angepasst. Zweitens werden aber auch neue Indikatoren erstellt. In einer agilen Organisation soll eine Modellbildung ja nicht die reale Welt eins zu eins abbilden. Aber das Modell muss natürlich wirksam sein. Das Schöne bei Cybersecurity: Es wird sehr schnell erkannt, ob das Modell wirksam ist. Findet man einen Angreifer, kann man ihn abwehren oder identifizieren und somit das Modell immer nachschärfen. Und die Pointe ist: Weil die Sprache durch die Policy für alle Landesgesellschaften gleich ist, werden Anpassungen jeweils für alle gleichermaßen und simultan wirksam.

Attack Vectors (Angriffsvektoren)
In der Cybersecurity wird mit dem Begriff Angriffsvektor der jeweilige Pfad oder die Methode beschrieben, mit der ein Angreifer (Hacker) in ein System eindringt und einen Schaden verursacht. Der Begriff stammt aus der Biologie bzw. Epidemiologie, wo der Vektor den Überträger eines Krankheitserregers bezeichnet. Beispielsweise transportiert die Anopheles-Mücke die parasitären Einzeller, die dann im Menschen die Malaria auslösen. Im IT-Bereich werden durch die Angriffsvektoren typischerweise bestimmte bekannte Schwächen der Zielsysteme ausgenutzt („exploits"). Zu den Vektoren zählen Pufferüberlauf, JavaScript-Schwachstellen, Netzwerkprotokoll-Schwachstellen oder Phishing.

Andreas Slogar: Die Transparenz des Modells zwingt gewissermaßen alle zur Kooperation. Wird das auch so genutzt – oder befinden sich jetzt alle im Wettbewerb, wer am schnellsten bei der Bekämpfung von Attacken ist?

Dr. Ralf Schneider: Ich würde es umdrehen. Es zwingt nicht zu Kooperation, sondern es gibt der Gruppe die Möglichkeit dazu. Man sollte die Möglichkeiten sehen, nicht den Zwang. Das ist bei Cybersecurity ein Riesenvorteil. Man hat ja einen gemeinsamen Gegner. Der Angriff bleibt nicht auf eine Landesgesellschaft beschränkt, sondern man ist immer eine Schicksalsgemeinschaft. Da siegen Kooperation und Best Practice Sharing immer. Man versucht nicht, selbst die beste Verteidigungsmethode zu entwickeln, sondern man kooperiert und befolgt dabei einen gemeinsamen Standard. In Trainings wird außerdem die dezentrale Nutzung der Cyberdefense-Tools geübt, nicht die Erfindung neuer Verteidigungen. Diese wiederum findet zentral statt.

Andreas Slogar: Du hast das Thema „agile Organisation" erwähnt. Die unmittelbare Reaktion auf eine dynamische Veränderung meiner Umwelt ist exakt das, was von der agilen Bewegung versprochen wurde, wobei ihr hier in der Königsklasse der Dynamik unterwegs seid, in der die Veränderungen in „Lichtgeschwindigkeit" auftreten. Ich kann eine Cyberbedrohung nicht erst diskutieren, sondern muss meine Maßnahmen auf dem Tisch haben und sie sofort selbstorganisiert anwenden. Kann dieses kybernetische Prinzip auch in anderen Bereichen einer Organisation angewendet werden?

Dr. Ralf Schneider: Absolut. Ich mache mal eine kleine Zeitreise. Es war 2008 oder 2009, als ich das erste Mal Kontakt mit dem agilen Manifest bekommen habe, wir haben das auch umgesetzt. Bei agiler Organisation haben wir immer das folgende wichtige Prinzip angewendet: Du musst zwei Dinge geben und zwei Dinge einfordern. Was du geben musst, ist natürlich Vertrauen. Vertrauen, dass die Leute das Richtige tun, aber auch das Richtige können. Das ist ganz wichtig, den Kolleginnen und Kollegen das Vertrauen entgegenzubringen. Und das Zweite ist Autonomie: Mittel an die Hand geben und sie autonom operieren lassen. Ganz wichtig: Autonomie heißt nicht Autarkie. Für eine effektive und effiziente agile Organisation ist Verantwortungsübernahme entscheidend. Die Verantwortung bleibt dann dort, wo du das Vertrauen hingegeben hast. Das ist zentral. Ich kann nicht gleichzeitig vertrauen und dann nicht wissen, was passiert. Transparenz stellt ein ganz wichtiges kybernetisches Prinzip dar. Nicht kleinteilig, sondern als Transparenz über die Wirksamkeit der autonomen Einheiten, so ähnlich wie auf dem Fußballplatz. Ich sehe, wie effektiv meine autonomen Einheiten sind, und kann intervenieren, indem ich Anweisungen gebe, die Strategie

ändere oder sogar auch jemanden auswechsle. Bei Cybersecurity kommt man gar nicht um die Autonomie der agilen Organisation herum. Im Management allgemein, im IT-Management im Besonderen und ganz im Besonderen in der Cybersecurity haben wir bislang einen blinden Fleck. Tayloristisch und arbeitsteilig kannst du hier aber nicht mehr steuern. Das geht nur noch über Selbstorganisation. Derjenige, der „an der Front" Hacker abwehrt, muss autonom agieren. Er ist dabei aber rückgekoppelt mit dem zentralen System und macht transparent, was er gerade tut.

Agile Organisationen
Agile Organisationen zeichnen sich durch schnelle Lern- und Anpassungsfähigkeit aus. Im Gegensatz zu hierarchischen Organisationen weisen sie offene Strukturen und komprimierte Entscheidungszyklen aus. Teams sind maximal autonom. Zu den Voraussetzungen gehören Transparenz und effektive Rückkopplungsschleifen. Agile Organisationen sind besonders für Situationen geeignet, die von einem hohen Grad an externer Unsicherheit geprägt sind. Vor allem im Bereich der Softwareentwicklung wurde das Konzept in den letzten zwei Jahrzehnten bekannt. 2001 wurden seine Prinzipien im „Manifesto for Agile Software Development" formuliert, mit Bezug auf Ansätze wie SCRUM und Kanban.

Andreas Slogar: Ihr habt also in der Policy ein gemeinsames Verständnis und Vorgehensmodell vereinbart. Genau damit bleibt ihr dezentral, zueinander kompatibel und anschlussfähig. Jeder ist selbstorganisiert dafür verantwortlich, dass die Policy in seiner Domäne angewendet wird. Und die Transparenz erlaubt es euch kollektiv, eine algedonische Schleife zu etablieren, um aus den Erfahrungen wieder eine Rückkopplung zu erzielen und so euer Modell weiterzuentwickeln.

Dr. Ralf Schneider: Ja. Im Dezember 2021 hatten wir mit Log4j ein Cyberthema, von dem wir sehr gut lernen konnten, weil es für alle neu war. Es wurde bekannt, dass eine Schwachstelle in einer Java-Bibliothek existierte, und es musste praktisch jeder Quellcode untersucht werden, ob diese Bibliothek benutzt wird. In der Allianz Deutschland haben zwei, drei Mitarbeiter einen Scan geschrieben, um die Schwachstellen zu finden. Und die konnten wir sofort der ganzen Welt operativ zur Verfügung stellen. Jeder konnte seine IP-Adressen eingeben und über den Algorithmus überprüfen, ob diese Gefahr aus dem Web vorhanden war oder nicht. Ich glaube, in nur drei Stunden wurden 7.500 IP-Adressen der Allianz untersucht.

Algedonische Schleife
Dieser Begriff wurde von dem amerikanischen Psychologen Henry Rutgers Marshall (1852–1927) geprägt und vom britischen Kybernetiker Stafford Beer (1926–2002) aufgegriffen. Er bezeichnet die Steuerung eines Organismus oder Systems durch Anreizrückkoppelungen wie Schmerz und Lust (von griechisch: algos = Schmerz, hedone = Lust). Wenn Verhaltensweisen nur auf diesen Anreizmechanismus, aber nicht mehr auf Umweltreize optimiert werden, besteht das Risiko von kontraproduktivem Verhalten.

Log4j
Log4j ist das dominante IT-Framework für das automatische Erstellen von Protokollen. Es wird u.a. im Rahmen des Apache-Logging-Projekts gepflegt. Heute wird es in vielen Programmiersprachen und Anwendungen verwendet. Im Dezember 2021 wurde eine Sicherheitslücke in Log4j-Version 2 bekannt, durch die Angreifer aus der Ferne Programmcode auf dem betroffenen System ausführen lassen konnten.

Andreas Slogar: Das ist ein Skalierungseffekt, der für sich selbst spricht. – Jetzt aber eine Frage zu dir: Wie bist du eigentlich zur Kybernetik gekommen?

Dr. Ralf Schneider: Die Kybernetik ist in Gestalt des Wirtschaftswissenschaftlers Fredmund Malik zu mir gekommen. Dabei ging es um das Thema Komplexität, um die Steuerung komplexer Systeme. Vor vier Jahren habe ich Herrn Malik kennengelernt, und er hat mir Kybernetik nähergebracht und vor allem, wie man sie im Management umsetzt. Ein entscheidendes Modell dafür ist das Viable System Model von Stafford Beer. Es beantwortet die Frage: Wie steuert man eine Organisation kybernetisch?

Viable System Model
Der Begriff Viable System Model („Modell lebensfähiger Systeme“) geht auf den Kybernetiker Stafford Beer zurück. Dabei wird anstelle von Gewinnmaximierung das Überleben des Systems als oberstes Ziel gesetzt. Eine zentrale Steuerung ist hierfür schlechter geeignet als eine dezentrale Selbststeuerung aller Systemelemente. Unter dem sozialistischen Präsidenten Salvador Allende wurde im Chile der frühen 1970er-Jahre von Stafford Beer und anderen der Versuch unternommen, ein entsprechendes computergestütztes Entscheidungssystem für die Steuerung der Volkswirtschaft umzusetzen (Cybersyn), als demokratischere Alternative zur sowjetischen Kommandowirtschaft.

Andreas Slogar: Spannend, wir sind ja beide große Fans von Stafford Beer und Heinz von Foerster, dem Viable System Model und allem, was man damit beispielsweise in Chile in den 1970er-Jahren erreicht hat.

Dr. Ralf Schneider: Ja, das muss man sich mal überlegen: Er hatte schon damals verstanden, worum es geht, und das in Chile umgesetzt. Wenn er dabei Cybersecurity-Sensoren hätte anwenden können, wäre das für ihn natürlich ein Highlight gewesen. Die sind heute ganz wichtig: Du musst automatisierte Sensoren haben! Du darfst dich in der Cybersecurity nicht auf Berichtswege verlassen, weil du sonst einfach zu langsam bist.

Andreas Slogar: Nun ist Kybernetik in der Wirtschaftswelt nicht sehr verbreitet. Wenn man darüber spricht, wird man oft verwundert angestarrt. Woran liegt das?

Dr. Ralf Schneider: Ich glaube, das liegt an diesem blinden Fleck, den wir gar nicht sehen, den Manager in ihrer Ausbildung und Berufspraxis nicht erfahren. Man trainiert sehr gut und sehr strukturiert, analytisch die richtige Entscheidung zu treffen. Gehen wir links oder rechts, oder untersuchen wir es noch genauer und überlegen uns einen dritten Weg? Bei Cybersecurity kannst du aber als Manager gar nichts mehr entscheiden. Da musst du dich darauf verlassen, dass das System und die Mitarbeiter die richtigen Entscheidungen treffen. Du kannst nur daran arbeiten, welches Prozess-, Steuerungs- und Organisationsmodell du verwendest. Und auf der Metaebene daran, wie gut Mitarbeiter auf dieses Modell trainiert sind. Dabei musst du eigentlich alles „entlernen“, was du vorher als Manager gelernt hast. Das gilt auch für Bauchentscheidungen von Managern. Bei Cybersecurity sind die ganz schlecht – anders als Bauchentscheidungen von Experten! Der Manager dagegen sollte stattdessen auf der Metaebene am Modell arbeiten. Das Problem ist aber: Wir sind alle Kinder des Taylorismus und der Arbeitsteilung. Das sind jedoch beides Strukturierungskonzepte, die nicht in die Kybernetik passen.

Andreas Slogar: Das würde ja bedeuten, dass Manager ihr Selbstverständnis um 180 Grad drehen müssten. Dass sie nicht diejenigen sind, die andere managen und ihnen Vorgaben machen. Sondern diejenigen, die sicherstellen, dass Management als Fähigkeit in einer Organisation praktiziert wird. Manager beobachten diese Fähigkeit und entwickeln sie weiter. Sie etablieren Selbstorganisation, so wie ihr sie bei euch aufgebaut habt.

Dr. Ralf Schneider: Absolut richtig! Es geht nicht mehr um Macht über Menschen, sondern um Macht mit Menschen. Das bedeutet, Systeme so zu bauen, dass man

Taylorismus
Der amerikanische Erfinder und Ingenieur Frederick W. Taylor (1856–1915) entwickelte ein wissenschaftlich fundiertes System der Arbeitsorganisation, etwa für Fabriken. Der Taylorismus basiert auf den Prinzipien der Arbeitsteilung: Produktionsabläufe werden in verschiedene Unterprozesse gegliedert, die von Arbeitern einzeln effizienter ausgeführt werden können, als wenn jeder Arbeiter sämtliche Prozessschritte durchführt (Beispiel Fließbandproduktion). Taylor unterlegte seinen Ansatz mit wissenschaftlichen Zeitmessungen realer Arbeitsabläufe und stellte so die Effizienz sicher. Der Begriff wird oft auch kritisch verwendet, um eine starre Arbeitsorganisation zu beschreiben.

wirklich effektiv ist. Je besser du bist, desto weniger musst du als Modelldesigner tun, desto weniger Arbeit hast du. Manager sind aber anders konditioniert. Sie denken: Je mehr Zeit sie investieren und je härter sie arbeiten, umso wichtiger sind sie. Dabei ist es genau umgekehrt! Je besser dein System selbstorganisiert läuft, umso effektiver ist es. Du musst dich als Manager mehr darauf konzentrieren, wie du die Experten förderst und forderst.

Andreas Slogar: Wenn sich nun jemand in dieses faszinierende Thema einarbeiten möchte, welche Tipps hättest du?

Dr. Ralf Schneider: Also ich würde zunächst das Buch „Kybernethik“ von Heinz von Foerster empfehlen. Das Wort „Ethik“ ist dabei sehr wichtig. Denn mit Kybernetik kann man alles steuern, auch einen Überwachungsstaat und eine Diktatur. Deswegen braucht Kybernetik auch

ein starkes ethisches Verständnis, sonst endet man in Dystopien. Dann sollte man sich Wissen über das Viable System Model aneignen. Erst einmal etwas Stafford Beer, und dann auch ein Buch von dir: „Die agile Organisation". Denn du bringst extrem gut auf den Punkt, wie das angewendet werden kann. Die große Kunst ist es nämlich, nicht nur intellektuell zu verstehen, was Kybernetik ist. Man muss es auch umsetzen. Und dann muss man loslassen. Das ist natürlich schwer. Fredmund Malik sagt, ich bekomme Kontrolle über Kontrolle und nicht mehr Kontrolle über Menschen. Das ist ein ganz anderes Mindset!

Andreas Slogar: Freut mich sehr, dass mein Buch so gut bei dir ankommt. Ich finde auch die Überlegungen von Ross Ashby zum Thema der Requisite Variety von Organisationen spannend. Das sind wirklich Sternstunden der kybernetischen Theorie. Aber das in den betrieblichen Alltag zu bringen, das ist schon nicht ohne. Ihr habt das gleich auf die „Königsklasse" angewendet, auf Cybersecurity. Aber man könnte auch mit kleineren Themen anfangen, die weniger anspruchsvoll sind. Zum Beispiel einen Kurs bei Fredmund Malik besuchen und dann in der eigenen Organisation die Anwendung ausprobieren.

Dr. Ralf Schneider: Und man kann es ja in der Praxis leicht überprüfen. Wenn jemand sagt, er steuert kybernetisch, dann würde ich fragen: Ja, wo ist denn dein Dashboard? Und als Zweites würde ich fragen: Wie aktuell ist denn dein Dashboard? Realtime? Daran kann man sehr viel erkennen.

Andreas Slogar: Ohne jetzt betriebliche Geheimnisse zu verraten: Wie geht die Reise mit der Kybernetik bei der Allianz weiter?

Requisite Variety
Der Begriff der erforderlichen Komplexität wurde von dem britischen Wissenschaftler W. Ross Ashby (1903–1972) geprägt. Sein „Gesetz der erforderlichen Varietät" (Law of Requisite Variety, Ashbysches Gesetz) bezeichnet das Mindestmaß an Komplexität (Handlungsvarietät), das ein System benötigt, um ein anderes zu steuern und dabei zugleich über ausreichend Spielraum für die Bewältigung der durch die Umwelt gestellten Herausforderungen (Störungen) zu verfügen. Dabei muss die Systemkomplexität derjenigen der Störungen mindestens entsprechen.

Dr. Ralf Schneider: Um hochkomplexe Systeme wie die Cybersecurity in der Allianz anzugehen, kommt man natürlich sofort zur IT. Allgemein gilt hier das gleiche Prinzip. Wie steuert man IT-Run, IT-Change und Projektentwicklung? Da liegt ein Bezugspunkt zur agilen Organisation. Sobald zehn oder 15 Menschen zusammenkommen, hat man ein hochkomplexes System. Dann braucht man kybernetische Steuerung. Das betrifft auch das Management, nicht nur IT oder Cybersecurity. Im Management sollten Hierarchien nur für das benutzt werden, wo sie wirklich ihre Stärke haben: um Freiräume zu geben und Ressourcen zu verteilen. Aber die eigentliche operative Steuerung läuft dann dezentral kybernetisch. So ist es ja auch beim Menschen. Würde jede Handlung durch das Gehirn gesteuert, ohne Selbststeuerung und Selbstregulierung mit Homöostase im Körper, wir kämen keine fünf Sekunden weiter. Auch Systeme und Organisationen müssen so gebaut werden.

Homöostase
Der aus der Biologie stammende Begriff bezeichnet den inneren Gleichgewichtszustand eines dynamischen Systems, der durch Selbstregulierung erzielt wird, etwa durch die Anpassungen im menschlichen Körper an eine Krankheit oder nach externen Einwirkungen. Physiologische Beispiele sind die Blutzucker- oder die Wärmeregulation.

Andreas Slogar: Das ist ein schönes Bild. Was die Kybernetik uns erklärt, ist nichts anderes als das, was jeder von uns im Alltag praktiziert. Es ist nur keinem so richtig bewusst. Wenn wir im System der Unternehmensorganisation sind, erlangen aber paradoxerweise plötzlich diese hierarchischen Modelle Macht über uns. Und wir geben das, was wir können, nämlich Selbstorganisation und Eigeninitiative, an der Garderobe ab.

Dr. Ralf Schneider: Genau. Im Unternehmen hängen wir drei großen Dinge nach. Wir wollen alles planen, am besten mit einer Quartalsplanung. Wir wollen alles vorhersehen, was passieren wird. Wir wollen alles bis auf die Nachkommastelle kontrollieren. Man weiß aber, dass komplexe Systeme weder planbar noch kontrollierbar und schon gar nicht vorhersehbar sind. Wir versuchen es aber trotzdem, obwohl der Mensch an sich das anders macht. Zum Beispiel merken wir, wenn wir ein drittes Mal gegen die Wand gelaufen sind, dass unser Modell nicht mehr funktioniert. Zunächst kennen wir die Wand nicht, dann erkennen wir sie. Ein viertes Mal laufen wir nicht dagegen. In Organisationen dagegen kann es passieren, dass wir nach dem dritten Mal dennoch wieder genau gleich planen, ein viertes, fünftes oder sechstes Mal. Wenn's nicht mehr funktioniert, dann hilft „mehr vom Gleichen" einfach nicht. Dann müssen auch Organisationen ihr Modell ändern.

Andreas Slogar: Das ist ein schöner Übergang zum Schluss. Ich möchte dazu jetzt fragen: Was würdest du denn Kollegen empfehlen, die das umsetzen wollen – im Hinblick auf deine Erfahrungen der letzten vier Jahre?

Dr. Ralf Schneider: Als Allererstes: extrem demütig sein. Nicht mehr glauben, die Systeme noch verstehen zu können oder unterscheiden zu können, was richtig und falsch ist. Um möglichst gute Entscheidungen zu treffen, ist wie gesagt Transparenz elementar. Als ITler würde ich sagen: Schau auf die Daten, mach aus Daten Informationen, setze Sensoren ein, bilde ein abstraktes Modell deiner Realität. So wie es der Mensch auch macht. Er sieht ja nicht alles, sondern nur ein Spektrum von Wellen und Farben. Orientiere deine Modellbildung auf den Zweck deines Unternehmens und lerne, es ganz schnell anzuwenden. Und eine zweite Empfehlung: eine gemeinsame Sprache über die Problemstellung entwickeln. Das vermisse ich häufig in Unternehmen. Vielleicht liegt das auch an meiner Historie als Mathematiker. Wenn ich eine gemeinsame Sprache habe, durch die Policy, dann kann ich überlegen, welche Controls ich einziehe, damit mein System funktioniert. Sind die Controls vollständig? Sind sie effektiv oder effizient genug? Das ist die Funktion der Rückkopplung. Man sollte dabei nicht einfach nur denken, etwas wurde falsch gemacht, sondern sich selber reflektieren und hinterfragen, ob das Problem überhaupt schon verstanden wurde.

Andreas Slogar: Ralf Schneider, ganz herzlichen Dank für diesen Blick hinter die Kulissen, und auch für deinen Ausblick, was man damit noch machen kann – wenn man diesen Ansatz im Sinne von Heinz von Foerster ethisch ernst nimmt und auch danach handelt.

Was ist Kybernetik?

Prof. Dr. Fredmund Malik | Malik International AG

Das Wort „Kybernetik“ kommt vom griechischen „kybernetes“. Das heißt Steuermann und ist die griechische Wurzel für Begriffe wie Governor, Gouverneur und Governance. Kybernetik ist die Wissenschaft, die Kunst und das Handwerk der Steuerung – und verallgemeinert der Steuerung, Regelung und Lenkung – durch Kommunikation.

Prof. Dr. Fredmund Malik ist anerkannter Managementexperte sowie Vorsitzender von Führungs- und Beratungsgremien in Wirtschaftsunternehmen. Er ist ein Pionier der Managementkybernetik und des Komplexitätsmanagements. Er war Mitglied des Direktoriums des Instituts für Betriebswirtschaftslehre und seit 1977 parallel dazu des Managementzentrums St. Gallen. Er ist Autor von mehr als 15 Büchern. Sein Buch „Führen Leisten Leben“ wurde unter die 100 besten Wirtschaftsbücher aller Zeiten gewählt. 2018 erhielt er den Life Achievement Award, die höchste Auszeichnung im deutschen Management-Bildungssystem.

Dass hinter dieser Kunst auch eine Wissenschaft steht, braucht man im Alltag nicht weiter zu beachten. Interessant und wichtig wird das erst, wenn Probleme auftauchen, für deren Lösung das Alltagsverständnis allein nicht mehr ausreicht.

Wie der anerkanntermaßen geniale Mathematiker Norbert Wiener zur Kybernetik kam, warum er sein Buch 1948 „Kybernetik“ nannte und wer auf diesem Gebiet sonst noch wichtig war, ist eine eigene Geschichte. Hier sei erwähnt, dass die Kybernetik die vielleicht wichtigste Wissenschaft des 20. Jahrhunderts ist und das 21. schon heute formt. Der volle Buchtitel lautet im Englischen: „Cybernetics – Control and Communication in the Animal and the Machine“. Im 2. Weltkrieg arbeitete Norbert Wiener an der Mathematik von sich selbst steuernden Raketen.

Vom 20. in das 21. Jahrhundert

Über die Atomphysik wurde öffentlich viel intensiver als über die Kybernetik diskutiert. Die Kybernetik ist es, die das 20. Jahrhundert in das 21. transformiert. Ihre vollen Auswirkungen werden unser Jahrhundert prägen. Sie werden unser Leben von Grund auf verändern. Ohne Kybernetik gäbe es keine Computer und Roboter; keine Elektronik und keine Informatik. Es gäbe weder die rasanten Fortschritte in den biologischen Disziplinen noch die Gentechnik. Die mit der Kybernetik verbundenen Entwicklungen schaffen Risiken, aber noch viel größere Chancen. Wer Erstere vermeiden und Letztere nutzen will, sollte sich mit Kybernetik befassen.

Es waren die Kybernetik und die eng mit ihr zusammenhängenden Gebiete der Systemwissenschaften und der Informationstheorie, die es ermöglicht haben, die dritte Grundgröße der Natur – die Information – zu verstehen, zu erklären und sie schließlich systematisch zu nutzen.

Bis dahin „kannte“ man in der Wissenschaft offiziell nur zwei elementare Größen – Materie und Energie. Das sind die „Gegenstände“, mit denen sich die Königsdisziplinen der Naturwissenschaften – Physik und Chemie – im Zuge der Aufklärung befassten. Und auf diese versuchte man die Erscheinungsformen der Welt zu reduzieren. Zweifellos hat uns dieser Forschungsansatz einen enormen Zuwachs an Erkenntnissen gebracht und gleichzeitig deren Anwendung in Form der Technik.

Das Jahrhundert der Vernetzung

Einige Wissenschaftler waren mit der Grundphilosophie der Naturwissenschaften nie ganz zufrieden. Irgendetwas fehlte – und zwar etwas Entscheidendes. Wenn man weiß, dass ein Gegenstand aus etwa 15 kg Kohle, 4 kg Stickstoff, 1 kg Kalk, ½ kg Phosphor und Schwefel, etwa 200 g Salz, 150 g Kali und Chlor und etwa 15 anderen Materialien sowie ziemlich viel Wasser besteht – was weiß man dann? Im Grunde gar nichts.

Geprägt durch konventionelle naturwissenschaftliche Denkweise und erzogen auf der Grundlage ihrer Logik, werden nur wenige auf die Idee kommen zu antworten: Es kommt darauf an, wie man diese Materialien organisiert … Genau darauf kommt es aber an.

Die genannten Rohmaterialen sind das, was wir erhalten, wenn wir einen Menschen in seine materiellen Bestandteile zerlegen. Nichts Bemerkenswertes bleibt übrig, wenn wir einem Lebewesen das nehmen, was es

zum Lebewesen macht. Wichtig sind nicht die Materialien. Sondern wichtig ist ihre Organisation, das Muster, die Ordnung, die sie aufweisen, oder die In-Formierung, welche die Materialien in eine Ordnung bringt. Leben ist nicht Materie und Energie; sondern Leben ist in-formierte Materie und Energie.

Das ist es, was die Kybernetik wichtig macht. Eine ihrer bedeutendsten Einsichten besteht darin, dass Materie und Energie für den Charakter und die Fähigkeiten eines Systems vergleichsweise wenig Bedeutung haben. Woraus ein System besteht, ist zwar wichtig. Wesentlich ist aber die Information, welche die Grundelemente ordnet und organisiert. Dadurch erst werden die Bauelemente zu einem System.

Vernetzung mit den Biowissenschaften – aber eigenständig

Zu den enormen Entwicklungen in den technischen Gebieten und in der Informatik treten Impulse aus den Biowissenschaften. Dort kommen sie wiederum in erster Linie aus den Neurowissenschaften, der Erforschung von Gehirnen und Zentralnervensystemen. Es ist Letzteres, das einen Organismus steuert, kontrolliert und lenkt. Hirnforschung ohne Kybernetik ist heute nicht mehr vorstellbar.

Die Kybernetik erhält von hier wichtige Impulse, ist aber mit der Hirnforschung nicht identisch. Sie ist eine eigenständige Wissenschaft. Die Basis der Kybernetik ist die Entdeckung, dass es natürliche Gesetzmäßigkeiten gibt, welche die Kontrolle und das Funktionieren aller Systeme bestimmen.

Dabei ist es gleichgültig, ob es sich um natürliche oder künstliche Systeme handelt, und egal, ob es biologische, physikalische, technische, soziale oder ökonomische Systeme sind. Das ist es, was die Kybernetik zu einer grenzüberschreitenden – transdisziplinären – Wissenschaft macht, was wiederum etwas anderes als interdisziplinär ist.

Das war es, was Norbert Wiener zu dem wichtigen, oft übersehenen oder unverstandenen Untertitel für sein Buch veranlasste: ... in the Animal and the Machine ..., womit er den Graben zwischen der natürlichen und der künstlichen Welt meinte, der seit der Antike das Verständnis für komplexe Systeme behinderte und uns heute die größten Fortschritte ermöglicht.

Design und Management agiler Cybersecurity-Organisationen

Andreas Slogar | Deloitte

Die Arbeit von Cybersecurity-Teams zur Abwehr von Cyberattacken in Unternehmen wirkt immer mehr wie der ungleiche Wettlauf zwischen Hase und Igel. Die Fabel handelt nicht von einem sportlichen Wettkampf, sondern vielmehr von einem existenziellen Konflikt – hier zwischen Cybersecurity-Spezialisten in Unternehmen und den angreifenden Cyber-Hackern. Es werden Hightechmittel eingesetzt und es gibt keine Regeln. Zumindest nicht für Hacker. Und wie beim Wettlauf von Hase und Igel gewinnen nicht diejenigen, die den größten Aufwand betreiben und sich mehr anstrengen, sondern die Kreativeren und Agileren. Es gewinnen die, die es schaffen, den Gegnern einen Schritt voraus zu sein oder sie auszutricksen.

Technische Finessen und Know-how werden von Cybersecurity- und Hacker-Teams gleichermaßen eingesetzt. Aber davon einmal abgesehen, stellen völlig untechnische Faktoren den eigentlichen Unterschied in diesem Konflikt dar. Hacker sind hochgradig flexibel, agil, kreativ und können vor allem mit geduldigem Versuchen, Ausprobieren und Experimentieren großen Schaden verursachen. Hacker müssen bei ihren Attacken nur einmal erfolgreich sein, um an ihr Ziel zu gelangen – egal welche Motive sie antreiben. Cybersecurity-Teams hingegen sind gezwungen, immer zu gewinnen, und zwar gegen jeden.

Vergleicht man die Organisationsstruktur von Hackern mit denen von Cybersecurity-Teams, dann werden weitere Unterschiede deutlich. Hacker sind autark oder autonom tätig. Sie arbeiten völlig dezentral und gehen agil vor, d.h., sie passen ihre Manöver den sich ergebenden Gelegenheiten und Möglichkeiten an. Durch das dezentrale Vorgehen erscheint ihre Arbeitsweise ausgesprochen resilient und redundant, auch wenn das keine primäre Eigenschaft, sondern ein sich ergebender Effekt ist. Die Lerngeschwindigkeit von Hackern ist sehr hoch, da sich Erfolg und Misserfolg in einer kontinuierlichen Feedback- und Lernschleife befinden. RACI-Matrizes und QS-geprüfte Geschäftsprozesse, Zuständigkeitsbereiche und Entscheidungsautoritäten spielen keine Rolle – ebenso wenig wie Managementstrukturen. Es ist immer die wirkungsvollste Attacke, die die Richtung vorgibt.

Richten wir dagegen den Blick auf die Organisationsstrukturen und Kooperationsmodelle von Cybersecurity-Teams (kurz CSTs) in Unternehmen, so scheinen die zuletzt genannten Begriffe ausgesprochen relevant zu sein. Rollenmodell, Zuständigkeiten und Entscheidungswege sind vorgegeben, Kompetenzen festgelegt und Geschäftsprozesse revisionssicher definiert und dokumentiert. Der Grad an autonomer oder gar autarker Handlungsfreiheit für CSTs und ihre Mitarbeitenden in der gesamten CISO-Organisation wird fest vorgegeben und ist meist rollenspezifisch limitiert.

Aus dieser Gegenüberstellung ergibt sich die Frage, wie das Design einer CISO-Organisation und das darin genutzte Kooperationsmodell aussehen müssen, um den Mitarbeitenden in den CSTs die Vorteile der Vorgehensweise von Hackern zu verschaffen.

Klassische CISO-Organisationen – drei Archetypen

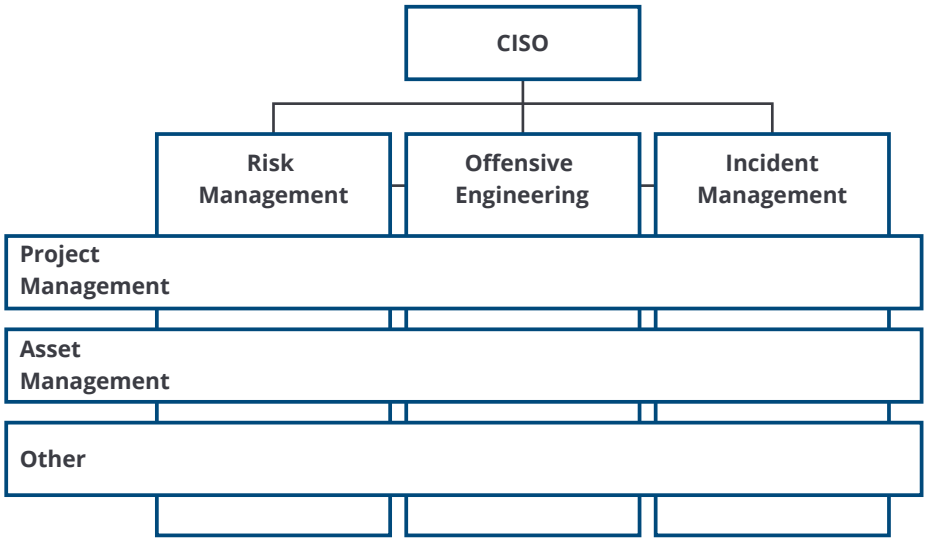
Betrachten wir zunächst typische Organisationsstrukturen von CSTs und ihren Organisationseinheiten, die überwiegend von CISOs verantwortet werden. Anschließend schätzen wir ein, inwiefern sie die Eigenschaften der Arbeitsweise von Hackern für die eigene Arbeitsweise prinzipiell nutzen oder fördern können.

CISO-Organisationen, die flache Hierarchien und Matrixstrukturen aufweisen, sind darauf ausgerichtet, Redundanzen in ihren Geschäftsfähigkeiten zu vermeiden. Sie fokussieren sich darauf, eine höchstmögliche Effizienz der eingesetzten Mitarbeitendenkapazität und der benötigten Ressourcen sicherzustellen. Ein derartiger Fokus will ein adäquates Leistungs- und Qualitätsniveau der CISO-Organisation zu geringsten Kosten erreichen.

Diese Ausrichtung geht zulasten von Resilienz und Redundanz, da ausgefallene Geschäftsfähigkeiten nicht von alternativen Funktionen abgefangen oder zumindest temporär übernommen werden können. Matrixorganisationen sind zusätzlich von multiplen Kommunikations- und Berichtswegen geprägt. Das führt bei der Einsatz- und Arbeitsplanung der Mitarbeitenden zu Zielkonflikten. Matrixorganisationen und Organisationsmodelle mit flachen Hierarchien versuchen einen Kompromiss zwischen den Verantwortungsbereichen des Managements und möglichst kurzen Kommunikationswegen zu finden.

Durch die Vielzahl an Kommunikationsschnittstellen der Teams und Mitarbeitenden werden die primären Ziele einer derartigen Organisationsstruktur nicht erreicht. Matrixorganisationen sind daher für eine Maximierung der Kommunikationsfähigkeit der CSTs ungeeignet.

Abb. 1 – A.) Fokus: flache Hierarchie und Matrix



Manche CISO-Bereiche fokussieren spezialisierte Abteilungen und Teams auf bestimmte Themengebiete oder Geschäftsfähigkeiten. Sie orientieren sich an klassischen Strukturierungsformen hierarchischer Organisationsmodelle. Dabei wird ersichtlich, in welcher Abteilung oder Unterabteilung eine individuelle Frage- oder Aufgabenstellung organisatorisch angeordnet ist. Wie diese Abteilung und die darin zusammengefassten Mitarbeitenden miteinander und mit ihrem Umfeld und ihrer Umwelt kooperieren, bleibt unklar.

Bei der geografischen Fokussierung des Organisationsmodells handelt es sich um eine Variante der vorhergehenden Struktur. Sie repräsentiert eine skalierte und in den etablierten Geschäftsfähigkeiten möglichst ähnliche Darstellung für global agierende Unternehmen. Damit nehmen diese Organisationsstrukturen vor allem die Darstellungsformen der übrigen Unternehmensbereiche wie Vertrieb, Marketing oder Finanzen auf, können die Kooperationsformen jedoch nicht repräsentieren. Da Landesgrenzen für Cybersecurity-Ereignisse irrelevant sind, ist auch diese hierarchische Organisationsform in ihrem Informationsgehalt und Nutzen als Orientierungshilfe sehr limitiert.

Die bisherigen Beschreibungen sind bewusst pointiert dargestellt, um die nachfolgend beschriebenen Alternativen klarer abzugrenzen. Sicher hat kein Unternehmen einen dieser drei Archetypen in Reinform etabliert. Eine Unterschiedsbildung soll Anregungen geben, die CSTs und CISO-Bereiche für sich adaptieren und integrieren können, um Handlungsfähigkeit, Entscheidungsgeschwindigkeit und Wirkungsgrad der eigenen Cybersecurity-Arbeit den jeweiligen Erfordernissen entsprechend anpassen zu können.

Abb. 2 – B.) Fokus: Geschäftsfähigkeiten

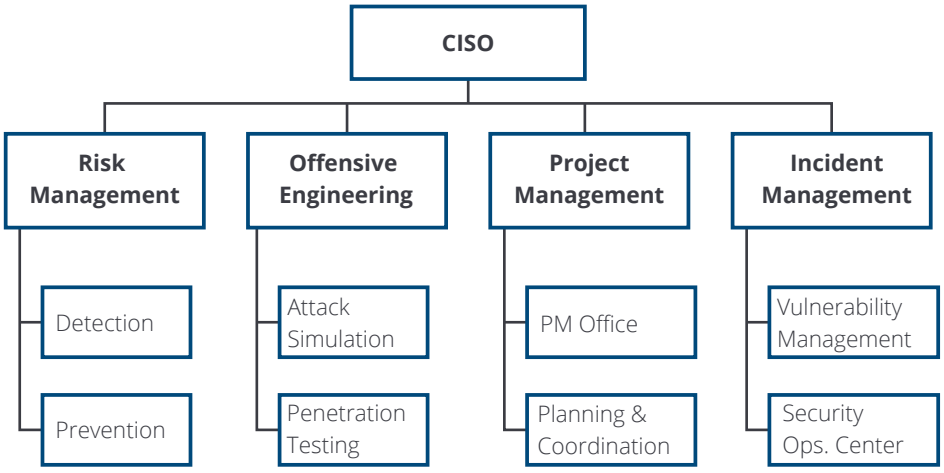
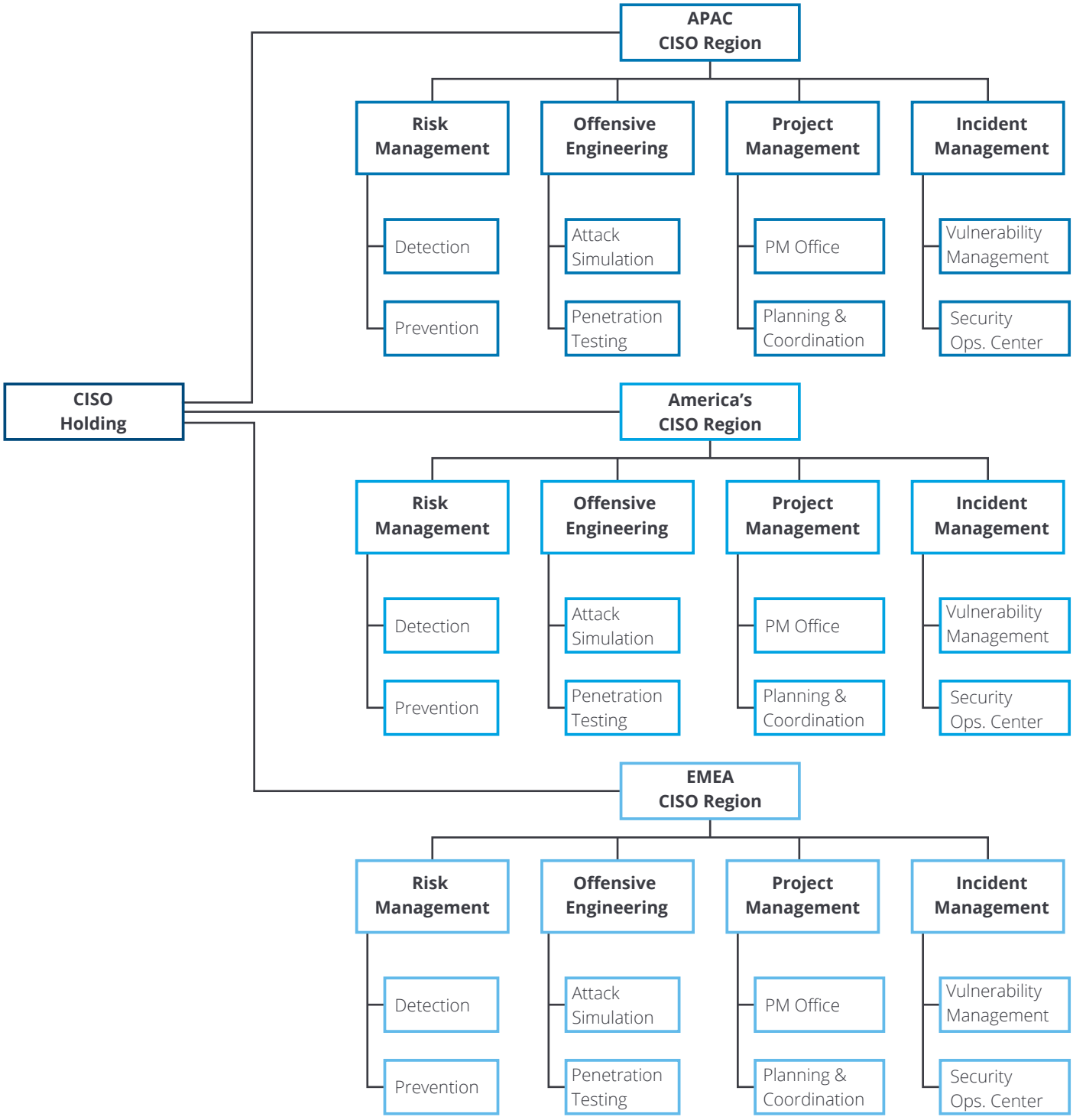
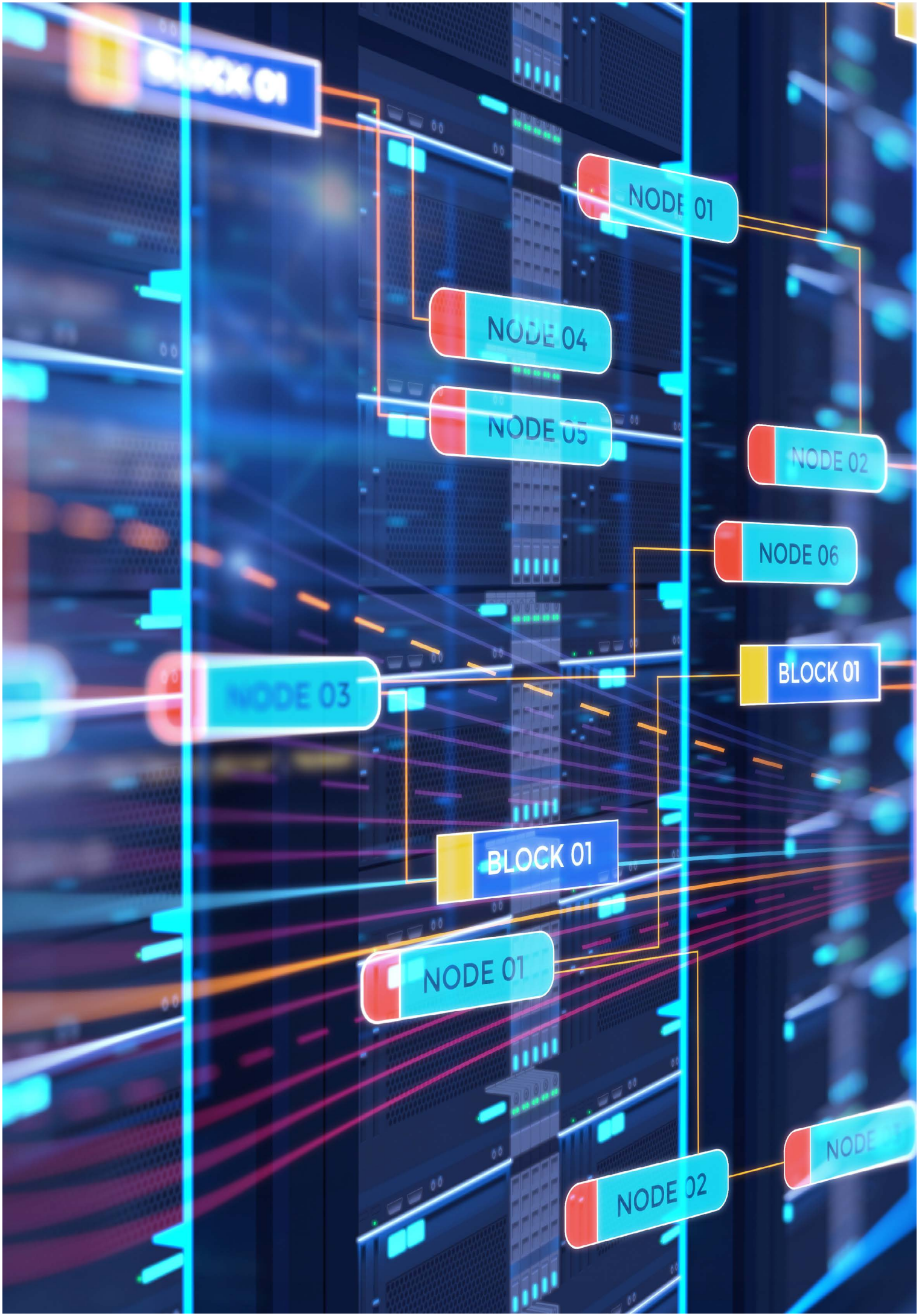


Abb. 3 – C.) Fokus: Geografie




NODE 01
NODE 04
NODE 05
NODE 02
NODE 06
NODE 03
BLOCK 01
BLOCK 01
NODE 01
NODE 02

Wie viel Igel steckt im CST?

In welcher Form unterstützen die aufgeführten Archetypen von CISO-Bereichen und ihren CSTs die charakteristischen Eigenschaften der Arbeitsweise von Hackern, um diese für sich zu nutzen und davon zu profitieren?

Dazu haben wir diese charakteristischen Eigenschaften zusammengestellt und mit den Archetypen dahingehend verglichen, ob sie sich dazu eignen, diese in die eigene Arbeit eines CST zu integrieren oder es potenziell unterstützen zu können.

Tab. 1 – Matrix requisiter Fähigkeiten

Eigenschaft	Definition	A	B	C
Autonomie (dezentral)	Mitarbeitende und CSTs sind frei, ihren Fähigkeiten, Kompetenzen und Kenntnissen entsprechend eigenständig und selbstorganisiert zu handeln.	Nein	Nein	Nein
Agilität	Individuelle Mitarbeitende und ihre Kollegen in den CSTs können die Handlungs- und Kooperationsweise und die benötigten Kompetenzen den sich verändernden Anforderungen, Einflüssen und Ereignissen anpassen.	Ja	Ja	Ja
Resilienz	Die verfügbare Kapazität an qualifizierten Mitarbeitenden und Ressourcen ist ausreichend, um über einen längeren Zeitraum in einer extremen Belastungssituation handlungsfähig zu bleiben und dieser zu begegnen.	Nein	Nein	Nein
Redundanz	Der CISO-Bereich verfügt über einen „doppelten Boden", der bestehende Fähigkeiten und Leistungen der Mitarbeitenden und CSTs auffängt, falls diese in Überlastsituationen, bei Attacken, Erkrankungen etc. ausfallen.	Nein	Nein	Ja
Transparente und offene Kommunikation	Alle Mitarbeitenden stellen einander alle Fakten und Erkenntnisse uneingeschränkt zur Verfügung, begegnen sich offen und respektvoll, geben sich wertschätzendes Feedback und sichern somit ein psychologisch sicheres Kooperationsumfeld.	Ja	Ja	Ja
Liquid Leadership	Je nach Anwendungsfall oder Typ des Cybersecurity-Ereignisses ist das jeweils kompetenteste oder mit dem Ereignis thematisch vertrauteste CST in der Lead-Rolle und gibt allen einzubeziehenden Teams und Experten Orientierung über die Sachlage, den Stand der Triage, die Identifikation der Attack Vectors und die Vorgehensweise.	Nein	Nein	Nein
Liquid Cooperation	Dem Cybersecurity-Ereignis entsprechend setzen sich die benötigten und fachlich qualifiziertesten CSTs und Mitarbeitenden spontan in einer adäquaten Kooperationsstruktur zusammen und organisieren sich untereinander nach dem Liquid-Leadership-Prinzip.	Ja	Ja	Ja
Feedback und Learning Loops	Fakten und Erkenntnisse werden konsequent und regelmäßig über etablierte oder institutionalisierte Kooperationselemente verfügbar gemacht, um Lernerfahrungen über direkte Kommunikationswege in der Organisation bereitstellen zu können und verwertbar zu machen.	Nein	Nein	Nein

Die Elemente Agilität, transparente und offene Kommunikation sowie das Konzept der Liquid Cooperation sind durchaus auch in den aufgeführten Archetypen operationalisierbar. Sie können in verschiedenen Unternehmen beobachtet werden. Die Fähigkeit, sich den wechselnden Anforderungen und Ereignissen im Kontext von Cybersecurity anzupassen und damit agil vorzugehen, ist für CISO-Bereiche eine größere Selbstverständlichkeit als für jeden anderen Bereich eines Unternehmens. Die Dynamik von Cybersecurity-Events fordert zwingend ein Mindestmaß an Agilität zusätzlich zur gegebenen Flexibilität. CISO-Bereiche neigen dennoch dazu, eine Vorgehens- und Kooperationsstruktur zu etablieren und diese im Falle eines Cybersecurity-Events zu praktizieren. Zu beobachten ist, dass diese vorbereiteten Strukturen im Ernstfall immer dann aufgelöst werden, wenn der Anwendungsfall die Möglichkeiten übersteigt. In derartigen Extremsituationen wird von den Mitarbeitenden automatisch die bestehende Struktur aufgelöst, sozusagen „verflüssigt". Dann ist ein Wechsel in eine Liquid Cooperation zu beobachten. Daher ist es grundsätzlich sinnvoller, die Kooperationsstruktur dem Event entsprechend zu konfigurieren, um im praktischen Einsatz keine Zeit mit Anpassungen und Korrekturen zu verlieren.

Was die Eigenschaft der Redundanz angeht, so ist lediglich die geografisch verteilte und selbstähnliche CISO-Organisation potenziell in der Lage, den Ausfall einer Geschäftsfähigkeit, eines CST oder einzelner Experten aufzufangen und die benötigte Leistung weiter aufrechtzuerhalten. Organisationen der ersten beiden Archetypen weisen durch ihr Design geringe bis keine Redundanzen auf, die im Extremfall genutzt werden könnten. Sie sind schließlich auf wirtschaftliche Effizienz ausgerichtet. Redundanzen, selbst im CISO-Bereich, werden hier als Kostenfaktoren bewertet, die es zu vermeiden gilt.

Vergleichbar verhält es sich mit der Eigenschaft der Resilienz. Auch diese wird aus ökonomischen Gesichtspunkten möglichst vermieden und als Nachteil bewertet. Das führt meist zu Überlastungserscheinungen der Mitarbeitenden in den CSTs und verursacht beispielweise Überstunden, einen erhöhten Krankenstand oder sogar Mitarbeiterfluktuation. Eine ganzheitliche Analyse dieser Wirkungen durch eine rein effizienzorientierte Kostenausrichtung hingegen wird in Unternehmen selten durchgeführt, um die Relevanz von Resilienz im Unternehmen zu priorisieren.

Autonomie und Liquid Leadership sind in den beschriebenen Archetypen nicht oder nur selten anzutreffen, da hierarchisch ausgerichtete Organisationsdesigns davon geprägt sind, die Entscheidungsautorität und die Orientierungsverantwortung im Ereignisfall alleinig bei den Führungskräften anzusiedeln. Diese Konzentration ist wirtschaftshistorisch nachvollziehbar, stellt im Kontext der hohen Dynamik von Cybersecurity-Events allerdings eine kritische Limitierung der Handlungsoptionen und Reduzierung notwendiger Entscheidungsgeschwindigkeit dar.

Feedback und Learning Loops sind in allen Unternehmen und vor allem in CISO-Bereichen ein immer wichtiger werdendes Thema. Sie werden stärker als Wert an sich verstanden. Was den Austausch von Erkenntnissen und den Aufbau von Cybersecurity-relevantem Wissen angeht, fokussieren sich diese Themen überwiegend auf die speziellen Zuständigkeiten innerhalb des CISO-Bereichs. Erkenntnisse und Wissen zu Cybersecurity im gesamten Unternehmen aufzubauen, wird vor allem als Kommunikationseinbahnstraße über Schulungen, Online-Seminare oder Kommunikationsmaßnahmen wie E-Mail-Rundschreiben und Newsletter praktiziert.

Um das Wissen über IT-Sicherheit, die Sensibilisierung für Cyberattacken und das Bewusstsein der Mitarbeitenden unternehmensweit zu fördern, sind Interaktion und Kommunikation zwischen dem CISO-Bereich und den übrigen Unternehmensteilen notwendig – auch bzw. vor allem in global agierenden Unternehmen. Hierbei ist die Rückkopplung für den CISO besonders relevant, um nachvollziehen zu können, welchen Reifegrad das Wissen und die Verhaltensweisen aller Mitarbeitenden aufweisen. So können konsequent und für die Mitarbeitenden anschlussfähig Informationspolitik und Schulungsvorgehen geplant und umgesetzt werden.

Kybernetik für das Design einer High-Responsive-Cybersecurity-Organisation

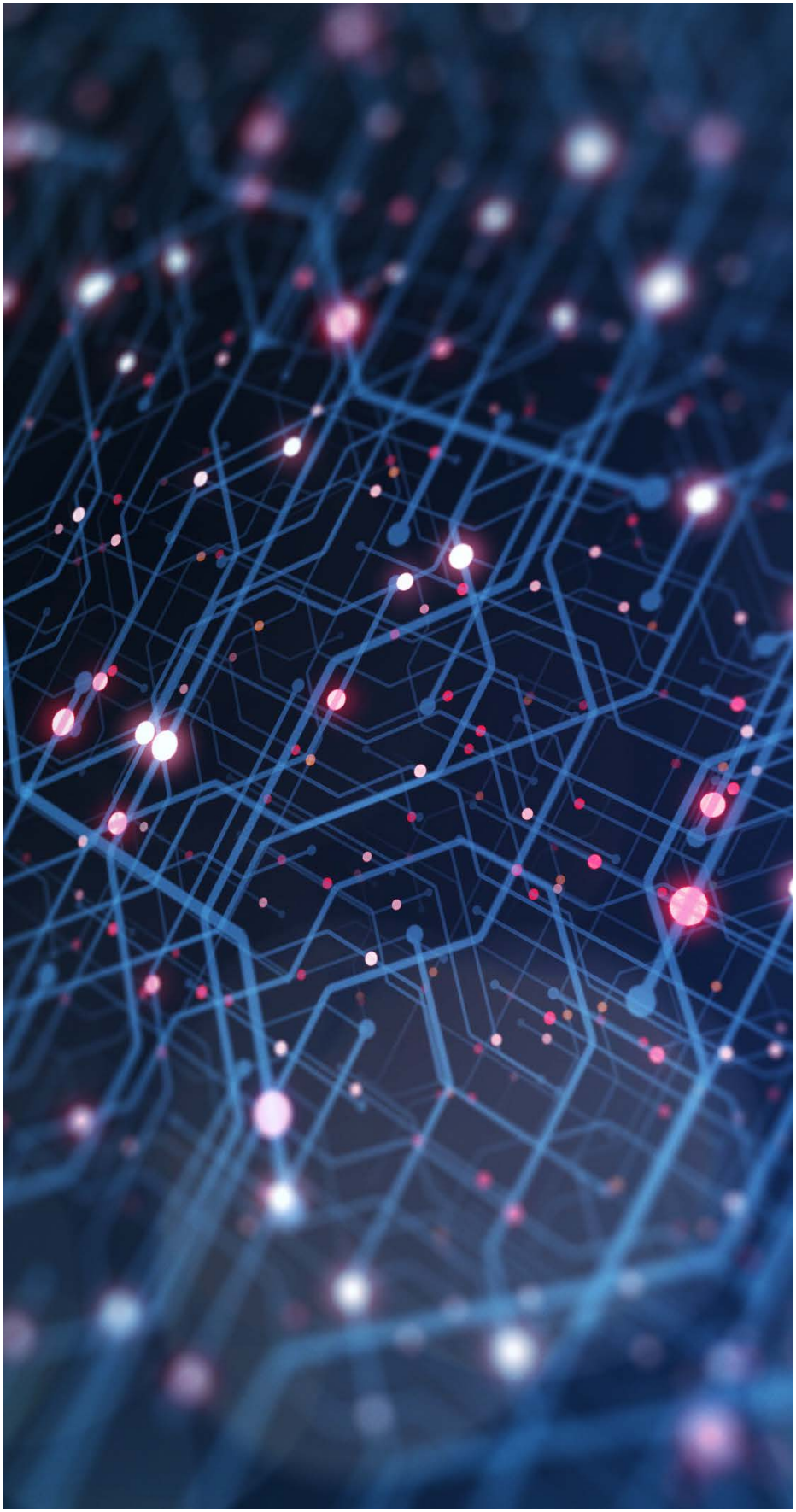
Für das Design eines CISO-Bereichs mit all seinen Teams und Geschäftsfähigkeiten kann man sich die Erkenntnisse der Kybernetik zur Funktionsweise komplexer Systeme zunutze machen. Dazu sollte man sich von der klassischen Arbeitsteilung hierarchisch geprägter Organisationsmodelle verabschieden. Als Denkmodell ist es sehr hilfreich, den Begriff der „Zuständigkeit" für fachliche Inhalte oder für Entscheidungen durch den des „Beitrags" zu ersetzen. In einem komplexen System ist immer ausschlaggebend, welchen Beitrag ein einzelnes Element leistet, um eine spezielle Eigenschaft oder Fähigkeit aufzubauen oder sicherzustellen.

Als Analogie bietet sich der menschliche Organismus an. Er besteht aus einer Vielzahl von Bestandteilen, die über neuronale und hormonelle Kommunikationswege miteinander interagieren. Jedes dieser Organe, inkl. des Gehirns, leistet einen spezifischen Beitrag zur Entwicklung und Existenzsicherung des komplexen Gesamtsystems Mensch. Fragen wie z.B. wer hier das Sagen hat oder wer „wichtig" ist, sind völlig irrelevant. In der Interaktion von Unternehmensorganisationen sind diese Fragen allerdings weit verbreitet und werden mit hohem Aufwand behandelt.

Davon sollte man sich lösen, bevor man sich auf den Beitrag der einzelnen Elemente fokussiert und damit das Design des Organisationsmodells sachlich auf seine Handlungs-, Anpassungs- und damit Existenzfähigkeit ausrichtet. Letzteres ist vor allem im Kontext der CISO-Bereiche und der Unternehmen, für die sie verantwortlich sind, besonders relevant.

Um das Design eines CISO-Bereichs zu entwerfen, empfehlen sich der Imperativ von Heinz von Förster sowie das Viable System Model (VSM) des britischen Managementkybernetikers Stafford Beer.

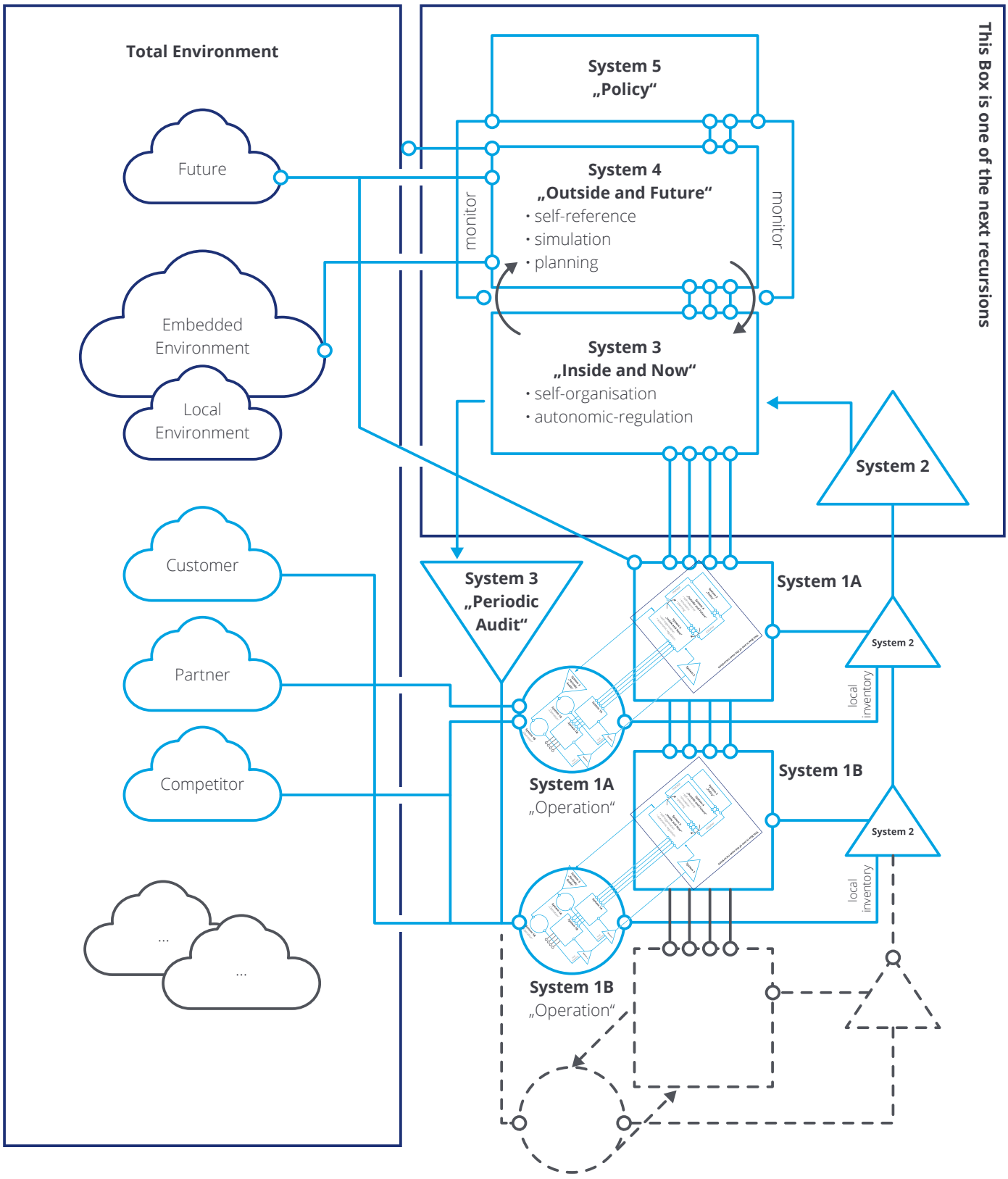
In seinem ethischen Imperativ, den Heinz von Förster an den Kant'schen Imperativ anlehnte, heißt es: „Handle stets so, dass die Anzahl der Wahlmöglichkeiten größer wird!" Dies lässt sich als grundsätzliches Designprinzip für CISO-Bereiche und alle darin zusammengefassten CSTs nutzen. Es ist sicherzustellen, dass jeder Bestandteil der Organisation, jedes Team und jede Fähigkeit so geplant und angewendet werden, dass das Portfolio der Handlungsoptionen, wenn es zu einem Cybersecurity-Event kommt oder davor geschützt werden soll, kontinuierlich erweitert wird. An der bei den Archetypen erwähnten Fokussierung auf ökonomische Effizienz im CISO-Bereich wird deutlich, dass sie Handlungsoptionen limitiert und nicht erweitert.



Stafford Beer hat Mitte der 1970er-Jahre sein VSM entwickelt und in der wirtschaftlichen Praxis validiert. Damit lässt sich eine Funktions- und Interaktionsweise für eine Organisation entwerfen, die komplexe, also unvorhersehbare Entwicklungen und Ereignisse, selbstverständlich verarbeiten kann. Zusätzlich ermöglicht das VSM, die vorher aufgeführten Eigenschaften wie Autonomie, Agilität, Redundanz oder transparente Kommunikation vollständig abzudecken und sicherzustellen.

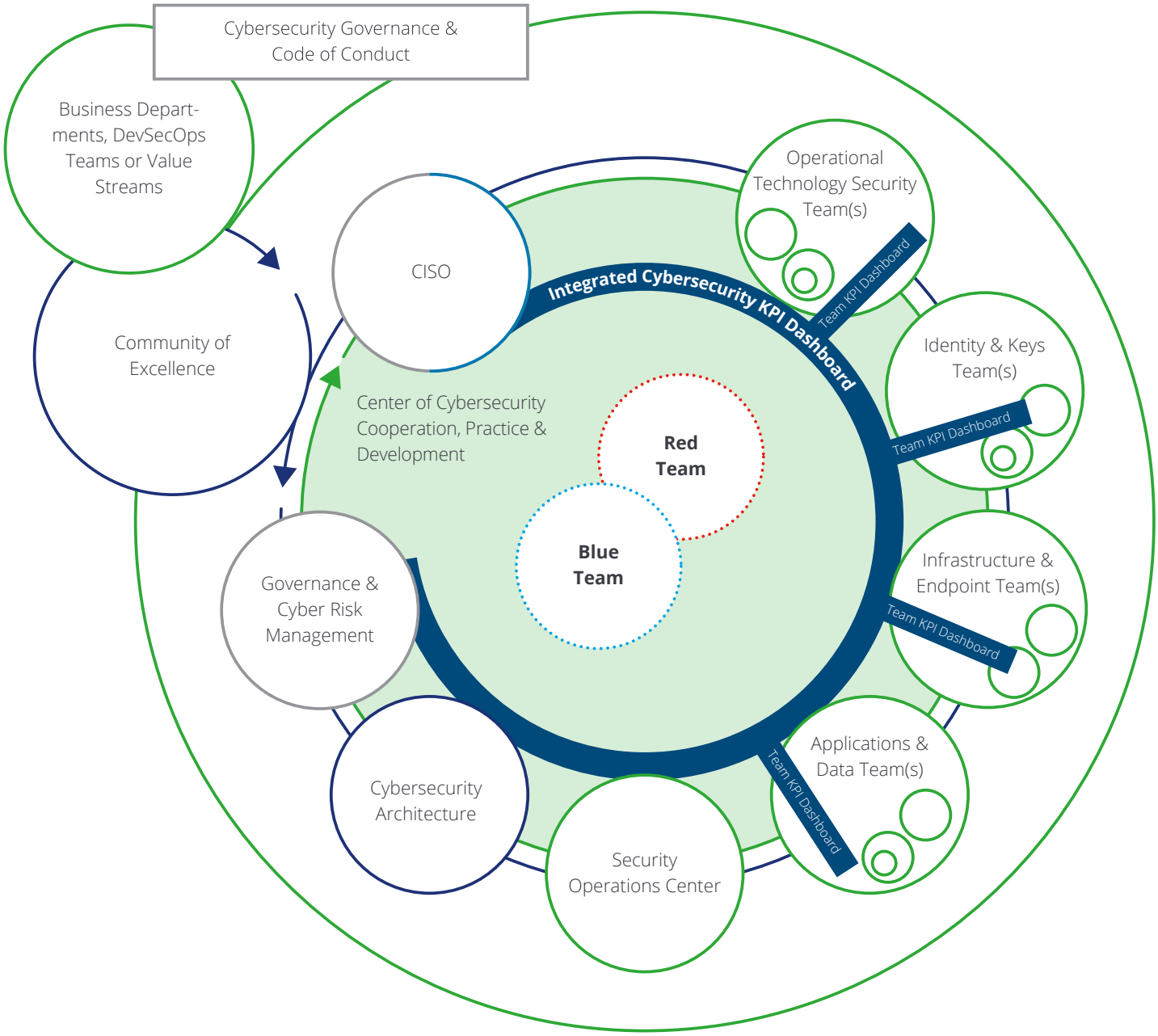
Für das Design eines VSM-basierten CISO-Bereiches wird die Darstellung nicht auf die eigenen CSTs limitiert, sondern um wesentliche Elemente ergänzt. Diese erlauben es, die Kooperationsgrundlage sowie die Kommunikationsinhalte und -wege innerhalb der eigenen Organisation und der übrigen Unternehmensbereiche zu erkennen. Die Elemente eines kybernetischen Organisations- und Kooperationsmodells für CISO-Teams werden im Folgenden in einer Gesamtsicht sowie in kurzen Beschreibungen dargestellt.

Abb. 4 – Viable System Model



Quelle: Viable System Model, Die agile Organisation, Andreas Slogar, Hanser, 2018, 2020

Abb. 5 – Kybernetisches Organisations- und Kooperationsmodell für CISO-Teams auf der Grundlage des Viable System Model



Cybersecurity Governance & Code of Conduct

Fundament und zentraler Orientierungspunkt der gesamten Kooperation und Interaktion für alle Akteure und Teams des gesamten Unternehmens sind Cybersecurity Governance & Code of Conduct. Hier werden Relevanz und Nutzen von Cybersecurity für das Unternehmen beschrieben und welche Qualität und Form der Zusammenarbeit sowie des individuellen Verhaltens aller Mitarbeitenden berücksichtigt werden müssen. Dies bildet das Fundament für den Beitrag und die Verantwortung, die jeder Mitarbeitende trägt, und für eine autonome und selbstorganisierte Kooperation in allen Belangen der Cybersecurity im individuellen und kollektiven Kontext.

Von diesem Ausgangs- und Bezugspunkt ausgehend werden die individuellen Ausprägungen von spezifischen Codes of Conduct der CSTs abgeleitet. Durch diesen Mechanismus wird ersichtlich, dass ein direkter Bezug zwischen übergreifender Regelung und individueller Umsetzung im Kontext einer Teamvereinbarung besteht. So kann verhindert werden, dass die allgemein verbindliche Regel zu einem bürokratischen, abstrakten, bedeutungs- und konsequenzlosen Überbau verkommt. Über eine regelmäßige Prüfung der Angemessenheit und Anwendbarkeit bleiben Cybersecurity Governance & Code of Conduct lebendige und praxisnahe Definitionen, die an notwendige Veränderungen angepasst werden.

Im Rahmen regelmäßiger Governance Sessions organisieren CISO und das CST Governance & Cyber Risk Management als Moderatoren den Entwicklungsprozess und stellen sicher, dass allen beteiligten und betroffenen CSTs und Akteuren die notwendigen Rahmenbedingungen zur Verfügung stehen, um die geltenden Vereinbarungen anzuwenden und durchzusetzen.

Die Rolle des CISO wandelt sich von einem technischen Experten in seinem Zuständigkeitsbereich zu einem Kommunikationsexperten, der für eine reibungslose Kooperation zwischen den technischen Experten sorgen muss.

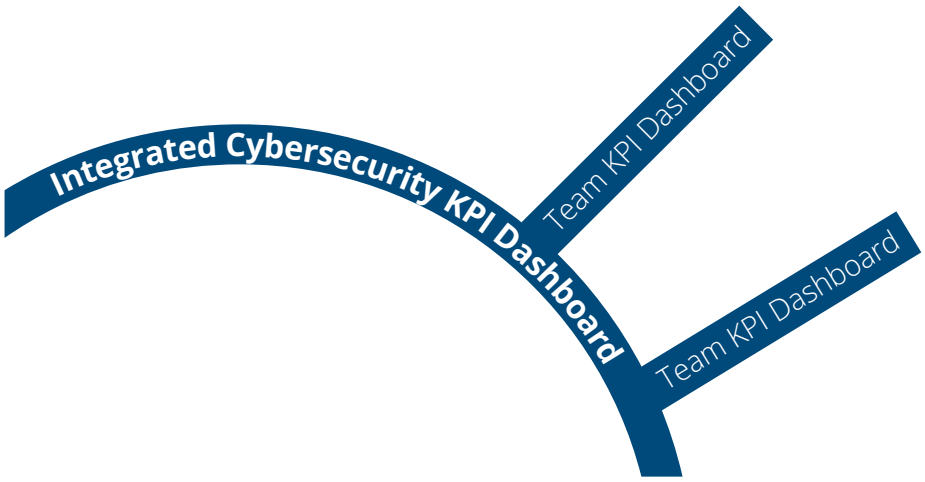
Dreh- und Angelpunkt der Kooperation und Kommunikation aller CSTs im CISO-Bereich sind die KPI-Boards auf Team- und aggregiert auf Gesamtebene. Alle Beteiligten und Betroffenen im CISO-Bereich haben prinzipiell die Möglichkeit, die Inhalte der Dashboards einzusehen und sich direkt über die Cybersecurity-Situation des Unternehmens zu informieren. Durch diese Transparenz von Zahlen, Daten und Fakten können die CSTs ihre individuelle Leistung mit der anderer Teams vergleichen, sich gegenseitig unterstützen und einen kontinuierlichen Erfahrungs- und Kenntnisaustausch fördern.

Durch einen Peer-Group-Vergleich der CSTs untereinander kann ein sportlicher Wettstreit über das höchste Leistungsniveau oder den weitesten Reifegrad ausgelöst werden. Dabei sollten der CISO und das CST Governance & Cyber Risk Management darauf achten, dass dieser Wettbewerb keine Dysfunktionalitäten oder Konflikte verursacht.

Die nachfolgende Darstellung von Strukturierung und Inhalten eines Dashboards auf Ebene des CST soll als Anregung im Kontext dieses Artikels verstanden werden. Sie enthält die Empfehlungen und Erfahrungen der Co-Autoren.

Bei Design und Konfiguration der CST-Dashboards und der darin enthaltenen Informationen ist zu beachten, dass auf der übergreifenden Rekursionsebene des CISO-Bereichs die vollständige Integration und Aggregation sichergestellt bleiben. Nur so können Abhängigkeiten und notwendige Kooperationen der CSTs untereinander, beispielsweise zur Analyse und Bearbeitung erkannter Angriffsvektoren, jederzeit identifiziert, kommuniziert und koordiniert werden.

Abb. 6 – KPI Dashboard



Tab. 2 – Beispiele für Kennzahlen

KPIs*
Erreichter vs. notwendiger Reifegrad
Health Indicators abhängig von Angriffsvektoren
Hackability Score

Tab. 3 – Beispiele für Controls

Action Backlog*	**Backlog**	**WIP**	**Completed**
Preventive controls	1	2	16
Protective controls	8	3	22
Corrective controls	6	2	9

* Beispiele lediglich exemplarisch und nicht vollständig oder erschöpfend.

Bevor auf die Ebene der CSTs eingegangen und die Arbeitsweise der Teams auf der Grundlage der bisherigen Aussagen und Prinzipien beschrieben wird, geht es nun um die operative Anwendung des VSM. So wird nachvollziehbar, wie CSTs ihre strategische und operative Planung sowie Arbeit darüber strukturieren, organisieren und kommunizieren können.

Hierfür werden die folgenden sechs Bausteine[1] des VSM benötigt, aus denen jedes einzelne Element des Designs einer CISO-Organisation konfiguriert wird. Die Bausteine definieren in ihrer Kombination die Qualität und Ausprägung der einzelnen Elemente wie eines CST oder beispielweise der Community of Practice.

Mit diesen Bausteinen können die operativen Anwendungsfälle kommunikativer oder planerischer Tätigkeiten modelliert und in Form von selbstorganisierter Kooperation realisiert werden. Über Steckbriefe, die über vorhandene Wiki- oder Kanban-Tools im Unternehmen veröffentlicht werden, können sich Mitarbeitende über die Aufgabenstellung eines CST informieren, Ansprechpartner unmittelbar finden und kontaktieren oder den aktuellen Arbeitsschwerpunkt und -fortschritt des Teams einsehen.

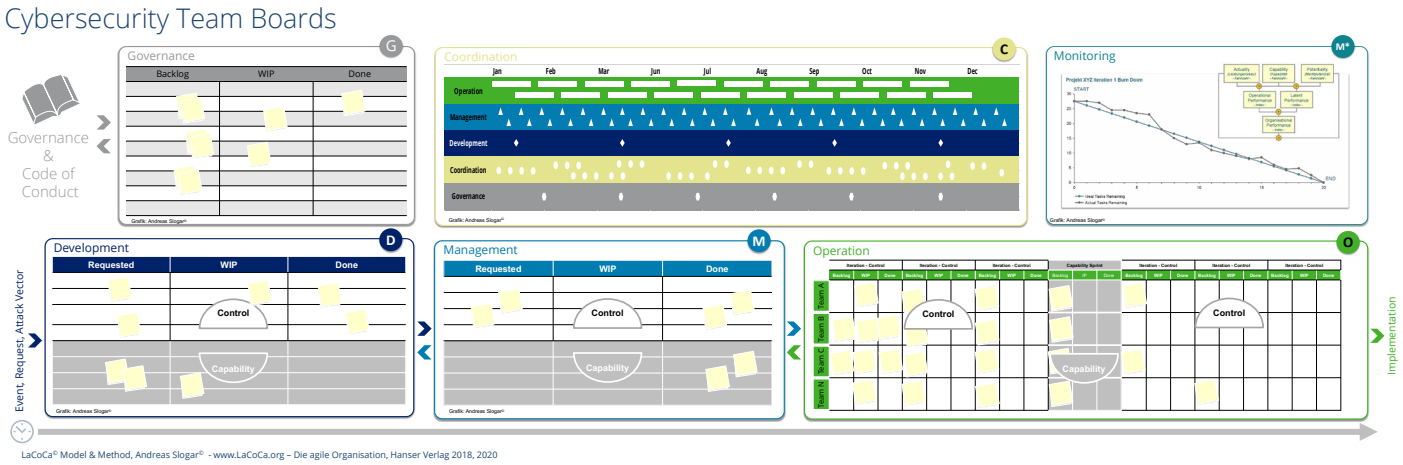
Ein derartiger Steckbrief kann als Zusammenstellung von Kanban-Boards konfiguriert sein, die eine integrierte Übersicht mit allen operativen und geplanten Tätigkeiten entlang der vorgenannten Bausteine bereithält.

Tab. 4 – Bausteine des Viable System Model

Baustein	Erläuterung
Operation O	• Durchführung einer operativen Cybersecurity-Funktion (z. B. Identity und Access Management, Data Security, Threat Analysis, Forensic oder Incidence Response) • Erbringung operativer Arbeit als Experte oder in Teams
Development D	• Identifikation und Analyse zukünftiger Cybersecurity-Entwicklungen, -Trends und -Technologien, externer Anforderungen und Einflüsse aus der Umwelt oder dem Unternehmen an den CISO-Bereich und seine Leistungen • Maßnahmenableitung zur Entwicklung zukünftig notwendiger Fähigkeiten, Interventionen oder Cybersecurity-Strategien auf Unternehmens-, CISO-Bereichs-, Team- und Mitarbeitendenebene
Governance G	• Sicherstellung von Sinn, Zweck und Identität der CISO-Organisation, seiner Teams und Mitarbeitenden • Erarbeitung und Einhaltung von Regeln der Zusammenarbeit und regulatorischen Vorgaben durch z. B. Code of Conduct und Richtlinien
Management M	• Bereitstellung organisatorischer und operativer Rahmenbedingungen für die Leistungserbringung und -entwicklung im CISO-Bereich • Bereitstellung notwendiger Ressourcen für die Erbringung der operativen Teamarbeit (z.B. technologischer Infrastruktur inkl. Software, Tools und Architektur, Budget für Investitionen und Projekte)
Coordination C	• Sicherstellung und Weiterentwicklung der Zusammenarbeit aller Teams innerhalb des CISO-Bereichs, des Unternehmensumfelds und der externen Umwelt • Sicherstellung von Form, Umfang, Qualität und Nachvollziehbarkeit der Informationen der Rollen und Teams untereinander und der Funktionsfähigkeit mit ihrer Umwelt
Monitoring M*	• Kontinuierliche Analyse und Kontrolle der operativen Leistungsfähigkeit aller Teams im CISO-Bereich durch Steuerungsmodell (KPI) • Begleitung aller CISO-Teams in der selbstorganisierten Ableitung von Handlungsmaßnahmen zur kontinuierlichen Entwicklung der Leistungsfähigkeit auf Basis der KPI-Analysen

[1] Bausteine werden im VSM-Systeme genannt und sind in diesem Artikel synonym zu verstehen.

Abb. 7 – Cybersecurity Team Boards



Der Steckbrief kann die bereits beschriebenen KPI-Dashboards enthalten oder sie können als zusätzliche Detaillierungsebene separat veröffentlicht werden. Die jeweilige Konfiguration ist vom jeweiligen CISO-Bereich, seinen CSTs sowie dem internen und externen Informations- und Kooperationsbedarf abhängig. In jedem Fall ist auch dieser Steckbrief in Form eines Cybersecurity Team Board in seinem Design und seiner Struktur so aufzubauen, dass eine übergreifende Aggregation auf der nächsten Rekursionsebene des CISO-Bereichs automatisiert möglich ist.

Die konsequente Nutzung von Cyber Boards in allen Teams und Communities ermöglicht eine nahtlose, transparente und skalierbare Orchestrierung der Kommunikation und Zusammenarbeit aller Mitarbeiter, Manager, Stakeholder und Kooperationspartner.

Damit alle Non-Cybersecurity- und Cybersecurity-Teams gleichermaßen im gesamten Unternehmen direkt in den Know-how-Aufbau und die Sensibilisierung aller Mitarbeitenden zu den Notwendigkeiten und dem Nutzen der IT-Sicherheit informiert und geschult werden, ist eine Community of Excellence (CoE) ein empfehlenswertes Designelement.

In einer CoE für Cybersecurity ist es den Learning-and-Development-Experten aus dem HR-Bereich möglich, in enger Zusammenarbeit mit dem CST Governance & Cyber Risk Management optionale und verpflichtende Schulungsformate für alle Mitarbeitenden zu entwickeln und durchzuführen.

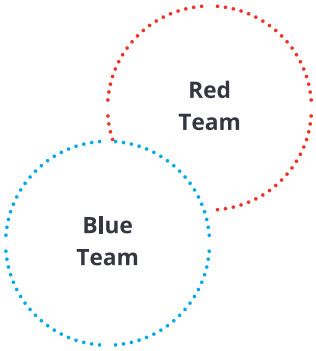
Über diesen Weg wird nicht nur der kontinuierliche Austausch zwischen CISO-Bereich und allen Mitarbeitenden institutionalisiert und gefördert, sondern auch den regulatorischen Anforderungen und der Entwicklung des organisationsweiten Reifegrads zum Umgang mit Cybersecurity-Belangen entsprochen.

Um einen konsequenten und konsistenten Informationsfluss und Erkenntnisaustausch zwischen allen CSTs zu fördern und sicherzustellen, empfiehlt sich das Etablieren eines Center of Cybersecurity Cooperation, Practice & Development (3CPD) für alle Mitarbeitenden des CISO-Bereichs. Unter der Moderation des CISO oder des CST Governance & Cyber Risk Management werden z.B. die aktuelle Bedrohungslage, die individuellen Planungen der CSTs sowie die Ergebnisse der bisherigen Red-Team- vs. Blue-Team-Manöver erörtert und die interdisziplinäre Zusammenarbeit koordiniert.

Innerhalb des 3CPD können unterschiedliche Kooperationsformate genutzt werden, die dem jeweiligen Informations- und Abstimmungsbedarf der CSTs und des CISO entsprechen. Neben Daily Stand-ups, wie sie in der inkrementellen Softwareentwicklung praktiziert werden, können Lagebesprechungen, Peer-Reviews oder Reverse Presentation Sessions geplant und durchgeführt werden.

Ein 3CPD ist als Informationsdrehscheibe oder -Hub zu verstehen, damit ein möglichst enger Informationsaustausch sichergestellt und einer Silobildung der CSTs untereinander entgegenwirkt wird. Außerdem werden durch die direkte Interaktion im Rahmen des 3CPD Informationsverluste und Fehlerquellen für Missverständnisse durch rein digitale bzw. schriftliche Kommunikation kompensiert oder vermieden. Selbstverständlich können 3CPDs nötigenfalls als Videokonferenz über die gängigen IT-Tools durchgeführt werden.

Das dritte und relevanteste Argument für das Etablieren eines 3CPD ist, dass übergreifende Lösungen für z.B. identifizierte Angriffsvektoren best- und schnellstmöglich bearbeitet und abgewehrt werden können, wenn eine enge Zusammenarbeit und möglichst reibungslose Kommunikation der Mitarbeitenden aller CSTs existiert.



Alle bisher eingeführten und dargestellten Bausteine eines CISO-Bereichs bilden den Rahmen, um ein letztes, aber existenzielles Element zu ergänzen. Es bildet den wesentlichen Unterschied, um aus dem ungleichen Wettkampf zwischen Hase und Igel zu entkommen oder zumindest den Hackern einen Schritt voraus zu sein. Wie eingangs festgestellt, ist es ein wesentlicher Erfolgsaspekt, zu versuchen, sich in die Denk- und Arbeitsweise von Hackern zu versetzen. Eine probate und weit verbreitete Methodik hierfür ist die möglichst realitätsnahe Simulation von Hacker-Attacken. Dabei werden aus den Mitarbeitenden der CSTs zwei Teams gebildet. Das Red Team versetzt sich in die Perspektive der Hacker und sucht systematisch, aber ohne Vorankündigung nach Lücken auf allen Ebenen und in allen CIs der IT-Architektur und IT-Infrastruktur. Das Blue Team hat die Aufgabe, Attacken zu erkennen sowie wirksame Gegenmanöver zu entwickeln und umzusetzen. Diese Form der Übung realer Bedrohungsszenarien ist dem Vorgehen des militärischen Bereichs entlehnt.

Relevant sind diese Manöver vor allem, weil sie die bestmögliche Plattform dafür bieten, die Mitarbeitenden der CSTs konsequent zu befähigen, die ihnen übertragene Entscheidungsautorität im Ernstfall auch souverän auszuüben. Je geringer die Verzögerungen sind, die durch Autorisierungsrückfragen oder Umsetzungsunsicherheiten entstehen, desto kürzer ist die Reaktionszeit und umso höher fällt der eigene Wirkungsgrad der Vorgehensweise im Falle einer Hacker-Attacke aus.

Die Ergebnisse und Erkenntnisse aus den Manövern der Teams Red und Blue sind durch Review-Sessions übergreifend auszuwerten und im Rahmen der Community of Excellence als Know-how-Entwicklung zu nutzen. Ergeben sich Erkenntnisse zu identifizierten Schwachstellen der IT-Landschaft, so können diese direkt von allen CSTs als Input für die Planung und Umsetzung spezifischer Kontrollmechanismen im jeweiligen Themengebiet genutzt werden.

Darüber hinaus können aufgetretene Zeitverluste durch unklare Vorgehensweisen, widersprüchliche oder sich überschneidende Zuständigkeiten oder Unsicherheiten bei Entscheidungspunkten, die im Laufe eines Manövers auftreten, beispielweise direkt in die Anpassung der Governance und des Code of Conduct auf Ebene des CISO-Bereichs oder der einzelnen CSTs einfließen.

Fazit

Das Design eines CISO-Organisationsmodells mithilfe der hier auszugsweise und in vereinfachter Form verwendeten Prinzipien und Werkzeuge der Kybernetik ermöglicht nicht nur die Darstellung des Organigramms bestehender CSTs. Es reichert es um die Kooperationsformen, die wichtigsten Kommunikationswege und -inhalte sowie um die Integration des gesamten CISO-Bereichs in die Unternehmensumwelt der Non-Cybersecurity-Bereiche an.

Auch wenn die Darstellungen in diesem Artikel nicht vollumfänglich sein können, so sind die Impulse sicherlich dazu geeignet, das bestehende, klassische und sehr verbreitete Verständnis von Design und Kooperationsmodell eines CISO-Bereichs zu hinterfragen. Sie können weiterentwickelt werden, um im Wettlauf mit Hackern eher die Cleverness des Igels zu nutzen, anstatt immer mehr Aufwand und Energie aufzubringen wie der Hase und letztlich doch an sich selbst und den Herausforderungen der Cybersecurity zu verzweifeln.

Antifragilität im Web3: eine kybernetische Sichtweise

Yip Thy-Diep Ta | Unit Network

Yip Thy-Diep Ta ist Gründerin bei Unit Network, einer Blockchain für die Token-Ökonomie. Mit ihren Initiativen DLT-Talents, Unit Masters und H.E.R. Dao bietet sie kostenfreie Ausbildungsprogramme und Stipendienprogramme zur Förderung der Chancengerechtigkeit in Web3. Yip ist Gründerin bei der Genossenschaft Balanced Being, welche Achtsamkeitstrainings für Unternehmen anbietet. Sie ist Autorin des Buches „Beautiful Brains change tomorrow... today" und hat mehrere Auszeichnungen als eine der einflussreichsten Frauen in Blockchain erhalten. Zuvor war sie als Beraterin bei McKinsey & Co. tätig.

Eine der wichtigsten Herausforderungen unserer Zeit ist der Umgang mit den Nebenwirkungen von Globalisierung und Konnektivität. Die Welt wird immer unberechenbarer. Wie können wir die Folgen der Globalisierung und der Vernetzung am besten angehen? Wie können wir der zunehmenden Häufigkeit von sogenannten Black-Swan-Ereignissen begegnen? Hier empfiehlt sich eine kybernetische Betrachtungsweise – weg von linearen Ursache-Wirkungs-Modellen hin zu zirkulären Modellen, in welchen interdependente Beziehungen vorherrschen.

Sich als Teilnehmer an zukünftigen Ökosystemen zu betrachten, ermöglicht es, die eigenen Auswirkungen zu erfassen und diese Informationen in die kontinuierliche Entwicklung antifragiler Systeme einzubeziehen. Diese Systeme werden durch die Entscheidungsfindung von Individuen geformt, die wiederum selbst als lebendes System mit ständiger Rückkopplung und Wachstum existieren. Menschen sind selbst Teil der Natur. Achtsamkeit ist eine kritische Kompetenz für den Aufbau von systemischer Antifragilität.

Ein interessanter Anwendungsfall ist Web3, das Internet der Werte (Internet of Value). Digitale Vermögenswerte (Kryptowährungen), die zugrundeliegenden Distributed-Ledger-Technologien (Blockchains) und die neuen Formen der Zusammenarbeit (dezentrale autonome Organisationen) schaffen einen fruchtbaren Boden für die Entstehung antifragiler Systeme.

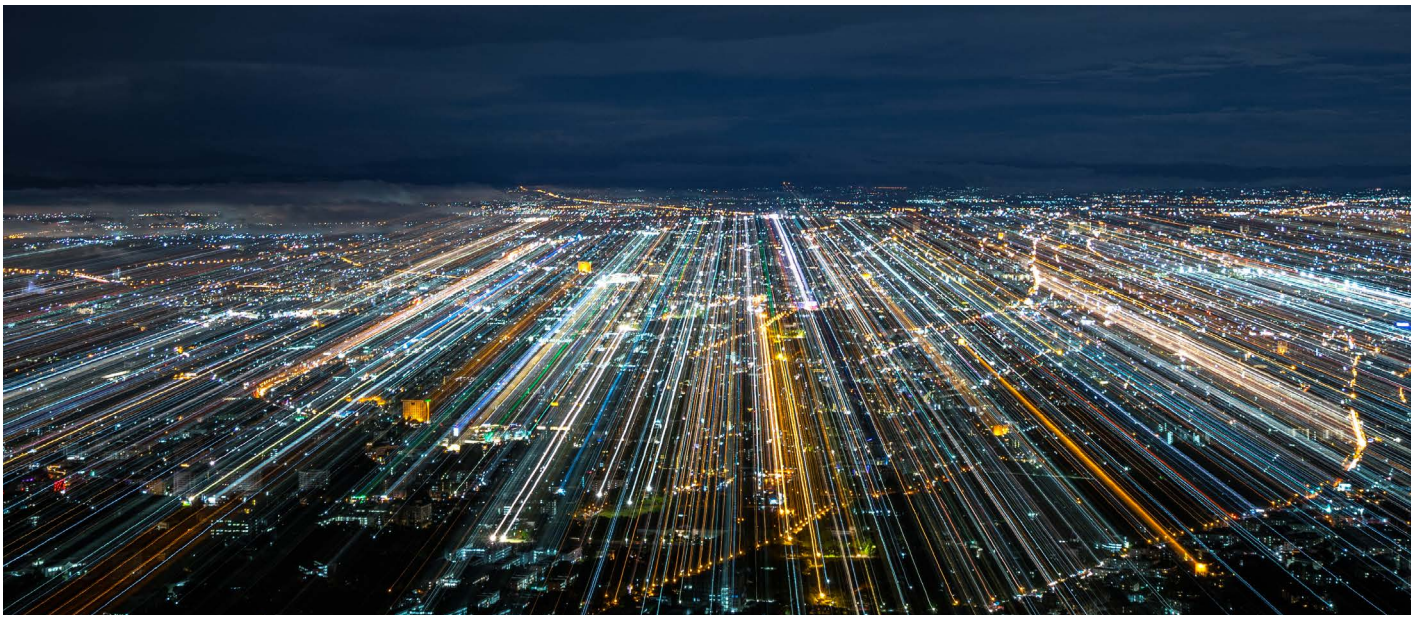
Was kann man in einer Welt tun, die man nicht versteht?

Der technologische Fortschritt und die Globalisierung haben – bei allen Vorteilen, die sie mit sich gebracht haben – zu komplexen Systemen voller gegenseitiger Abhängigkeiten geführt, die mit zunehmender Größe der Systeme immer schwieriger zu erkennen sind. Diese Interdependenzen führen unbemerkt zu Ketten unvorhergesehener Auswirkungen, die katastrophale Ausmaße annehmen können. In der Zukunft werden wir immer häufiger von sogenannten „Schwarzen Schwänen" (Black Swans) heimgesucht werden – unvorhersehbaren, seltenen Ereignissen mit potenziell katastrophalen Folgen.

Anstatt sich darauf zu verlassen, dass alle Interdependenzen in einem System von globalem Ausmaß erkannt und berücksichtigt werden können, sollte die Anfälligkeit für diese katastrophalen Black-Swan-Ereignisse und ihre Auswirkungen eingeschätzt und Systeme aufgebaut werden, in denen Volatilität mehr Bereicherung als Gefahr darstellt. Schließlich kommt es auf die Sensibilität und Schlagfertigkeit gegenüber diesen unvorhersehbaren, seltenen Ereignissen an und nicht auf die Wahrscheinlichkeit des Auftretens dieser Ereignisse.

Antifragilität ist eine Eigenschaft, die einer Situation zugeschrieben wird, in der ein Objekt oder eine Person einen Gewinn oder anderweitig definierte Bereicherung erfährt, die die potenziellen Verluste als Reaktion auf Unbeständigkeit übersteigen. In seinem Buch „Antifragilität: Anleitung für eine Welt, die wir nicht verstehen" stellt der Statistiker und ehemalige Börsenhändler Nassim Taleb die These auf, dass es unmöglich ist, die Wahrscheinlichkeit des nächsten „Schwarzen Schwans" vorherzusagen, und dass vor diesem Hintergrund die optimale Handlungsstrategie darin besteht, sich für das bestmögliche Ergebnis zu positionieren, wenn diese Ereignisse eintreten.

Im Idealfall folgt die Nutzenfunktion einer solchen Handlungsstrategie einem konvexen Verlauf ähnlich einem Smiley, wobei Ereignisse mit der geringsten Wahrscheinlichkeit die größten positiven Auswirkungen auf das System haben. Größere Abwei-



chungen vom erwarteten Mittelwert führen in einem solchen System zu höheren Gewinnen. Antifragilität geht über Robustheit hinaus, da antifragile Einheiten solchen Abweichungen nicht nur widerstehen, sondern sich mit jeder weiteren Abweichung kontinuierlich verbessern.

Taleb schlägt eine bimodale Strategie vor, bei der im Falle seltener negativer Schwarzer Schwäne der Abwärtstrend begrenzt und im Falle seltener und extrem positiver Ereignisse der Aufwärtstrend maximiert wird. Dies sorgt für Robustheit im Falle extremer negativer Schocks und optimiert die Exposition gegenüber vorteilhaften Situationen (positiven Schwarzen Schwänen). Um dem Risiko katastrophaler Ereignisse zu begegnen, werden negative Ergebnisse mit geringen Verlusten als Lernchancen gefördert und tragen zur allgemeinen Gesundheit des Systems bei. Dies führt zur Entwicklung einer systematischen Reaktionsstrategie, die mit jeder weiterer Abweichung von Sollwerten positiv verstärkt in sich selbst zurückfließt. Je mehr Fehler auftreten, desto schneller verbessert sich das System. Es werden kleine Schwachstellen entdeckt, die, wenn sie nicht behoben werden, mit der Zeit zu größeren Schäden führen können. Fehler sind also kein Problem, sondern eine Bereicherung, da sie die Entstehung von größeren Fehlern mit schwerwiegenden Folgen verringern. Durch diese Form der kontinuierlichen Verbesserung lassen sich Schwarze Schwäne zwar nicht ausschalten und auch nicht besser vorhersagen, aber die Überlebenschancen im Falle des Auftretens eines Schwarzen Schwans werden verbessert.

Sobald sichergestellt ist, dass das Risiko des Ruins bestmöglich reduziert ist, ist jede Optimierung, die zu mehr Optionen zur Exposition hinsichtlich positiver Ergebnisse im Sinne der Organisationsziele führt, eine gewinnbringende, sofern die Kosten zur Sicherung der Optionen im Vergleich zu möglichen Auszahlungen vernachlässigbar gering sind. Zusammenfassend lässt sich sagen, dass wir einem System Antifragilität verleihen, wenn wir Folgendes umsetzen:

- Bestmögliche Reduzierung des Risikos des kompletten Ruins
- Entwicklung einer systemischen Reaktionsstrategie, die auf sich selbst zurückwirkt, indem sie eine positive Fehlerkultur ermöglicht
- Erhöhung der Optionalität mit Bezug auf Ereignisse, die hohe Auszahlungen erwarten lassen

Um eine Reaktionsstrategie für ein bestimmtes System zu entwickeln, müssen auch sämtliche Personen als wesentlicher Bestandteil dieses Systems einbezogen werden. Die menschlichen Akteure agieren, das System reagiert, was wiederum die menschlichen Akteure und ihre nächsten Reaktionen beeinflusst – alles in einer ständigen zirkulären Rückkopplungsschleife. Dies ist der Bereich der Kybernetik zweiter Ordnung. Wenn die Reaktionsstrategie den Prinzipien der Antifragilität folgt, wird sie zu einem System der kontinuierlichen Verbesserung zwischen den Bestandteilen des Systems.

Eine kybernetische Sichtweise auf Wirkung und Verantwortung

In der Kybernetik zweiter Ordnung, wie sie von Heinz von Foerster definiert wurde, versteht sich der Beobachter als Akteur in dem von ihm beobachteten System. In dieser Betrachtungsweise wird die objektive Unabhängigkeit des Subjekts vom System aufgehoben: Alle Handlungen der Teilnehmer sind Teil des internen Rückkopplungsprozesses, der bestimmt, wie sich das System entfaltet. Keiner der beobachtenden Akteure kann sich von einer gewissen Verantwortung für die beobachteten Ergebnisse – ob positiv oder negativ – freisprechen. Die Rolle der menschlichen Akteure besteht darin, ihre Interpretation der vom System wahrgenommenen Informationen und ihre Reaktionsstrategien zu wählen.

Wie Viktor Frankl in „Man's Search for Meaning" schrieb, liegt unsere Verantwortung in unserer Fähigkeit, eine Reaktion auf eine gegebene Situation zu wählen – und diese Reaktion schließt die Art und Weise ein, wie wir die Situation selbst wahrnehmen. Unsere Verantwortung liegt darin, unsere Verantwortbarkeit zu erhöhen, das heißt, die Anzahl der Antwortoptionen zu erhöhen. Wir können dies tun, indem wir beispielsweise die Fähigkeit der Wahrnehmung trainieren und uns der Wirkung unserer Handlungen, kurz unserer Mitwirkung im System bewusst werden.

Im Folgenden geht es um Achtsamkeit als die kritische Fähigkeit, mit welcher durch Schärfung der subjektiven Wahrnehmung die Rückkopplungsschleife von handelnden Beobachtern mittels erweiterter Informationsgrundlagen kontinuierlich verbessert und damit die Antifragilität des Systems erhöht werden.

Achtsamkeit: eine kritische Fähigkeit für kybernetische Antifragilität

In den 1970er-Jahren führte der Forscher Jon Kabat Zinn die Achtsamkeit in die westliche Wissenschaftswelt ein. Er definierte sie als „Achtsamkeit, die durch gezielte Aufmerksamkeit im gegenwärtigen Moment entsteht, ohne zu urteilen" (Moore, 2019).

Achtsamkeit ist eine wichtige Fähigkeit, um eine bessere Selbstwahrnehmung zu erlangen und blinde Flecken bei der Entscheidungsfindung zu erkennen. Dies geschieht, indem die Anzahl der Informationsquellen vom intellektuellen, faktenbasierten Verständnis einer Situation auf die emotionale Intelligenz und die verkörperte Intuition ausgeweitet wird.

In den letzten Jahren haben Organisationen damit begonnen, Achtsamkeitstrainings einzuführen, um die Leistungsfähigkeit der Organisation insgesamt zu verbessern, indem sie die Kompetenzen zur (emotionalen) Selbstregulierung der Akteure in ihren Systemen erweitern. Achtsame Mitarbeiter treffen Entscheidungen anders und kommunizieren mit sich und anderen besser.

Achtsamkeitstraining führt zu einem gesteigerten Bewusstsein für innere Reaktionen, was die Wahlfreiheit bei der Entscheidungsfindung erhöht. Achtsamkeitstrainings umfassen in der Regel Körperscans, um die Auswirkungen von Gedanken und Emotionen auf den Körper zu verstehen, sowie Übungen, die helfen, ein detaillierteres Vokabular der emotionalen Landschaft zu entwickeln.

Übungen zur Steigerung von Mitgefühl zielen darauf ab, eine emotionale Reaktion zu kultivieren, die im Interesse des Wohlergehens eines anderen Akteurs und nicht aus empathischer Not heraus erfolgen kann. Mitgefühl, wenn es auf das eigene Selbst angewandt wird, steigert beispielsweise die Motivation, sich trotz Misserfolgen weiterhin mit dem zugrundeliegenden Lernobjekt zu befassen (Breines & Chen, 2012). Mitfühlende Kommunikation beinhaltet die Praxis, die eigenen inneren Gedankenprozesse und im Körper verankerten emotionalen Schmerzreaktionen als die eigene vorprogrammierte Antwort auf einen externen Auslöser zu untersuchen und eine Antwort zu wählen, die mit dem Verständnis dessen übereinstimmt, was für die beteiligten Akteure, einschließlich der eigenen Person, die verantwortbare Lösung darstellt.

Einer der Hauptvorteile der Kultivierung einer beständigen Praxis von Achtsamkeit und Mitgefühl besteht darin, dass sie das Bewusstsein für die Unbeständigkeit der Natur der Dinge schärft und so die Praktizierenden darin schult, der von Schwarzen Schwänen geprägten stürmischen Welt des immerwährenden Wandels mit Leichtigkeit und Anmut zu begegnen. Sie bereitet die Entscheidungsträger darauf vor, dem Schwarzen Schwan mit Gleichmut ins Auge zu blicken, ohne dabei den Verstand auszuschalten.

Die sich in einem frühen Stadium befindende neurowissenschaftliche Forschung im Zusammenhang mit Achtsamkeit hat gezeigt, dass verschiedene Arten von Achtsamkeitsübungen Gehirnregionen beeinflussen, die mit Wahrnehmung, Bewusstsein, Schmerztoleranz, Emotionsregulierung, Introspektion, komplexem Denken und Selbstwertgefühl zusammenhängen. Studien zeigen Veränderungen in der Dichte der grauen Substanz in verschiedenen Hirnregionen auf, z.B. im vorderen zingulären Kortex (ACC), einem Bereich, der mit der Selbstregulation und der Fähigkeit, die Aufmerksamkeit gezielt zu lenken, in Verbindung gebracht wird, und im Hippocampus, einem Teil des limbischen Systems, der mit Emotionen und Gedächtnis in Verbindung steht (Congleton/Hoelzel/Lazar, 2015).

Achtsamkeit und Mitgefühl in der Kommunikation wirken sich nicht nur auf die Beziehungen, die Kreativität und die Leistung der einzelnen Beteiligten aus, sondern sind unverzichtbare Pfeiler für die Rückkopplungsschleifen in antifragilen kybernetischen Systemen.

Internet der Werte, Token-Ökomomie und DAO

Web3, gemeinhin als Internet der Werte bezeichnet, ist die nächste Phase des Internets. Es folgt den Fußstapfen des Web1, des Internets der Informationen, und des Web2, des Internets der Kommunikation, die zum einen die Kosten für Information und zum anderen die Kosten der weltweiten Kommunikation erheblich gesenkt haben.

Das Internet der Werte ist ein wichtiger Wegbereiter für die antifragilen kybernetischen Systeme der Zukunft, da es den Menschen ermöglicht, eigenständig neue Formen von Werten zu schaffen. Die Fähigkeit, mittels genehmigungsfreier Technologie allen möglichen Unternehmungen digitale Werte zuzuschreiben, diese Werte zu verteilen und Beiträge zur Wertsteigerung auf nahezu kostenfreie Weise zu koordinieren, ermöglicht die radikale Senkung der Kosten im globalisierten wirtschaftlichen Austausch und schafft bislang ungesehene Möglichkeiten für mehr Teilhabe an der Wirtschaft und die Verringerung der Wohlstandsungleichheit.

Zum Zeitpunkt der Erstellung dieses Berichts wird der Web3-Markt auf etwa 1 Bill. USD geschätzt, was gerade einmal 1 Prozent des weltweiten Aktienmarktes entspricht. Im Juli 2022 hatten die zehn beliebtesten Anwendungen im Durchschnitt nur 500.000 Nutzer pro Monat (DappRadar, Juli 2022). Obwohl sich diese Branche noch im Anfangsstadium befindet, hat sie das Potenzial, die Zahl der Menschen, die von den Vorteilen einer auf freiem, offenem und freiwilligem Austausch basierenden Wirtschaft profitieren können, massiv zu erhöhen. Laut dem Vermögensverwalter Wells Fargo sind „digitale Vermögenswerte eine transformative Innovation, die dem Internet, dem Auto und der Elektrizität in nichts nachsteht" (Wells Fargo, 2022).

Das Wohlstandspotenzial dieser Branche ist auch Hackern nicht entgangen, die seit 2011 für den Diebstahl von Krypto-Vermögenswerten im Wert von 14,5 Mrd. USD verantwortlich sind. Allein in der ersten Hälfte des Jahres 2022 wurden digitale Vermögenswerte im Wert von mehr als 2,5 Mrd. USD aus den zehn größten dezentralen Finanzprojekten gestohlen – aus Projekten, die einen der ersten großen Anwendungsfälle des Internet of Value darstellen (CoinDesk).

Im Web3 wird der Wert in digitalen Containern namens „Token" gespeichert, die sofort und unmittelbar von Nutzer zu Nutzer (Peer-to-Peer) verschickt werden können, ohne dass eine zentrale intermediäre Funktion erforderlich ist. In der sogenannten Token-Ökonomie gibt es keine Grenzen für die Vielfalt der Werte, die dargestellt, modelliert und ausgetauscht werden können. Sowohl Transaktionen als auch die Handlungen von Entscheidungsträgern sind für das gesamte Ökosystem transparent sichtbar.

Diese Token-Ökomomie baut auf dem Internet der Werte auf und kann die vorherrschende Wohlstandsungleichheit verringern, indem sie allen Teilnehmern die Möglichkeit gibt, von der durch sie geschaffenen Wertsteigerung zu profitieren. Dies ermöglicht den Aufbau von unternehmerischen Kooperationsmodellen, in denen viel mehr Menschen an der ökonomischen Wertschöpfung teilhaben können, beispielsweise indem sie einen digitalen Anteil an der gemeinschaftlichen Unternehmung erwerben, zu deren Wertschöpfung sie durch ihre Mitwirkung in erster Linie sichtbar und messbar beigetragen haben. Im Web3 sind dank der technologischen Architektur und der durch digitale Tokens repräsentierbaren Werte die Wirkung und der Wertbeitrag der unternehmenden Akteure unmittelbar miteinander verbindbar.

Web3 ist ein System, in welchem die Rechenschaftspflicht von einer aktiven zu einer passiven Form der Berichterstattung transformiert wird: Jederzeit ist jedem Akteur die Einsicht in alle im Ökosystem („on-chain") durchgeführten Wert-Transaktionen möglich. Die unsichtbare Handlungsphilosophie wird in solchen Systemen mit der Prämisse „ich weiß, dass du weißt, dass ich weiß" unterlegt, da die Transparenz per Design im System codiert ist. Diese Transparenz verbessert die Entscheidungsfindung, da sie vorherrschende Informationsasymmetrien reduziert.

Eine der wichtigsten Innovationen des Web3 ist die DAO, die Dezentrale Autonome Organisation. DAOs können als Genossenschaften betrachtet werden, die im Besitz ihrer Mitglieder sind und von diesen gemeinsam verwaltet werden, wobei die Blockchain-Technologie für koordinierte Aktionen und Entscheidungsfindung genutzt wird. In DAOs werden die Entscheidungsbefugnisse und die Verwaltung der Finanzen unter den Beteiligten verteilt, anstatt sie in den Händen einiger weniger Manager zu zentralisieren. Die dezentrale Kryptowährungsbörse UniSwap beispielsweise verfügt mit Stand Juli 2022 über Krypto-Vermögenswerte im Wert von 4 Mrd. USD, die von einer Gemeinschaft von 350.000 Token-Inhabern und deren Delegierten verwaltet werden, welche Upgrades für das Projekt vorschlagen und über diese abstimmen. Seit ihrer Gründung im August 2021 haben die Mitglieder der UniSwap-DAO über 89 Vorschläge abgestimmt, an denen sich insgesamt 8.300 Wähler beteiligt haben, mit einer Erfolgsquote von 45 Prozent (DeepDao Database, Juli 2022). Die Ergebnisse der Vorschläge und die Wertströme in und aus den Kassen können über kostenlose Online-Tools eingesehen werden, die es allen Beteiligten ermöglichen, zu allen vergangenen und gerade stattfindenden Transaktionen Auskunft zu erhalten.

Der nächste Schritt im Web3: von DAOs zu TAOs

Die Einführung von kybernetischen Prinzipien, Achtsamkeit und Mitgefühl in der Kommunikation ist der nächste Schritt in der Entwicklung des Web3-Ökosystems. DAOs werden zu TAOs: Transiente Antifragile Organismen. Wenn die kybernetische Sichtweise auf die Art der Zusammenarbeit angewandt wird, wird die DAO zu einem lebenden Organismus, einer Einheit, bei der das Ganze mehr ist als die Summe seiner Teile. TAOs sind darauf ausgelegt, sich schnell zu entwickeln und zu skalieren sowie sich immer wieder neu zu erfinden. TAOs haben keine Angst vor Hackerangriffen, da sie Prozesse entwickelt haben, um ihre Schwachstellen zu erkennen und das Risiko einer vollständigen Eliminierung zu verringern. Der TAO zeichnet sich durch drei Schlüsseleigenschaften aus:

- Robustheit: Fähigkeit, das Risiko des Untergangs zu erkennen und zu verringern
- Anpassungsfähigkeit: Fähigkeit, die Angst vor dem Untergang loszulassen
- Wachstum: Fähigkeit, Kapital aus der Volatilität von Ereignissen zu schlagen

Als transienter Organismus ist der TAO ein Gebilde, das von Natur aus vergänglich ist und nur so lange existiert, wie er dem Zweck, für den er ins Leben gerufen wurde, tatsächlich dient. Im TAO stellt der teilnehmende, sich selbst regulierende Akteur den Mechanismus dar, der das Gleichgewicht im Organismus aufrechterhält, indem er Veränderungen der Bedingungen erkennt und sich in der iterativen Feedbackschleife entsprechend anpasst.

Die Entscheidungsträger im TAO sind in den Disziplinen der Kybernetik, der Achtsamkeit und des Mitgefühls ausgebildet. Sie wissen, dass Vergänglichkeit kein Grund zur Sorge ist, da alles Wissen, was die TAO-Mitglieder angelegt haben, selbst bei Eintreten des kompletten Ruins für die Menschheit nicht verloren gehen wird. Indem er die Volatilität – oder in anderer Betrachtungsweise die Lebendigkeit der Welt – als Chance zur immerwährenden Verbesserung begreift, ist der TAO gut gerüstet, um mit mitfühlender Neugier statt mit lähmender Angst in das Auge des Schwarzen Schwans zu blicken und damit seinen historischen Beitrag zur Token-Ökonomie und zur Verringerung der vorherrschenden Ungleichheit im materiellen Wohlstand leisten.

Quellen

- Baydakova, A. (2022, Juli 27): DeFi Has Become Crypto Crime's Main Arena, Crystal Blockchain Says. CoinDesk, https://www.coindesk.com/business/2022/07/27/defi-has-become-crypto-crimes-main-arena-crystal-blockchain-says/.
- Breines, J. G.; Chen, S. (2012): Self-Compassion Increases Self-Improvement Motivation. Personality and Social Psychology Bulletin, 38(9), 1133–1143.
- Congleton, C.; Hölzel, B.; Lazar, S. (2015): Mindfulness Can Literally Change Your Brain (Digest Summary). Harvard Business Review.
- Foerster, H. von (1995 [1975]): Kybernethik. Berlin: Merve Verlag.
- Moore, C. (2019, April 9): What Is Mindfulness? Definition + Benefits (Incl. Psychology). PositivePsychology. Retrieved July 25, 2022, from https://positivepsychology.com/what-is-mindfulness/.
- Organizations (2022): DeepDAO. Retrieved July 25, 2022, from https://deepdao.io/organizations.
- Taleb, N. N. (2012): Antifragile: Things that gain from disorder. New York: Random House.
- Top Blockchain Dapps. (2022): DappRadar. Retrieved July 27, 2022, https://dappradar.com/rankings/1.
- Wells Fargo (2022, August): Digital Assets – A World of Possibilities. Wells Fargo Advisors, https://www.wellsfargoadvisors.com/research-analysis/reports/cryptocurrency/digital-assets.htm.

Autorenverzeichnis

Schutz vor Hacking – ein ewiger Wettlauf im Unternehmen?
Dr. Karsten Nohl ist Hacking-Experte und Gründer von Autobahn Security in Berlin. Karsten schafft Bewusstsein für Cybersicherheit – durch Hacking-Forschung und -Beratung. Dabei fasziniert ihn besonders der Zielkonflikt zwischen Security und Innovation.

Cybersecurity und Kybernetik
Dr. Ralf Schneider ist seit 2010 Group CIO der Allianz SE und verantwortet global die IT Governance, Strategy und Security. Davor war er IT-Vorstand der Allianz Managed Operations & Services SE (2010–2016) und CIO der Allianz Deutschland (2006–2010). Nach seinem Studium der Mathematik und einer Promotion in Informatik fing er 1995 bei der Allianz an. Seit über 25 Jahren hat er führende Positionen im IT-Bereich inne, so war er u.a. Abteilungsleiter des Bereichs Informationssysteme Vertrieb und Fachbereichsleiter des Fachbereichs e-Business und Projektcontrolling Deutschland. Zusätzlich ist er Mandatsträger mehrerer Cyber-Security-Organisationen wie des Cyber Security Sharing & Analytics e.V., der Deutschen Cyber Sicherheitsorganisation und des Digital Society Institute an der ESMT.

Was ist Kybernetik?
Prof. Dr. Fredmund Malik ist anerkannter Managementexperte sowie Vorsitzender von Führungs- und Beratungsgremien in Wirtschaftsunternehmen. Er ist ein Pionier der Managementkybernetik und des Komplexitätsmanagements. Er war Mitglied des Direktoriums des Instituts für Betriebswirtschaftslehre und seit 1977 parallel dazu des Managementzentrums St. Gallen. Er ist Autor von mehr als 15 Büchern. Sein Buch „Führen Leisten Leben" wurde unter die 100 besten Wirtschaftsbücher aller Zeiten gewählt. 2018 erhielt er den Life Achievement Award, die höchste Auszeichnung im deutschen Management-Bildungssystem.

Design und Management agiler Cybersecurity-Organisationen
Andreas Slogar war in über 20 Ländern, den USA, Europa, dem Mittleren Osten und Afrika tätig und hat u.a. als CIO umfassende Erfahrung in strategischer und operativer Managementarbeit aufgebaut. Slogar ist als Experte auf die Transformation ganzer Unternehmen in einen veränderungsfähigen Kollaborationszustand spezialisiert und ist Autor diverser Fachartikel, Podcasts und des Buches „Die agile Organisation" (Hanser Verlag, 2018, 2020).

Antifragilität im Web3: eine kybernetische Sichtweise
Yip Thy-Diep Ta ist Gründerin bei Unit Network, einer Blockchain für die Token-Ökonomie. Mit ihren Initiativen DLT-Talents, Unit Masters und H.E.R. Dao bietet sie kostenfreie Ausbildungsprogramme und Stipendienprogramme zur Förderung der Chancengerechtigkeit in Web3. Yip ist Gründerin bei der Genossenschaft Balanced Being, welche Achtsamkeitstrainings für Unternehmen anbietet. Sie ist Autorin des Buches „Beautiful Brains change tomorrow... today" und hat mehrere Auszeichnungen als eine der einflussreichsten Frauen in Blockchain erhalten. Zuvor war sie als Beraterin bei McKinsey & Co. tätig.

Ansprechpartner

Nils Dennstedt
Partner
Sector Lead Insurance
Tel: +49 40 32080 4463
ndennstedt@deloitte.de

Marius von Spreti
Partner
Cyber
Tel: +49 89 29036 5999
mvonspreti@deloitte.de

Andreas Slogar
Senior Manager
Agile Business Transformation
Tel: +49 151 58077936
aslogar@deloitte.de

Deloitte.

Stand 11/2022