Systemgesetze und die Sicherheit (1)

Verletzung „natürlicher“ Bedürfnisse und Prioritäten schadet der Security

Überall, wo Menschen involviert sind, geht es nicht nur um Logik, sondern auch um Empfindungen. Selbst positive Absichten können negative Folgen haben, wenn sie bestimmte „Systemgesetze“ verletzen. Wer diese kennt, kann sie sich umgekehrt zunutze machen – auch für die Sicherheit.

Von Dieter Bischop, Hamburg & Kiel, und André Hojka, Kiel

Security arbeitet nicht im „luftleeren Raum“ einer rein technischen Welt, sondern ist in ein komplexes System aus Menschen, Maschinen und Organisationseinheiten eingebettet. Neben der Definition und Umsetzung technischer und organisatorischer Maßnahmen spielen daher nicht nur die Bereitschaft und Befähigung der Mitabeiter, sondern auch die Unternehmenskultur eine wesentliche Rolle für das Funktionieren des großen Ganzen – und damit auch für die Informations-Sicherheit (vgl. Kasten).

Darüber hinaus beginnen jedoch viele Probleme – und somit auch Chancen – bereits bei der Kommunikation. Noch unterhalb der bekannten Sach- und Beziehungsebenen lässt sich ein dritter Level als Fundament (und oft auch Ursache für Schwierigkeiten) modellieren: die Systemgesetzebene (vgl. Abb.). Sie entscheidet darüber, ob die Beziehungs- und Sachebene überhaupt funktionieren und stabil sein können – die Verletzung von Systemgesetzen führt zu Konflikten, deren Auswirkungen sich durch alle Ebenen fortsetzen.

Der Mensch ist ein beträchtlicher Risikofaktor, das ist nicht neu. Der „tiefliegendste“– und somit womöglich bedeutendste – Einflussfaktor ist auch beim Menschen die Ebene der Systemgesetze (vgl. Kasten). Die Systemgesetze wirken! Sie sind den Menschen normalerweise zwar nicht bewusst – man spürt jedoch die Wirkung bei Einhaltung der Systemgesetze in positiver und bei Verletzung in negativer Form:

_____ Werden die Systemgesetze eingehalten, so ist das ganze System (z. B. Team, Familie, Organisation, Unternehmen) motiviert – die Beziehungen stimmen, jeder Einzelne fühlt sich unterstützt und gestärkt. Die Einhaltung der Systemgesetze bildet so auch die Basis für eine „gelebte“ Sicherheit.

_____ Werden Systemgesetze missachtet, folgt eine Schwächung oder Demotivation des Systems und jedes Einzelnen. Typische Symptome für die Verletzung von Systemgesetzen in Organisationen sind überraschend kündigende Mitarbeiter oder Kunden, interne Machtkämpfe, Mobbing, Sabotage, massive Umsatzeinbrüche, lähmende Stagnation oder Demotivation.

Abbildung 1: Bereits unterhalb der Sach- und Beziehungsebene sorgen Systemgesetze oft für Gelingen oder Scheitern einer Kommunikation – oder eines Projekts.

Systemgesetze

Der Begriff der Systemgesetze hat sich erst im 20. Jahrhundert entwickelt und wird in politischen sowie physikalisch-technischen und biologischen Systemen verwendet. Die im Folgenden dargestellte Systematik von zehn Systemgesetzen entstammt dem Buch „Coachen und Führen mit System“ [1] von Dr. Dieter Bischop und ist nach der Stärke ihrer Wirkung sortiert, also der Heftigkeit des mit einer Verletzung verbundenen Gefühls („Einschlag in der Bauchgegend“).

Grundbedürfnisse

1. Zugehörigkeit

Das wichtigste Systemgesetz ist die Zugehörigkeit zum eigenen System – denn das bedeutet Überleben. So ist es heute noch im Tierreich; und wir bringen dieses Erbe, das in unseren Verhaltensprogrammen gespeichert ist, aus unserer Entstehungsgeschichte mit. Das Recht auf

Zugehörigkeit, allem voran Nicht-Ausschluss, kann sich dabei auf einen Personen- oder Kulturkreis beziehen, auf eine Idee, Entscheidungsfindung et cetera.

Reaktionen auf eine Verletzung dieses Systemgesetzes sind in der Regel heftig und können sich als Gegenwehr (Kampf), Rückzug (Flucht) oder auch Revanche (Rache – Ausschluss des Verletzers, „Auge-um-Auge"-Prinzip) äußern.

2. Anerkennung

Das zweitwichtigste Systemgesetz fordert Anerkennung, Wertschätzung und Respekt (einer Person, aber auch Kultur oder Ordnung etc.). Ohne Anerkennung kann kein System langfristig funktionieren: Sie ist der Motor, der ein System zum Laufen bringt und am Laufen hält – fehlt sie, gerät er ins Stottern und das System stagniert. Anerkennung und Wertschätzung sind an keine Bedingung geknüpft, kein Mitglied muss etwas aktiv dafür tun, in einem System anerkannt zu werden; ansonsten kommt es zu Verletzungen.

Respekt ist hingegen Anerkennung, die an eine Bedingung geknüpft ist. Beispielsweise kann ein Chef nur dann Respekt erwarten, wenn er auch wirklich seiner Rolle und Verantwortung als Chef nachkommt. Erhält er den Respekt nicht, weil er Systemgesetze verletzt oder nicht klar führt, so fordert er oft Loyalität ein. Das ist aber ein untauglicher Versuch: Muss man Respekt (wie auch Liebe, Loyalität oder Dankbarkeit) einfordern, so hat er keinen Wert mehr.

Ebenen ganzheitlicher Sicherheit

Eine im Sinne ihres Zieles wirksame IT- beziehungsweise Informations-Sicherheit kann nur dann gelingen, wenn neben den technischen (z. B. Netzwerksicherheit, Virenschutz, Verschlüsselung, ...) und organisatorischen Voraussetzungen (z. B. nach ISO 27001, BSI Grundschutz, NIST, ITIL, …) der Ebene „Umgebung" noch sechs weitere Ebenen berücksichtigt werden. Das Modell der IT-Sicherheits-Ebenen beschreibt auch anschaulich, weshalb es keine 100%-ige Sicherheit geben kann – im besten Fall erreicht man eine hohe Sicherheit, wenn alle aufgeführten Punkte Beachtung finden.

Dieses Modell ist gleichermaßen für ganze Unternehmen, Teams oder einzelne Personen gültig. Auf der Ebene, in der Technik und Organisation eine bestimmende Rolle spielen, lässt sich Sicherheit weitestgehend „bereitstellen" (Ausnahmen: NSA etc.), indem man organisatorische Regelungen trifft und technisch flankiert. Doch selbst hier bleiben der Mensch und sein Verhalten ein beträchtliches Sicherheitsrisiko – auf den weiteren Ebenen gilt das umso mehr, weswegen hier Beispiele für den Risikofaktor Mensch das gesamte Modell der sieben Ebenen verdeutlichen sollen.

_____ *Umgebung:* Auch wo (u. a.) gute Firewalls, gesicherte Serverräume, redundanter Betrieb, klare Sicherheitskonzepte und ein zertifiziertes ISMS vorliegen, können unsichere Passwörter, veraltete und damit störanfällige Hardware, Investitionsstaus, Prozess- und Dokumentationslücken et cetera zu Problemen führen.

_____ *Verhalten:* Probleme resultieren häufig aus zu wenig Aufklärung, mangelnder Bekanntheit oder Beachtung von IT-Sicherheitsrichtlinien, fehlender Kommunikation, Fehlinterpretationen et cetera.

_____ *Fähigkeiten:* Fehlende Schulungen oder mangelndes Bewusstsein für negative Auswirkungen von Sicherheitslücken bedeuten Risiken.

_____ *Überzeugungen:* Probleme erwachsen beispielsweise, wenn die IT-Sicherheit nicht als Erfolgsfaktor des eigenen Unternehmens angesehen wird, IT-Risiken nicht ausreichend bekannt sind oder man Vertrauen in Dienstleister nicht hinterfragt.

_____ *Identität:* Heikel wird es, wenn die Identität des Unternehmens („Wer sind wir?") nicht bekannt ist oder nicht auf die Informationssicherheit übertragen wird – das notwendige Zusammenspiel von Strategie, Kultur und Struktur findet dann keine Beachtung.

_____ *Vision:* Die Vision des Unternehmens („Wofür stehen wir?") und die Bedeutung der Security zur Verwirklichung dieser Vision müssen vermittelt werden – sonst fehlt es an einer grundlegenden Motivation.

_____ *Systemgesetze:* Die Einhaltung der Systemgesetze führt zu einem „stimmigen", funktionierenden Gesamtsystem, zu motivierter Zusammenarbeit mit Anerkennung und Respekt. Systemgesetzverletzungen führen zu Demotivation – je nach Stärke der Verletzung kann es unbewusst oder bewusst zu sicherheitskritischem Verhalten kommen (z. B. „Meldefaulheit", Datenpreisgabe, Extremfall: Sabotage – vgl. [3]).

3. Gleichgewicht

Der Wunsch nach Gerechtigkeit ist ebenfalls ein Grundbedürfnis. Jeder hat ein Gefühl dafür, ob etwas ausgeglichen ist – ob ein Gleichgewicht von Geben und Nehmen besteht. Die dahinter stehende Frage lautet: „Sind alle Teile (Menschen, Ideen, Projekte etc.) gleichberechtigt?" beziehungsweise „Wer oder was ist wichtiger?"

Grundsätzlich streben Systeme durchaus einen ausgeglichenen Zustand an. Wesentlich ist hierbei aber auch die Einsicht, dass es bei der Befriedigung dieses Systemgesetzes nicht nur um eine „objektive", messbare Größe geht, sondern auch um das Gefühl einer Person oder Gruppe, sich in einem ausgeglichenen Zustand zu befinden.

Ordnung

Während die ersten drei Systemgesetze essenzielle Bedürfnisse abdecken, bildet das zweite Tripel eine Ordnungshierarchie: Jedes dieser Gesetze beschreibt in sich einen Vorrang und Gesetz 4 hat Vorrang vor Gesetz 5, das wiederum Vorrang vor Gesetz 6 hat.

4. Zeit

Dienstalter, Warte- oder Laufzeit und andere temporale Größen bedingen einen Anspruch auf Vorrang. Hier gilt „früher vor später" – ganz im Sinne von „Wer zuerst kommt, mahlt zuerst" als Standard.

5. Einsatz

In zweiter Linie steht der Vorrang durch höhere Verantwortung oder höheren Einsatz – wer mehr bringt, wagt, macht, verantwortet et cetera, der hat Priorität.

6. Kompetenz

Erst als dritte Instanz entscheiden größere Kompetenz, mehr Wissen oder Vergleichbares. So müssen beispielsweise Mitarbeiter den Chef als Vorgesetzten anerkennen, wenn er seine Führungsrolle lebt, auch wenn sie womöglich auf ihrem Gebiet mehr Kompetenz besitzen.

Der hier bezeichnete Vorrang muss sich gemäß der Systemgesetze in Anerkennung äußern – beispielsweise des „später Gekommenen" vor dem Dienstälteren oder des Kompetenteren vor der Führungskraft. Anerkennung zeigen heißt dabei auch, anerkennend *handeln* – Worte allein genügen nicht.

Nachrrangiges

7. Generationsfolge

Wenn alle sechs vorherigen Systemgesetze befriedigt werden, erhält ein neues System Vorrang vor einem alten. Hierdurch bekommen Innovation und Evolution eine zusätzliche Betonung. Das entwicklungsgeschichtliche Vorbild ist hier etwa die Priorität, für das Überleben der eigenen Kinder zu sorgen.

8. Gemeinschaft

In ähnlicher Weise erhält das Gesamtsystem Vorrang vor einzelnen Komponenten (Personen oder Teilsystemen) – so wie beispielsweise das Ergebnis der ganzen Mannschaft wichtiger ist als das Abschneiden eines Einzelnen. Dies führt jedoch häufig zu Systemgesetzverletzungen, wenn nicht Gesetz 9 angewendet wird.

Bereinigendes

Die beiden letzten Prinzipien sind der Schlüssel entweder zum Lösen von Verletzungen anderer Systemgesetze oder bei beabsichtigter Umkehrung der Prioritäten aus den Gesetzen 4–6.

9. Aus- und Ansprache

Aussprechen und anerkennen, was geschehen ist beziehungsweise geschehen soll, kann „Schmerzen" beseitigen – es nicht zu tun, kann „Schmerzen" verstärken.

10. Ausgleich

Einen Ausgleich auf anderer Ebene zu schaffen ist hilfreich, jedoch meist erst dann erfolgreich möglich, wenn Systemgesetz 9 zu seinem Recht gekommen ist.

Fazit

Die Systemgesetze gelten nicht nur für zwischenmenschliche Beziehungen, sondern sind auch das Fundament für die Organisations- und Unternehmensentwicklung. Ein Unternehmen hat normalerweise eine Vision mit der passenden Strategie, eine Struktur sowie eine Kultur. Werden etwa bei einer Unternehmensnachfolge, einer Fusion oder einer Umstrukturierung die Systemgesetze nicht beachtet, so kommt es zu Konflikten. Dies kann jedoch auch im „Alltag" geschehen.

Eine Verletzung der Systemgesetze bewirkt bewusste oder unbewusste Verhaltensänderungen, in deren Folge – auf unser Anwendungsgebiet bezogen – die Sicherheit von Informationen oder IT gefährdet werden kann:

Die Motivation für die Sicherheit und deren Bedeutung schlägt in Demotivation um. Es kann sogar zur absichtlichen Schädigung des Unternehmens kommen, je nach Stärke der Verletzung.

Im Umkehrschluss lautet das Fazit, dass man die gesetzten Ziele zur IT- und Informations-Sicherheit nur dann erreichen kann, wenn neben den technischen und organisatorischen Faktoren auch der Mensch mit allen zuvor beschriebenen Ebenen stärkere Berücksichtigung findet. Berücksichtigen heißt dabei, die Systemgesetz-Ebene mit Zugehörigkeit und Anerkennung zu erfüllen und zu „leben" sowie bereits vorhandene Systemgesetzverletzungen aufzulösen. ■

Dr. Dieter Bischop (bischop@hanseatisches-institut.de) ist Gründer des Hanseatischen Instituts für Coaching, Mediation & Führung. Dr. André Hojka (ahojka@vater-gruppe.de) ist Fachgruppenleiter „IT-Security" des Clustermanagements Digitale Wirtschaft in Schleswig-Holstein und arbeitet für die Informationssicherheitsberatung Vater Solution GmbH.

In der nächsten Ausgabe behandelt der zweite Teil dieses Beitrags anhand von Beispielen aus der Praxis Strukturen, die zu Systemgesetzverletzungen führen können – und wie man das vermeidet.

Literatur

[1] Dr. Dieter Bischop, Coachen und Führen mit System, Als Führungskraft, Coach und Mediator systematisch Wirkung erzielen, Verlag Ludwig, 2010, ISBN 978-3-86935-009-7

[2] Hanseatisches Institut für Coaching, Mediation & Führung, Systemgesetze, www.hanseatisches-institut.de/coaching-mediation/systemgesetze.html

[3] Entsicherung am Arbeitsplatz, Erkenntnisse und Folgerungen zur Psychologie der IT-Sicherheit, <kes> 2006#6, S. 61, online auf http://2014.kes.info/archiv/online/06-6-061.htm