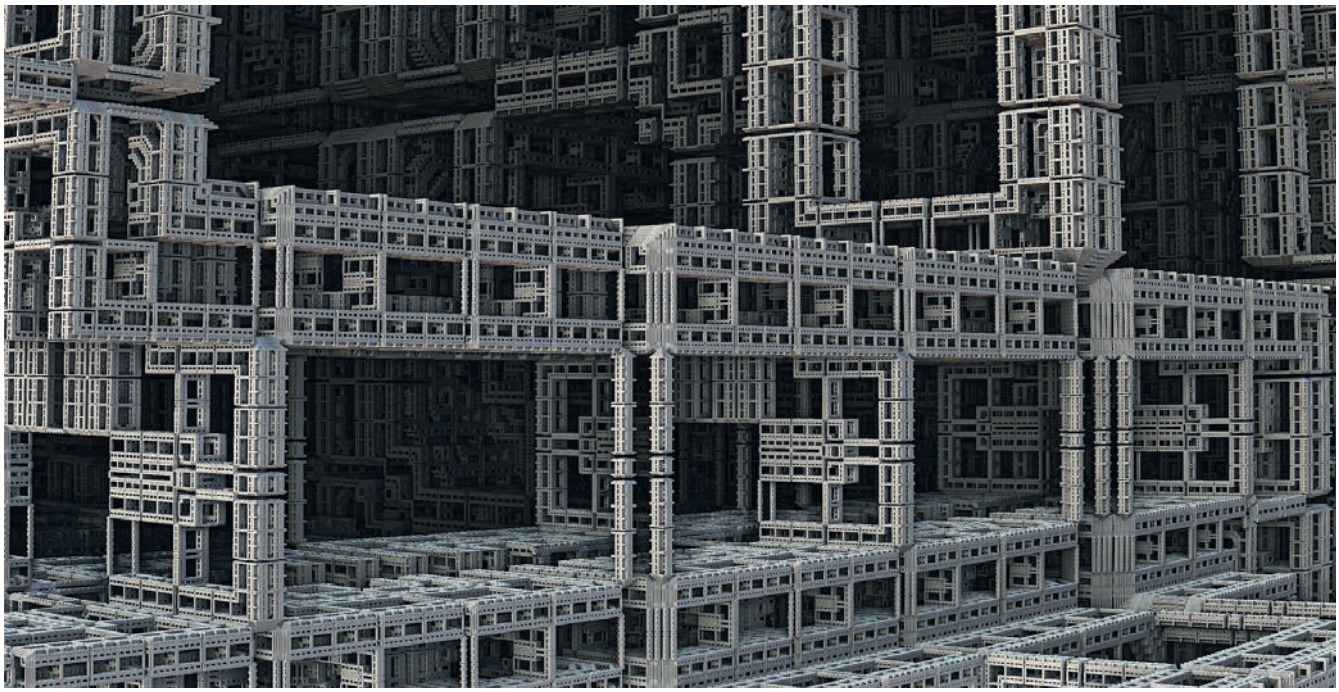

Kompliziert oder komplex?

Cybersecurity in der Praxis | Menschen wünschen sich einfache Lösungen. So auch für die Cybersecurity. Viele KMU wähnen sich mit einer Firewall, Antivirus-Software und einem Spam-Filter sicher und wundern sich, wenn sie Opfer von Cyber-Attacken werden. Der Schwachpunkt besteht darin, ein komplexes Problem zu einfach und allein mit Technik lösen zu wollen.

LEVENTE J. DOBSZAY

Komplizierte und komplexe Probleme erfordern unterschiedliche Lösungsstrategien. Daher ist es entscheidend, zu verstehen, ob ein Problem komplex, kompliziert oder sogar nur einfach ist. Einfache Probleme bedürfen keiner weiteren Analyse oder Modellierung. Wir können sie erkennen, kategorisieren und ziehen die passende Lösung aus unserer Schublade. Komplizierte Probleme bedürfen zunächst einer Analyse. Ihre Lösung können wir dann als «Schritt für Schritt»-Anleitungen beschreiben. Das Fachwissen für die entsprechenden Lösungen können wir uns erarbeiten. Für das Verständnis komplizierter Systeme reichen meist statische Modelle. Komplexe Probleme hingegen müssen zuerst überhaupt als solche erkannt werden und können gar nicht abschliessend analysiert werden. Für das Verständnis von komplexen Systemen bedarf es dynamischer Modelle. Lösungen können nur ansatzweise und nur für Teilaspekte vorausgedacht werden. Wir können für komplexe Probleme keine fertigen Lösungen im Voraus «auf Halde» erarbeiten, sondern können uns auf sie nur möglichst gut vorbereiten, um im Eintretensfall angemessen reagieren zu können.

Unterschied zwischen kompliziert und komplex

Ein kompliziertes Problem (lat. complicare = verwickeln) ist eines, das aufgrund der Menge von Elementen schwer zu überschauen ist, obwohl seine Struktur auf einer endlichen Menge relativ einfacher Regeln aufbaut. Ein solches Problem lässt sich mit entsprechendem Aufwand (Zeit, Ressourcen) lösen. Die Beziehung zwischen Ursache und Wirkung lässt sich ermitteln, denn sie ist deterministisch. Komplizierte Sachverhalte lassen sich formal beschreiben und komplizierte Probleme mit Hilfe von Technik und Fachwissen effizient lösen. Der Grad der Kompliziertheit ist jeweils eine Frage der Wahrnehmung.

Ein komplexes Problem (lat. complectere = verflechten) ist eines, dessen zugrundeliegende Struktur viele Verflechtungen und Abhängigkeiten besitzt und dessen Regeln unerwartet ändern können. Die Einflussfaktoren

Bild: Pixabay

können sich durch Wechselwirkungen und Rückkopplungseffekte gegenseitig beeinflussen und oft ist nicht einmal ihre genaue Anzahl bekannt. Entsprechend ist die Lösung nur schwer bis gar nicht voraussagbar. Komplexität ist auch ein Mass für die Überraschung, die einem System oder Problem innewohnt. Die meist multikausale Beziehung zwischen Ursache und Wirkung kann erst im Nachhinein ermittelt werden. Komplexe Sachverhalte lassen sich höchstens in Teilbereichen formal beschreiben. Komplexe Probleme sind daher nicht völlig beherrschbar und können auch nicht allein durch Technik gelöst werden. Sie benötigen Fachwissen und Zeit und können nur von Menschen gelöst werden.

1. Organisation	11. USB und externe Datenträger
2. Ziele, Strategie und Kennzahlen	12. Datenspeicherung und -übertragung
3. Asset Management	13. Backup und Restore
4. Risikoanalyse und Security Testing	14. Patch Management
5. Sicherheitsarchitektur	15. Visibilität und Entdeckung
6. Ausfallsicherheit und Redundanz	16. Überwachung und Alarmierung
7. Systemhärtung	17. Notfall Management
8. Netzwerkzonierung	18. Richtlinien und Schulung
9. Identitäts- und Zugriffskontrolle	19. Lieferanten-Management
10. Fernzugriff	20. Budgetierung

Bild 1 Cybersecurity-Schlüsselelemente für industrielle KMU.

Cybersecurity ist komplex

Logistik und Maschinen sind kompliziert. Cybersecurity hingegen ist komplex, weil hinter Cyber-Attacken Menschen stehen, deren Motivation und Vorgehen unterschiedlich ist. Menschen, die sich in ihrem Verhalten unterscheiden, stellen die grösste Schwachstelle dar. Cybersecurity ist ein Katz-und-Maus-Spiel, dessen Ausgang schwer voraussagbar ist. Dafür gibt es ebenso wenig eine einfache Lösung wie es eine allgemeine, eindimensionale Lösung für ein n-dimensionales Problem gibt.

Komplexe Probleme zu lösen, ist eine intellektuelle Herausforderung, die ein Gespür für die Thematik verlangt. Sie jemals gänzlich zu beherrschen, ist eine Illusion. Cybersecurity ist nicht bloss ein technisches Problem, für welches allein die IT-Abteilung zuständig ist. Da es auch um organisatorische, betriebswirtschaftliche, wahrnehmungspsychologische und rechtliche Aspekte geht, ist nur eine interdisziplinäre Betrachtungs- und Vorgehensweise zielführend. Jeder, der von der Problematik betroffen ist, hat seinen Beitrag zu leisten.

Ein komplexes Problem kann nur durch eine schrittweise Annäherung und nur bis zu einem begrenzten Grad gelöst werden. Das Vorgehen besteht aus Erkennen, Verstehen, Konzipieren, Validieren beziehungsweise Ausprobieren, Dazulernen, Korrigieren und wieder Ausprobieren. Dafür ist eine Lösungsstrategie zu wählen, die ebendies nicht nur zulässt, sondern auch unterstützt. Das Vorgehen zur Erarbeitung einer Lösung für ein komplexes Problem sollte möglichst einfach und für alle Beteiligten verständlich sein. Mitunter mag es kompliziert sein und eine bestimmte Fachkompetenz erfordern. Komplex darf es aber keinesfalls sein, weil sonst der Weg zu keiner hinreichenden Lösung des Problems führt.

Um ein komplexes System zu verstehen, muss dieses zuerst entflochten werden. Daraus sollen dann komplizierte oder idealerweise einfache Teilprobleme entstehen, die mit der nötigen Fachkompetenz gelöst werden können. Bei der Cybersecurity gilt es, die Schlüsselelemente zu finden und deren Erfüllungskriterien zu ergründen.

Lösungsansätze

Einen praxisorientierten Ansatz stellen die 20 «CIS Controls» des Center for Internet Security dar. Sie lassen aber einige weisse Flecken offen. Im Gegensatz dazu stellt das Cybersecurity Framework des Nist einen wasserfallmodellartigen Ansatz dar, der für eine Reifegradmessung dienlich sein kann. Die praktische Umsetzung dieses Frameworks erweckt manchmal jedoch den Eindruck einer komplizierten akademischen Übung und lässt dabei trotzdem noch einzelne Fragen offen. Das IT-Grundschutz-Kompendium des BSI wiederum mag nach deutscher Gründlichkeit bis ins Detail strukturierte Anleitungen geben, lässt seinen Anwender aber schnell den Wald vor lauter Bäumen nicht mehr sehen und ist daher für Cybersecurity-Neulinge eher ungeeignet. Alle diese Standards stellen eine spezielle Sicht mit eigenen Akzenten auf die gleichen Schlüsselelemente dar. Mögen sie noch so richtig sein, ihre Anwendung stellt für Einsteiger und für mit dem Thema Ver- und Betraute ohne vertieftes Fachwissen eine Herausforderung dar.

Deshalb hat Electrosuisse die relevanten Standards entflochten und ihre Essenz zu 20 Schlüsselelementen zusammengefasst, die einzeln behandelt werden können, und dabei die weissen Flecken geschlossen. Daraus resultiert ein praxisorientiertes Framework, das vor allem den Anforderungen von Industrieunternehmen und Energieversorgern Rechnung trägt **(Bild 1)**.

Es beabsichtigt nicht, bestehende Standards zu ersetzen, sondern will das Thema verständlich und einfach handhabbar machen, ohne wichtige Elemente durch Vereinfachungen zu verlieren. Auch der Cybersecurity-Kurs von Electrosuisse basiert auf diesem Ansatz. Klare Erfüllungskriterien helfen vor allem Cybersecurity-Neulingen, sich auf das Wesentliche zu fokussieren. Es mag vielleicht erstaunen, dass eigentliche Schutztechnologien wie Firewalls, Antivirus-Software und Spam-Filter nur einen kleinen Teil der Punkte 5 und 8 abdecken. Cybersecurity ist eben ein komplexes Problem und besteht aus mehr als nur ein paar technischen Schutzmassnahmen.

Link
www.electrosuisse.ch/cybersecurity

Autor
Levente J. Dobszay ist Cybersecurity Specialist bei Electrosuisse.
→ Electrosuisse, 8320 Fehraltorf
→ levente.dobszay@electrosuisse.ch

Bild: Electrosuisse