FROM CISO TO HERO

Was es wirklich braucht, um Informationssicherheit im Unternehmen zu verankern

von Flo Zegar

wescaleIT AG

> Der erste CISO war vielleicht nicht der beste Techniker. Er war aber garantiert ein guter Kommunikator.

Flo Zegar

Eine Bemerkung vorab

Bevor es losgeht, ein kurzer Hinweis zu dem, was dieses Buch ist und was es nicht ist.

Es ist kein Fachbuch im klassischen Sinne. Du wirst hier keine detaillierten Anleitungen finden, wie man eine bestimmte Sicherheitsarchitektur aufbaut oder eine Norm Punkt für Punkt umsetzt. Davon gibt es genug, und vieles davon ist hervorragend. Dieses Buch beschäftigt sich mit dem, was zwischen den Zeilen dieser Fachbücher steht: mit der Frage, wie aus Wissen Wirkung wird.

Es ist auch kein Buch, das du in einem Zug durchlesen und dann ins Regal stellen solltest. Es ist eher als Begleiter gedacht. Lies ein Kapitel, denk darüber nach, probier etwas aus. Komm zurück, wenn eine bestimmte Situation ansteht. Die Werkzeuge im Anhang und die Fragen am Ende jedes Kapitels sind genau dafür da.

Und es ist bewusst kompakt gehalten. Ich hätte zu jedem Kapitel ein eigenes Buch schreiben können. Aber ich glaube nicht, dass mehr Seiten zu mehr Wirkung führen. Im Gegenteil. Das Wesentliche lässt sich oft kurz sagen. Das Schwierige ist nicht, es zu verstehen, sondern es zu tun.

Genau dabei soll dieses Buch helfen.

Für wen dieses Buch ist

Dieses Buch ist für alle, die Verantwortung für Informationssicherheit tragen und das Gefühl haben, dass sie mehr erreichen könnten, als sie aktuell erreichen.

Es ist für den ISO, CISO oder ISB im Mittelstand, der allein gegen einen Berg aus Aufgaben kämpft und nicht weiß, wo er anfangen soll. Es ist für den IT-Leiter, der gerade zusätzlich die Sicherheitsverantwortung übernommen hat und merkt, dass das ein anderer Job ist als der, den er kennt. Es ist für den erfahrenen Sicherheitsexperten, der technisch alles beherrscht, aber immer wieder an derselben Wand landet: Niemand hört zu.

Vielleicht erkennst du dich in einer dieser Beschreibungen wieder. Vielleicht passt keine genau, und trotzdem spürst du, dass etwas in deiner Rolle nicht so läuft, wie es könnte. Dann bist du hier richtig.

Was du mitbringen solltest, ist nicht ein bestimmter Wissensstand, sondern eine Bereitschaft: deine eigene Arbeit ehrlich anzuschauen und dabei nicht nur deine Systeme zu hinterfragen, sondern auch dich selbst. Genau an dieser Schnittstelle zwischen Nachdenken und Handeln entsteht die Veränderung, um die es in diesem Buch geht. Auf geht's!

Vorwort

Dieses Buch hat keinen wohlgemeinten Ratschlag als Ausgangspunkt. Es hat eine Frustration.

Ich habe in den letzten Jahren mehr CISOs kennengelernt, als ich zählen kann. Menschen mit echtem Wissen, echter Erfahrung und echtem Willen. Menschen, die ihre Unternehmen wirklich schützen wollen, die nachts über Bedrohungslagen nachdenken, die sich durch Regulatorik arbeiten, die technisch auf der Höhe sind. Und fast alle erzählten mir irgendwann dieselbe Geschichte: Ich weiß, was zu tun ist. Aber ich komme nicht durch.

Das Top-Management hört nicht zu. Das Budget fehlt. Die Maßnahmen kommen nicht an. Die Arbeit verpufft. Es ist, als würde man gegen eine Wand reden, die höflich zurücklächelt und dann zur Tagesordnung übergeht.

Das ist kein Versagen dieser Menschen. Es ist ein Strukturproblem. Und Strukturprobleme kann man lösen, wenn man bereit ist, sie beim richtigen Namen zu nennen.

Genau dafür haben wir bei der wescaleIT AG das Programm From CISO to Hero entwickelt. Nicht weil wir ein Produkt bauen wollten. Sondern weil wir verstanden haben, dass das Sicherheitsniveau in deutschen

Unternehmen nicht steigt, solange die Menschen, die es heben sollen, nicht die Werkzeuge bekommen, die sie dafür brauchen. Das betrifft die einzelnen Unternehmen. Es betrifft Lieferketten, kritische Infrastrukturen, die gesamte Wirtschaft.

Ein CISO, der nicht gehört wird, ist nicht nur für sein Unternehmen ein Problem. Er ist ein gesamtgesellschaftliches Risiko. Denn jedes Unternehmen, das schlecht geschützt ist, ist ein Einfallstor. Und in einer vernetzten Wirtschaft trifft ein Einfallstor irgendwann alle.

Dieses Buch ist kein Begleitmaterial zu unserem Programm. Es ist ein eigenständiges Werk. Es beschreibt, was einen wirkungsvollen CISO ausmacht, welche Fallen es gibt und wie man sie umgeht, und was sich verändert, wenn man anfängt, Sicherheit nicht nur zu machen, sondern auch zu führen.

Ich habe versucht, ehrlich zu schreiben. Über das, was funktioniert, und über das, was nicht funktioniert, auch wenn es auf dem Papier gut klingt. Manche Dinge in diesem Buch wirst du vielleicht schon geahnt haben. Andere werden dich herausfordern. Beides ist Absicht.

Dieses Buch gibt Antworten. Aber es gibt sie absichtlich nicht vollständig. Nicht weil ich etwas zurückhalte, sondern weil Wirkung nicht aus dem Lesen entsteht. Sie

entsteht aus dem Tun. Und das Tun braucht mehr als Seiten.

Wenn du nach der letzten Seite das Gefühl hast, dass sich etwas verändern kann, dann hat dieses Buch seinen Zweck erfüllt.

Flo Zegar

Vorstand, wescaleIT AG

Inhalt

Eine Bemerkung vorab	4
Für wen dieses Buch ist	5
Vorwort	7
Wo stehst du gerade?	11
Der CISO ohne Königreich	14
Die fünf Fallen	24
Handwerk, Sprache, Haltung	31
Das große Bild sehen	39
Die Sprache der Geschäftsführung	47
Struktur als Machtinstrument	56
Budget durchsetzen	64
Der erste Eindruck und die ersten 100 Tage	73
Wenn es brennt: Krisenkommunikation	79
Die Beziehung zur IT und zum Unternehmen	84
Messen, was zählt	92
Netzwerk als Überlebensstrategie	98
Der CISO als Marke	105
Die Psychologie der Sicherheit	111
Der Weg nach vorn	119
Die eigene Entwicklung nicht vergessen	125
Drei Geschichten, die alles zeigen	132
Der erste CISO war kein Techniker	139
Ein letzter Gedanke	142
Werkzeuge für die Praxis	143
Kleines Glossar	151
Über wescaleIT	155
Deine Goodies	157