T.I.S.P./T.P.S.S.E. COMMUNITY MEETING 2026 · BERLIN · 10. NOVEMBER 2026

Umdenken statt Abhaken

Ein Jahr bei Kestner

Handout zum Vortrag, T.I.S.P./T.P.S.S.E. Community Meeting 2026

Kai Jendrian, Secorvo Security Consulting

Firma und Personen sind frei erfunden. Ähnlichkeiten mit realen Firmen, Personen oder Handlungen sind rein zufällig und nicht beabsichtigt. Wer sich trotzdem wiedererkennt, ist in bester Gesellschaft: Die Szenen sind aus vielen Beratungsgesprächen zusammengesetzt, und keine davon ist ein Einzelfall.

Inhalt

Vorbemerkung ... **3**
Die Firma ... 3
Die Personen ... 3
Prolog: Die Vorlage (Februar bis April) ... **4**
Szene 1: Alle sagen Risiko (März bis Mai) ... **5**
Szene 2: Neue Zahlen aus der Holding (Juni) ... **6**
Gleiche Einstufung, andere Reihenfolge ... 6
Zweimal 16 ... 8
Was heißt Risiko 8 in Euro? ... 9
50 000 € weniger ... 10
Szene 3: Wofür die Vorlage kein Feld hat (Juli) ... **11**
Zwei Schätzungen, ein gelbes Feld ... 11
Drei Abteilungen, zwei Szenarien ... 13
Meistens gelb, manchmal grün, zur Saison rot ... 14
Szene 4: Wohin mit den 120 000 €? (September) ... **14**
Frau Brandt zählt zusammen ... 14
Zwei Kandidaten und ein Vergleich, alle grün ... 16
100 000 Jahre Kestner ... 16
Eine Toleranz, die sich prüfen lässt ... 17
Verteilung statt Ordinalzahl ... 18
Lohnt es, genauer zu wissen? ... 19
Szene 5: Wie gut schätzt Kestner? (Oktober) ... **19**
Fünf von zehn statt neun von zehn ... 19
Schlechte Schätzer, und trotzdem simulieren? ... 20
Szene 6: Wer entscheidet was? (Oktober) ... **21**
Der obere Rand bestimmt die Ebene ... 21
Szene 7: Ordnung per Software? (Oktober) ... **22**
Szene 8: Das Audit (November) ... **23**
„Wo ist denn Ihre Risikomatrix?“ ... 23
Wie aus der Verteilung ein Matrixfeld wird ... 24
Auflösung: Die 120 000 € ... **25**
Schlussbemerkung: Kestner hatte Glück ... **25**
Wo Kestner hätte scheitern können ... 25
Wenn Sie sich wiedererkannt haben: drei erste Schritte ... **26**
Epilog: Grenzen der Analyse ... **26**
Anhang ... **28**
A 1 Glossar ... 28
A 2 Schätzvorlage ... 28
A 3 Simulationsskript ... 29
A 4 Die Zuordnungsregel: von der Verteilung ins Feld ... 32
A 5 Zum Weiterlesen ... 32
Kontakt ... 33

Vorbemerkung

Dieser Beitrag ist die Geschichte, die dem Vortrag zugrunde liegt. Sie begleiten eine Informationssicherheitsbeauftragte durch ein Jahr, vom ersten Ausfüllen einer Risikomatrix bis zum Zertifizierungsaudit. Unterwegs stößt sie auf vier Hürden: die Begriffe, die Rechnung, den Ablauf und das Werkzeug. Jede Szene endet mit dem Satz, den sie daraus mitnimmt.

Alles, was im Vortrag nur auf Nachfrage oder in der Kurzfassung gar nicht vorkommt, steht hier an der Stelle, an die es gehört. Längere Rechnungen stehen in eigenen Kästen „Genauer hingeschaut“. Wer nur der Geschichte folgen will, kann sie überspringen. Alle Zahlen und Grafiken sind dieselben wie im Vortrag, gerechnet mit Simulationen, die jede Organisation an einem Nachmittag nachbauen kann.

Der Anhang ist für den Montag nach dem Vortrag gedacht: ein Glossar, eine Schätzvorlage mit ausgefülltem Beispiel, ein kurzes Simulationsskript, die Regel, nach der Kestner seine Matrix für die Holding füllt, und eine Leseliste.

Die Firma

Die Kestner Antriebstechnik GmbH baut Getriebe für Landmaschinen und Fördertechnik. Sie hat rund 200 Beschäftigte, ein Werk und 48 Millionen Euro Umsatz, das Jahresergebnis liegt bei rund 2 Millionen Euro. Ein Großkunde verlangt bis zum Jahresende ein Zertifikat nach ISO/IEC 27001. Aus eigenem Antrieb hätte Kestner es nicht angestrebt, aber ohne Zertifikat verliert die Firma den Kunden. Der Termin steht, das Budget ist knapp.

Die Personen

Nora Albrecht Informationssicherheitsbeauftragte, seit acht Monaten im Amt
Winfried Werkstudent bei Nora
Herr Kübler Leiter der IT, seit fünfzehn Jahren im Haus
Herr Demir Produktionsleitung
Frau Brandt Controlling
Dr. Hesse kaufmännische Geschäftsführerin
Außerdem die Holding, ihr Dienstleister, ein Berater und ein Auditor
Nora und Winfried nennen wir beim Vornamen, alle anderen beim Nachnamen. Nora, weil wir ihr ein Jahr lang über die Schulter schauen und viele ihre Rolle aus eigener Erfahrung kennen. Winfried, weil einen Werkstudenten im Betrieb ohnehin jeder beim Vornamen ruft.

Prolog: Die Vorlage (Februar bis April)

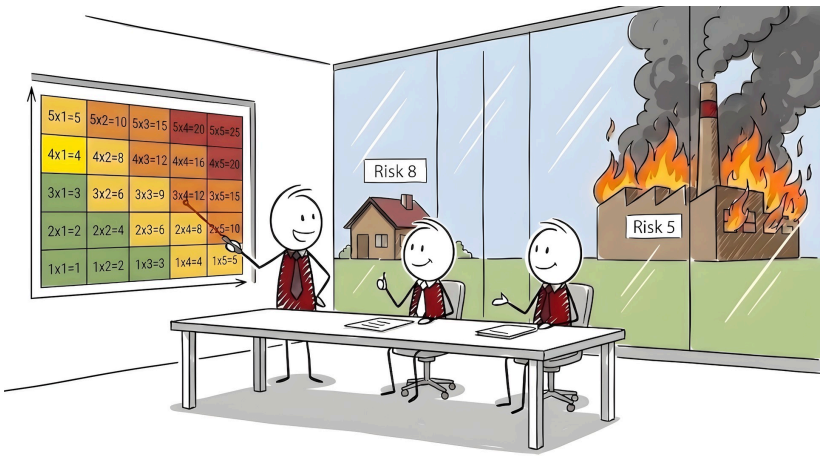


Abbildung 1: Apfel mal Handtuch: Die Matrix multipliziert Stufen, als wären es Zahlen. Das Haus bekommt Risiko 8, das brennende Werk Risiko 5.

Im Februar gibt der Berater, der die Gap-Analyse gemacht hat, Nora eine Excel-Vorlage für die Risikobewertung. Fünf Stufen Wahrscheinlichkeit, fünf Stufen Schaden, das Produkt bestimmt die Farbe. Grün ist alles bis 4, gelb bis 8, orange bis 12, darüber rot. Akzeptiert ist alles bis 8. „Füllen Sie das aus“, sagt der Berater, „dann sind Sie fürs Audit gerüstet.“ Er meint es gut, die Vorlage hat schon viele Audits überstanden. Hinter den Stufen stehen Klassengrenzen: Die Wahrscheinlichkeit reicht von „unter 10 % im Jahr“ bis „80 % und mehr“, der Schaden von „unter 50 000 €“ bis „5 Mio. € und mehr“.

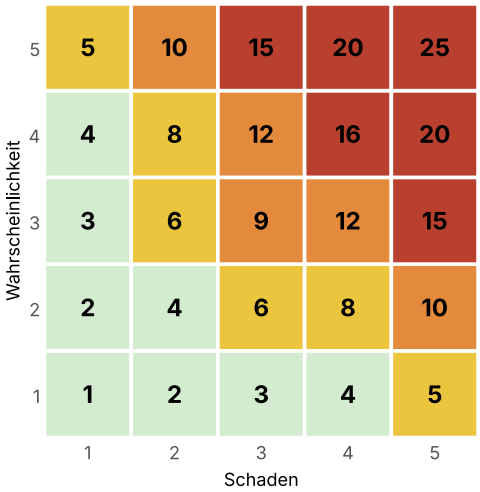


Abbildung 2: Kestners Vorlage: Wahrscheinlichkeit mal Schaden, je fünf Stufen. Akzeptiert ist alles bis 8.

Nora moderiert drei Workshops. Im April liegt das Register vor: 47 Risiken, drei davon rot, acht orange, elf gelb. Formal steht darin alles, was Abschnitt 6.1.2 der Norm verlangt. Nora legt den Bericht der Geschäftsführung vor. Die drei roten Risiken stehen alle im selben Feld: Laut Register kommen sie fast jedes Jahr und kosten jedes Mal einige hunderttausend Euro. Wo Häufiges auf Teures trifft, rechts oben, ist das Register leer.

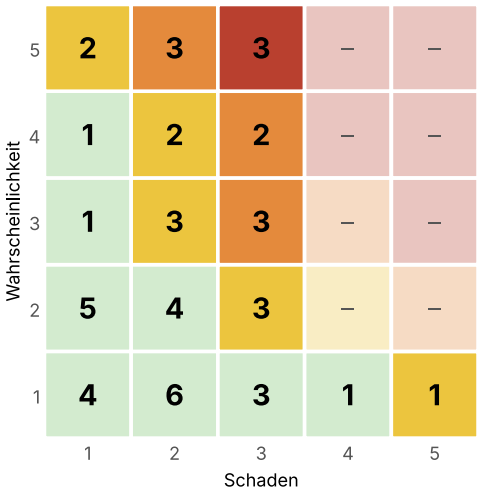


Abbildung 3: Kestners Register im April: Anzahl Risiken je Feld, in den Farben der Vorlage. Rechts oben, wo Häufiges auf Teures trifft, steht nichts.

Dr. Hesse liest den Bericht und sagt: „Schön. Wir haben 120 000 € frei. Wofür?“

Nora blättert im Register und findet keine Antwort. Drei Risiken sind rot, aber welches kostet Kestner im schlechten Jahr am meisten? Was bringt ein Euro wo? Naheliegend wäre: in die roten. Das Kästchen „Risikobewertung“ ist abgehakt, aber besser entscheiden kann die Firma damit nicht. Geprüft hat das auch niemand. Nora will wissen, warum die Antwort fehlt. Bis zum Audit im November stößt sie auf vier Hürden: die Begriffe, die Rechnung, den Ablauf und das Werkzeug. Der rote Faden bleibt die Frage nach den 120 000 €.

> **Was Nora mitnimmt:** Ein vollständiges Register enthält noch keine Antwort auf die Budgetfrage.

Szene 1: Alle sagen Risiko (März bis Mai)

Nora denkt an den Workshop in der Produktion zurück. Innerhalb einer Stunde fielen drei Sätze. Herr Demir: „Das Risiko ist Ransomware.“ Herr Kübler: „Die alten Steuerungsrechner sind ein Risiko.“ Nora selbst: „Das Risiko ist 12.“ Danach stritten sie 40 Minuten darüber, ob die 12 richtig sei.

Erst im Rückblick sieht Nora, dass die drei von verschiedenen Dingen sprachen. Herr Demir meinte eine Bedrohung, Herr Kübler eine Schwachstelle, sie selbst ein Maß für das Risiko. Niemand merkte es, und so waren die Einstufungen weder vergleichbar noch prüfbar. Der Streit um die 12 setzte außerdem voraus, dass es den einen richtigen Wert gibt. Ein Risiko ist aber eine Einschätzung. Herr Demir und Herr Kübler wissen Verschiedenes, deshalb kommen sie zu verschiedenen Ergebnissen, und beide können begründet sein.

> **Was Nora mitnimmt:** Was Risiko ist, hat niemand gesagt. Deshalb haben alle aneinander vorbeigeredet.

Im Mai liest Nora Abschnitt 6.1.2 noch einmal. Bisher hatte sie ihn so gelesen: Die Norm verlangt eine Risikobewertung, die Vorlage hat eine Matrix, fertig. Das ist Abhaken. Jetzt liest sie die Anforderung als Frage, und das ist der Kern des Umdenkens: Die Norm verlangt konsistente, gültige und vergleichbare Ergebnisse. Liefert die Vorlage das? Fast jede Anforderung der Norm ist sinnvoll, aber nicht jede lässt sich nur mit der Vorlage erfüllen. Solange drei Leute mit „Risiko“ drei Dinge meinen, kann keine Vorlage vergleichbare Ergebnisse liefern, egal wie sie rechnet.

Nora lädt zu einem halben Workshoptag ein. Am Ende stehen zwei Seiten Glossar. Der erste Satz übernimmt die Definition aus ISO 31000, die auch ISO/IEC 27000 verwendet: Risiko ist die Auswirkung von Unsicherheit auf Ziele. Ein Risiko misst sich also an Zielen: Wie weit verfehlt Kestner ein Ziel, und wie sicher ist das? Der zweite Satz sagt, dass eine Risikoeinschätzung eine begründete Aussage ist, die sich mit neuem Wissen ändert. Danach trennt das Glossar Bedrohung, Schwachstelle, Szenario und Risiko. Ransomware ist jetzt eine Bedrohung, die alten Steuerungsrechner sind eine Schwachstelle, und die 12 misst ein Risiko, ist aber keines. Als Vorlage dient Nora das Glossar der Society for Risk Analysis. Eine fertige Taxonomie bietet Open FAIR, ein Standard der Open Group, der Risiko in Häufigkeit und Schadenshöhe zerlegt und die Bausteine darunter benennt. Das Glossar im Anhang ist eine Kurzfassung von Noras zwei Seiten.

> **Was Nora mitnimmt:** Vergleichbar wird nur, was alle gleich verstehen. Vor der Matrix steht ein gemeinsames Verständnis der Begriffe, allen voran von Risiko.

Szene 2: Neue Zahlen aus der Holding (Juni)

Im Juni übernimmt eine Industrieholding Kestner. Ab jetzt berichtet Nora im Format des Konzerns, und die Holding schickt ihre eigene Vorlage mit. Sie hat dieselben fünf Schadensklassen von „sehr gering“ bis „sehr hoch“, beschriftet sie aber nicht mit 1 bis 5, sondern mit 1, 2, 4, 8 und 16. Die Wahrscheinlichkeit bleibt bei 1 bis 5, die Farben der Felder bleiben, wie sie sind.

Schadensklasse	sehr gering	gering	mittel	hoch	sehr hoch
Kestner-Vorlage	1	2	3	4	5
Konzernvorlage	1	2	**4**	**8**	**16**

Die Holding begründet das so: Schaden wächst nicht linear, jede Stufe höher kostet ein Vielfaches. Damit hat sie recht. Kestners Schadensklassen enden bei 50 000 €, 250 000 €, 1 Million und 5 Millionen, jede Stufe ist vier- bis fünfmal so teuer wie die vorige. Die neuen Zahlen liegen näher an der Wirklichkeit als 1 bis 5.

Gleiche Einstufung, andere Reihenfolge

Winfried, Noras Werkstudent, rechnet die 47 Risiken an einem Nachmittag neu. An den Einstufungen ändert er nichts, er setzt nur die neuen Zahlen ein. Am nächsten Morgen hat das Register eine andere Reihenfolge. Nora vergleicht zwei Zeilen. Phishing-Mails an Sammelpostfächer kommen fast sicher in jedem Jahr, kosten aber wenig: Wahrscheinlichkeit 5, Schaden 2. Ein Brand im Serverraum kommt sehr selten vor, kostet aber sehr viel: Wahrscheinlichkeit 1, Schaden 5. Mit Kestners Zahlen lag Phishing vorn, 10 gegen 5. Mit den Zahlen der Holding wird aus der 5 eine 16, und der Brand zieht vorbei, 16 gegen 10. „Ich habe nur neu gerechnet“, sagt Winfried. „Warum steht der Brand jetzt vor Phishing?“

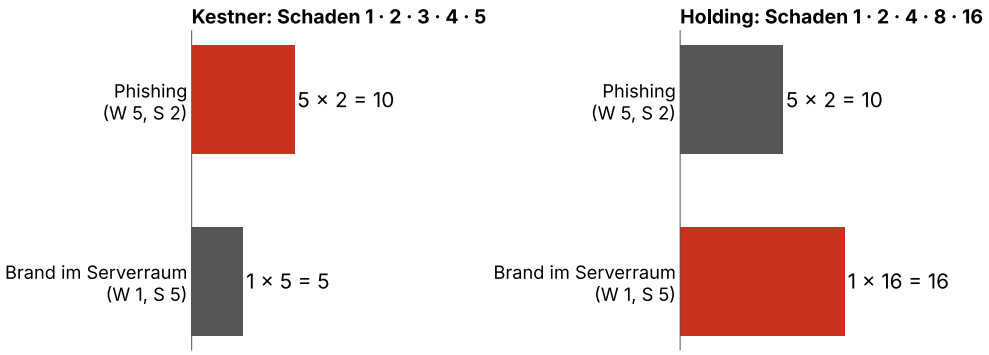


Abbildung 4: Dieselben zwei Risiken, zwei Beschriftungen: Phishing-Mails an Sammelpostfächer und Brand im Serverraum tauschen die Plätze, obwohl sich an der Einstufung nichts geändert hat.

Risiken und Einstufungen sind dieselben geblieben. Die Priorität hängt nur an den Zahlen, die jemand an die Klassen geschrieben hat, und beide Beschriftungen sind gleich gültig. Die Stufen einer Matrix bilden eine Ordinalskala: Sie legen eine Reihenfolge fest, mehr nicht. Auf einer solchen Skala ist jede streng steigende Beschriftung so gut wie jede andere, das hat der Psychologe Stanley Smith Stevens schon 1946 beschrieben. Wer einwendet, die Zahlen der Holding seien näher an der Wirklichkeit, meint Beträge, keine Stufen. Dann lässt sich gleich in Euro schätzen. Genau das tut Nora in Szene 4.

Nora will wissen, ob das ein Zufall dieser zwei Zeilen war. Sie nimmt 15 Risiken aus dem Register, jedes aus einem anderen belegten Feld der Matrix, von W 5 · S 3 bis hinunter zu W 1 · S 1. Bewusst nimmt sie nicht nur die oberen, sie will sehen, ob sich die Liste über die ganze Breite verschiebt. Dann lässt sie den Rechner 2 000 Beschriftungen würfeln, getrennt für Wahrscheinlichkeit und Schaden. Die einzige Regel lautet: Jede Stufe bekommt eine größere Zahl als die vorige. Die erste Stufe heißt immer 1, jede weitere liegt um einen zufälligen Abstand höher. Mehr verlangt eine Stufenskala nicht.

Tabelle 2: Vier gleich gültige Beschriftungen und der Platz des Brands unter den 15 Risiken.

Beschriftung	Wahrscheinlichkeit	Schaden	Brand im Serverraum (W 1 · S 5)
Kestner-Vorlage	1 · 2 · 3 · 4 · 5	1 · 2 · 3 · 4 · 5	1 × 5 = 5, Platz 7
Konzernvorlage	1 · 2 · 3 · 4 · 5	1 · 2 · 4 · 8 · **16**	1 × 16 = 16, **Platz 2**
gewürfelt	1 · 1,2 · 1,8 · 2,5 · 2,8	1 · 1,4 · 1,9 · 6,4 · **10,1**	1 × 10,1 = 10,1, **Platz 1**
gewürfelt	1 · 5,4 · 6,3 · 7,8 · 8,6	1 · 1,2 · 1,9 · 2 · **2,2**	1 × 2,2 = 2,2, **Platz 11**

Weil die unterste Stufe immer 1 heißt, ist der Wert des Brands immer die Zahl an der obersten Schadensstufe. Mit Kestners Zahlen liegt er auf Platz 7, gleichauf mit W 5 · S 1. Mit den Zahlen der Holding steht nur noch das rote Feld W 5 · S 3 davor, 5 × 4 = 20. In der ersten gewürfelten Reihe reicht der Schaden bis 10,1, die Wahrscheinlichkeit nur bis 2,8, und der Brand steht vor allen roten und orangen Risiken. In der zweiten reicht der Schaden nur bis 2,2, die Wahrscheinlichkeit springt schon bei Stufe 2 auf 5,4, und zehn der 15 Risiken ziehen am Brand vorbei. Keine der vier Reihen ist falscher als die anderen.

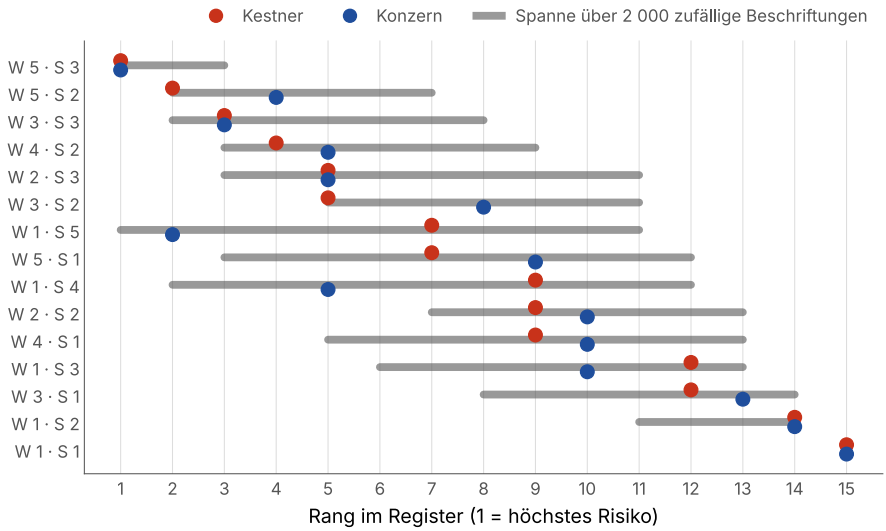


Abbildung 5: 15 Risiken, 2 000 zufällige Beschriftungen. Jede Zeile ist ein Risiko, sortiert nach dem Platz mit 1 bis 5. Grau: die Spanne der Plätze, die ein Risiko je nach Beschriftung einnimmt. Kestners Vorlage und die der Holding sind zwei Beschriftungen von vielen.

Über alle 2 000 Beschriftungen überstreicht ein Risiko im Mittel gut sechs Plätze. Fest steht nur das kleinste Risiko, W 1 · S 1. Selbst das größte, das rote W 5 · S 3, rutscht bis auf Platz 3. Dazwischen entscheidet, wer die Vorlage gebaut hat.

Was Nora mitnimmt: Die Rangfolge hängt an den Zahlen für die Stufen, nicht an den Risiken.

Genauer hingeschaut: 25 Felder, 14 verschiedene Werte. Eine 5×5-Matrix hat 25 Felder, aber nicht 25 verschiedene Werte. In Kestners alter Vorlage gibt es nur 14. Die 4 kommt dreimal vor (1 × 4, 2 × 2, 4 × 1), die 2, 3, 5, 6, 8, 10, 12, 15 und 20 je zweimal. Die Konzernvorlage hat 17 Werte, und die 16 steht dreimal da: bei W 1 · S 5, W 2 · S 4 und W 4 · S 3. Kestners 47 Risiken belegen 17 Felder, bekommen aber nur 11 verschiedene Werte. Gleichstände entstehen also genau dort, wo die Risiken verschieden sind.

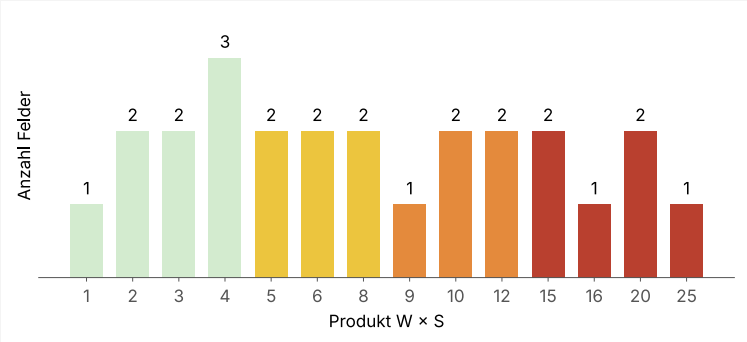


Abbildung 6: Kestners alte Vorlage: 25 Felder, 14 verschiedene Werte.

Zweimal 16

In der nächsten Sitzung der Geschäftsführung legt Nora das Register im Format der Holding vor. Dr. Hesse geht die Liste von oben durch. Zwei Zeilen haben den Wert 16. In der einen fällt in zwei von drei Jahren beim Gussteil-Lieferanten die IT aus, etwa durch Ransomware. Seine Lieferungen stocken, und die Montage steht zwei Tage still: Wahrscheinlichkeit 4, Schaden 3, also 4 × 4. Die andere ist der Brand im Serverraum, einmal in Jahrzehnten, danach steht das Werk: 1 × 16. „Beide 16“, sagt Dr. Hesse.

„Dann machen wir für beide dasselbe.“ Das eine Risiko braucht aber Vorbeugung, das andere einen Notfallplan und eine Versicherung.

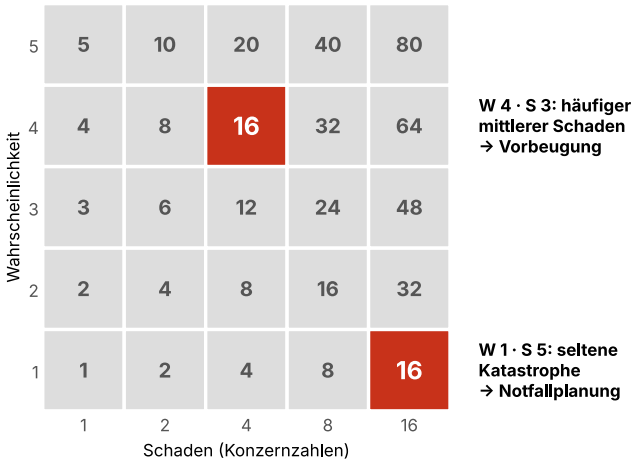


Abbildung 7: Zweimal 16 in der Konzernvorlage: ein häufiger mittlerer Schaden und eine seltene Katastrophe.

Die Holding hatte ihre Zahlen eingeführt, damit große Schäden mehr zählen. Trotzdem landet die Katastrophe auf derselben Zahl wie der häufige mittlere Schaden. Eine andere Beschriftung verschiebt nur, welche Risiken zusammenfallen, denn eine Zahl bildet zwei Dimensionen nicht ab. Selbst bei gleichem erwartetem Verlust bräuchten die beiden verschiedene Maßnahmen.

Warum steht ein Lieferant überhaupt im Register der Informationssicherheit? Die Ursache ist ein IT-Ausfall beim Lieferanten, und damit geht es um die Sicherheit der Lieferkette. ISO/IEC 27001:2022 behandelt sie in Anhang A 5.19 bis 5.22, die NIS-2-Richtlinie in Art. 21 Abs. 2 Buchst. d. Kestner ist als mittleres Unternehmen des Maschinenbaus voraussichtlich eine wichtige Einrichtung im Sinne von NIS 2, im Einzelfall wäre das zu prüfen.

> **Was Nora mitnimmt:** Ein Wert zeigt nicht, ob ein Risiko häufig oder schwer ist. Das eine braucht Vorbeugung, das andere einen Notfallplan.

Was heißt Risiko 8 in Euro?

Frau Brandt aus dem Controlling sieht das Register zum ersten Mal. Bei Ransomware steht eine 8. „Was heißt Risiko 8 in Euro?“, fragt sie. Im Controlling ist das die naheliegende Frage: Wie viel Verlust im Jahr steckt dahinter? Nora sucht alle Felder mit diesem Wert und rechnet mit den Klassengrenzen nach, untere Grenze mal untere Grenze, obere mal obere.

Tabelle 3: Drei Felder mit dem Wert 8 in der Konzernvorlage.

Feld mit Wert 8	Wahrscheinlichkeit im Jahr	Schaden je Ereignis	erwarteter Verlust im Jahr
W 1 · S 4 (1 × 8)	unter 10 %	1 bis 5 Mio. €	0 bis 500 000 €
W 2 · S 3 (2 × 4)	10 bis 30 %	250 000 € bis 1 Mio. €	25 000 bis 300 000 €
W 4 · S 2 (4 × 2)	50 bis 80 %	50 000 bis 250 000 €	25 000 bis 200 000 €

Zusammen reicht der erwartete Jahresverlust in diesen Feldern von fast null bis 500 000 €. Noras eigene Schätzung für Ransomware lautet 8 Prozent im Jahr, typisch 1 Million Schaden, schlimmstenfalls 4 Millionen. Im Mittel sind das 112 000 € im Jahr. Die Zahl liegt in der Spanne, an der 8 lässt sie sich nicht ablesen. Mit Kestners alter Vorlage wäre es nicht besser: Dort hat die 8 zwei Felder, W 2 · S 4 und W 4 · S 2, zusammen 25 000 € bis 1,5 Mio. € im Jahr. Ransomware stünde dort auf 4, erst die Zahlen der Holding machen eine 8 daraus.

„Dann zeichne ich das mal maßstabsgetreu“, sagt Frau Brandt. Sie trägt die Felder auf echten Achsen auf, die Wahrscheinlichkeit linear, den Schaden logarithmisch, jede Marke ein Faktor 10. Die Felder sind

plötzlich sehr verschieden groß, das rote Feld rechts oben reicht von 5 Millionen bis ins Unendliche. Linien gleichen erwarteten Verlusts, 10 000 €, 100 000 € und 1 Mio. € im Jahr, laufen quer durch die Farben. „Bei uns im Controlling“, sagt sie, „wäre das ein Fehler im Berichtswesen.“

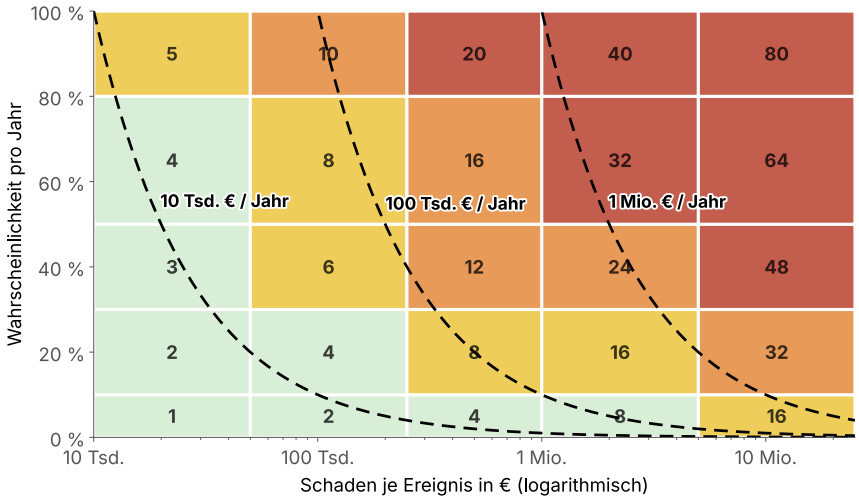


Abbildung 8: Die Matrix auf echten Achsen: Wahrscheinlichkeit linear, Schaden logarithmisch. Gestrichelt: gleicher erwarteter Jahresverlust.

Wie oft das zu falschen Entscheidungen führt, zeigt eine Simulation mit zufälligen Risikopaaren, gleichmäßig über die Fläche verteilt. Bei jedem sechsten Paar gleicher Farbe liegt der erwartete Verlust mehr als den Faktor 10 auseinander. Bei knapp 7 Prozent der Paare verschiedener Farbe steht die Ampel sogar falsch herum. Die Anteile hängen an der Annahme, wie die Risiken verteilt sind, das Muster nicht. Es folgt allein aus Klassengrenzen und Farben und gilt für Kestners alte Vorlage genauso wie für die der Holding.

> **Was Nora mitnimmt:** Risiko 8 heißt irgendwo zwischen fast null und 500 000 € im Jahr. Gleiche Farbe heißt nicht gleiches Risiko.

50 000 € weniger

Im Frühjahr hat Herr Kübler zum ersten Mal geübt, die Produktions-IT aus der Datensicherung wiederherzustellen. Nach einem Ransomware-Angriff liefe die Fertigung nach neuneinhalb statt zehn Tagen wieder. Jetzt, im Juni, füllt Herr Demir den Fragebogen der Cyberversicherung aus. Gefragt sind die Wiederanlaufzeit und der Schaden je Stillstandstag, und Herr Demir rechnet den Ransomware-Schaden in der Produktion mit dem neuen Wert nach: Stillstand, Nacharbeit, Vertragsstrafen. Ein Stillstandstag kostet Kestner rund 100 000 € Deckungsbeitrag.

Im Register stand bisher 1 Million, genau auf der Grenze zur Schadensklasse 4. Herr Demir kommt auf 950 000 €, fünf Prozent weniger. Damit rutscht die Schätzung unter die Grenze, der Matrixwert halbiert sich von 8 auf 4, und Ransomware fällt im Register hinter alle Risiken mit 5, 6 oder 8 zurück. Der erwartete Verlust sinkt nur von 112 000 auf 107 000 € im Jahr. Ein Schaden von 300 000 € bekäme dieselbe 4, obwohl sein erwarteter Verlust mit 34 000 € nur ein Drittel beträgt. „Wir sind doch nur einen halben Tag schneller“, sagt Herr Demir. Die Verbesserung ist echt, aber klein. In der Matrix sieht sie aus, als wäre das Problem halb gelöst.



Abbildung 9: Klassengrenze bei 1 Million: 50 000 € weniger halbieren den Matrixwert, 650 000 € weniger ändern ihn nicht.

Versichert ist der Stillstand noch nicht. Der Versicherer will vor der Deckung Mindestmaßnahmen sehen. Den Wiederanlauftest hat Kestner bestanden, die Trennung der Produktions-IT vom Büronetz fehlt noch. Bis dahin ist die Betriebsunterbrechung durch Ransomware von der Deckung ausgeschlossen.

> **Was Nora mitnimmt:** Ein kleiner Schritt über die Klassengrenze kippt die Priorität. Ein großer innerhalb der Klasse ändert nichts.

Nora notiert sich einen Satz für später: Als Bild taugt die Matrix weiter, als Rechnung mit Stufen nicht.

Szene 3: Wofür die Vorlage kein Feld hat (Juli)

Bis hierher ging es darum, was die Vorlage falsch rechnet. Im Juli zeigt sich, wofür sie gar kein Feld hat: wie unsicher eine Schätzung ist.

Zwei Schätzungen, ein gelbes Feld

Nora fragt Herrn Kübler und Herrn Demir nach einem Szenario: Ein fehlerhaftes Update des Dienstleisters legt die Fertigungssteuerung lahm. Wie oft, wie teuer? Herr Kübler ist seit fünfzehn Jahren im Haus und betreut den Dienstleister von Anfang an. Er hat die letzten drei Updates begleitet und ist sich sicher: 15 bis 25 Prozent im Jahr, 300 000 bis 550 000 €. „Nach zwei Tagen läuft es wieder“, sagt er. Was ein Stillstandstag kurz vor der Saison kostet, hat er nicht im Blick. Seine Bandbreite passt in ein einziges Feld.

Herr Demir hatte mit dem Dienstleister nie zu tun. Wie oft ein Update schiefgeht, weiß er nicht, er nennt 5 bis 60 Prozent. Dafür weiß er, was die IT nicht sieht: In den sechs Wochen vor dem Saisonstart der Erntemaschinen kostet jeder Stillstandstag das Fünffache. Beim Schaden nennt er 50 000 € bis 2,5 Millionen. Seine Bandbreite reicht über zwölf Felder, von Grün bis Rot. Die beiden streiten, ob das Risiko gelb ist oder rot, nach demselben Muster wie im März beim Streit um die 12. In der Vorlage zählt aber nur der typische Wert, und der liegt bei beiden im selben gelben Feld. Ist der Streit damit beendet?

Nora zieht aus beiden Bandbreiten Tausende mögliche Ausfälle. Bei Herrn Kübler landet fast jeder im gelben Feld. Bei Herrn Demir verteilen sie sich auf 14 der 25 Felder, und im Feld seines typischen Werts liegt nicht einmal jeder fünfte.

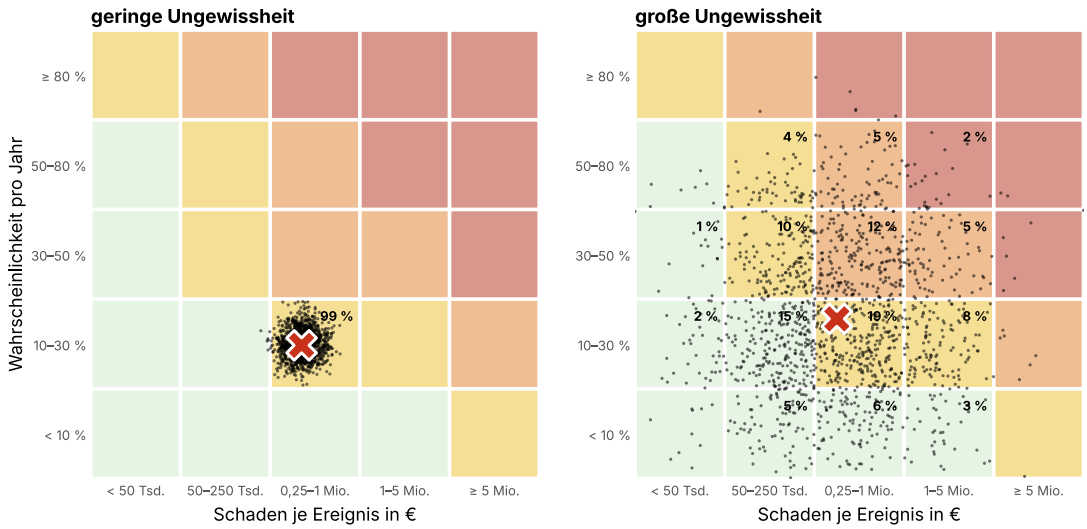


Abbildung 10: Jeder Punkt ist ein möglicher Ausfall. Links die Schätzung von Herrn Kübler, rechts die von Herrn Demir. Das Kreuz markiert den typischen Wert, der in der Vorlage zählt.

Herr Demir hatte im Workshop genau das gesagt: „Meistens gelb, manchmal grün, zur Saison rot." Recht hatten beide, jeder mit seinem Teil. Herr Kübler kennt die Updates und ist sich sicher, Herr Demir weiß, wovon der Schaden abhängt. Seine weite Bandbreite hat zwei Gründe: Über die Updates fehlt ihm Wissen, und der Schaden selbst schwankt, je nachdem, wann der Ausfall kommt. Im Feld steht dieser Unterschied nicht.

Was Nora mitnimmt: In einem Feld steht nicht, wie unsicher die Schätzung ist.

Genauer hingeschaut: Der typische Wert unterschätzt. Die Bandbreite von Herrn Demir, noch vor der Update-Sperre (siehe Szene 4), hat eine weitere Folge. Schäden sind rechtsschief: nie negativ, viele Ausfälle kosten wenig, wenige sehr viel. In der Praxis, etwa bei Hubbard und Seiersen und in Werkzeugen für Open FAIR, beschreibt man sie deshalb meist mit einer logarithmischen Normalverteilung. Die beiden Ränder der 90-%-Bandbreite legen sie vollständig fest, der 5-%-Punkt P5 und der 95-%-Punkt P95. Der Median ist die Wurzel aus P5 mal P95, der Mittelwert liegt deutlich darüber. Bei Noras Ransomware-Schätzung aus Szene 4, 250 000 € bis 4 Mio. €, ist der Median √(250 000 × 4 000 000) = 1 Mio. €, der Mittelwert 1,4 Mio. €. Wie man P5 und P95 gut schätzt, zeigt Szene 5.

Bei Herrn Demir, 50 000 € bis 2,5 Mio. €, liegt der typische Schaden, der Median, bei rund 350 000 €, der Mittelwert über alle Fälle bei rund 720 000 €. Nach der Vorlage ergeben die typischen Werte, rund 26 Prozent mal 350 000 €, rund 90 000 € im Jahr. Mit allen möglichen Fällen gerechnet sind es rund 200 000 € im Jahr, mehr als doppelt so viel. Wenige teure Fälle ziehen den Mittelwert hoch. Wer nur den typischen Wert einträgt, unterschätzt, und zwar umso mehr, je unsicherer die Schätzung ist.

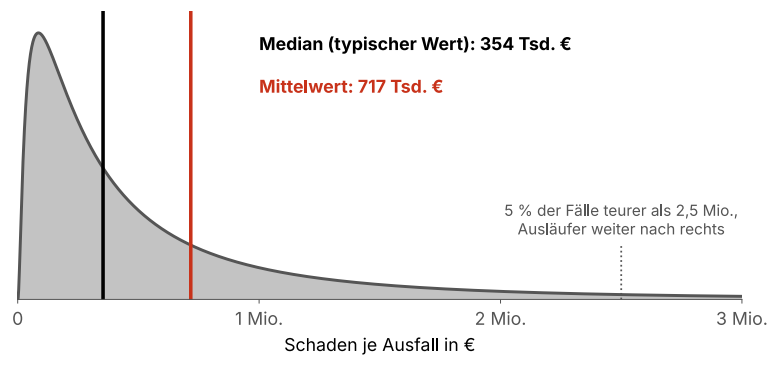


Abbildung 11: Schätzung von Herrn Demir für die Fertigungssteuerung: wie sich die möglichen Schäden je Ausfall verteilen. Der lange Ausläufer nach rechts zieht den Mittelwert weit über den typischen Wert.

Genauer hingeschaut: Eine Annahme, keine Tatsache. Die logarithmische Normalverteilung ist ein Modell mit langem rechtem Ausläufer. Bei sehr weiten Bandbreiten erzeugt sie einzelne Schäden, die niemand für möglich hält. Dann kappt man sie bei einem plausiblen Höchstwert, etwa der Summe, bei der Kestner insolvent wäre. Umgekehrt kann sie echte Extremfälle unterschätzen. Für die Entscheidung zählt deshalb weniger die genaue Form als die Frage, ob das Ergebnis hält, wenn sich P5 und P95 verschieben. Wie Nora das prüft, zeigt der Abschnitt „Hält die Toleranz?“ in Szene 4.

Drei Abteilungen, zwei Szenarien

Im nächsten Workshop steckt die Unsicherheit nicht in einer Schätzung, sondern zwischen den Schätzungen. Nora fragt Vertrieb, IT und Konstruktion, was es kostet, wenn Konstruktionsdaten abfließen. Der Vertrieb denkt an Angebote und Preislisten und sagt 1: „Da sind doch nur Angebote drin.“ Die IT will wissen, welche Daten gemeint sind, und legt sich in die Mitte, auf 3. Die Konstruktion denkt an die Zeichnungen, mit denen ein Wettbewerber das Getriebe in einem Jahr nachbaut, und sagt 5. Die Excel-Datei bildet den Mittelwert: 3.

Beim Ausfall des ERP-Systems sind sich dagegen alle einig: „Zwei Tage ohne ERP, dann stehen Einkauf und Versand.“ Dreimal 3, Mittelwert 3.

Was kostet es, wenn …	Konstruktionsdaten abfließen?	das ERP-System ausfällt?
Vertrieb	1	3
IT	3	3
Konstruktion	5	3
Mittelwert in der Excel-Datei	**3**	**3**

Im Register stehen beide Risiken mit 3 nebeneinander, obwohl die Runde beim einen einig war und beim anderen vier Stufen auseinanderlag. Alle drei Abteilungen haben recht: Der Schaden hängt daran, welche Daten abfließen, und das weiß heute niemand. Der Mittelwert verschluckt diese Unsicherheit wie das gelbe Feld bei Herrn Demir.

Was Nora mitnimmt: Auch Uneinigkeit ist Unsicherheit. Der Mittelwert macht aus 1 und 5 eine 3.

Genauer hingeschaut: Gleiche Stimmen, andere Mittelwerte. Nora rechnet die Stimmen aus dem Workshop auch in der Konzernvorlage nach. Mit Kestners Stufen ergeben beide Risiken im Mittel 3, sie stehen gleichauf. Mit den Zahlen der Holding wird aus 1, 3 und 5 ein 1, 4 und 16, im Mittel 7. Der ERP-Ausfall kommt auf dreimal 4. Niemand hat seine Meinung geändert, trotzdem liegt der Datenabfluss jetzt fast beim Doppelten. Ein Mittelwert braucht Abstände zwischen den Stufen. Die

liefert erst die Beschriftung, und die ist willkürlich. Der Median, also die mittlere Stimme, besteht die Probe: Er bleibt bei beiden Beschriftungen die Stufe „mittel“. Den Streit zwischen Vertrieb und Konstruktion zeigt aber auch er nicht.

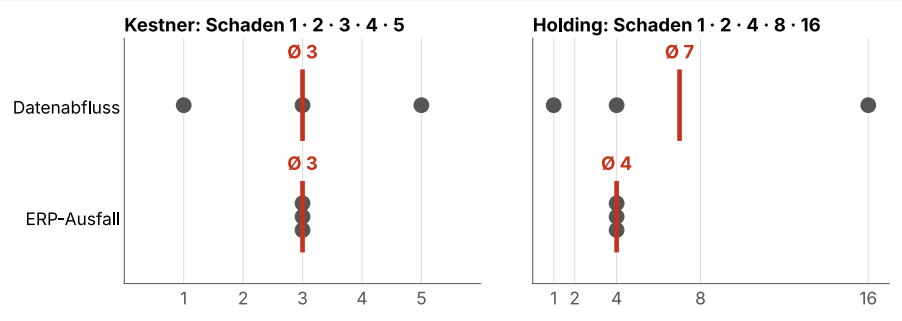


Abbildung 12: Dieselben Stimmen, zwei Beschriftungen: Mit Kestners Stufen stehen Datenabfluss und ERP-Ausfall gleichauf, mit den Zahlen der Holding liegt der Datenabfluss fast beim Doppelten.

Stufen sagen nur, was größer ist, nicht um wie viel. Einen Mittelwert gibt es auf ihnen nicht.

Meistens gelb, manchmal grün, zur Saison rot

Nora ändert das Register. Es bekommt drei neue Spalten: günstig, typisch, ungünstig. Die Bandbreite steht auf der vorhandenen Farbskala, die Holding bekommt weiter ihre Ampel. Beim Datenabfluss steht jetzt günstig 1 und ungünstig 5 statt der 3, bei der Fertigungssteuerung nach Herrn Demir grün bis rot statt nur gelb. Die Ränder multipliziert Nora nicht miteinander, sonst wäre sie beim Problem aus Szene 2. Dafür braucht es weder eine neue Skala noch Software. Auch der BSI-Standard 200-3 zeichnet solche Bandbreiten in seinem Anhang als Balken in die Matrix. Für viele Organisationen ist das schon ein ausreichendes Ziel.

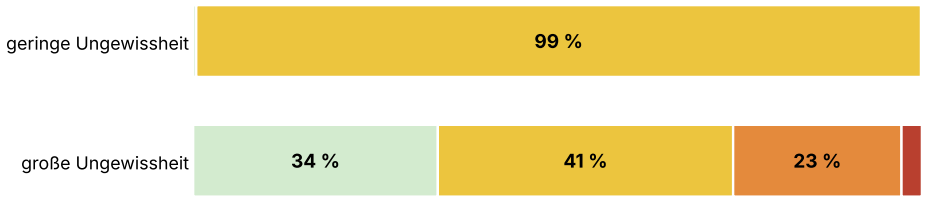


Abbildung 13: Anteil der möglichen Ausfälle je Farbe. Bei Herrn Kübler fast nur gelb, bei Herrn Demir meistens gelb, manchmal grün, zur Saison orange und rot.

Was Nora mitnimmt: Ins Register gehört die Bandbreite, nicht nur der typische Wert.

Szene 4: Wohin mit den 120 000 €? (September)

Im September kommt die Budgetrunde, und Dr. Hesse will wissen, wohin die 120 000 € gehen. „Und die drei roten Risiken aus dem April?“, fragt sie. Das liegt nahe: Rot ist die höchste Farbe im Register. Die Antwort hat Frau Brandt.

Frau Brandt zählt zusammen

Vor der Budgetrunde hat Frau Brandt getan, was im Controlling naheliegt: Sie hat das Register in Euro umgerechnet. Für jedes Feld nimmt sie die Mitte der Wahrscheinlichkeitsklasse und den mittleren Schaden der Schadensklasse. Ransomware, Datenabfluss und Zahlungsbetrug lässt sie weg, weil Nora

sie einzeln rechnet. Auch den Brand im Serverraum lässt sie weg, ihn deckt die Feuerversicherung. Für die übrigen 43 Risiken ergibt das Register rund 4 Millionen Euro Schaden im Jahr, drei Viertel davon aus Rot und Orange. „Laut Register verlieren wir jedes Jahr doppelt so viel, wie wir verdienen", sagt Frau Brandt. „Das Register kann nicht stimmen." In der Buchhaltung findet sie für solche Fälle im Vorjahr rund 180 000 €: Phishing an Sammelpostfächer, Nacharbeit, ein paar Stunden Ausfall, zwei Tage Montagestillstand nach dem IT-Ausfall beim Gussteil-Lieferanten. Einen einzelnen Fall über 150 000 € findet sie in den letzten Jahren nicht.

Im August haben Nora und die Abteilungen die übrigen Risiken deshalb neu geschätzt, in Euro statt in Stufen: für jedes Risiko, wie oft es im Jahr eintritt und was ein Fall kostet, mit Bandbreite. Die Einstufung „häufig" stimmt meist, „teuer" nicht. Die roten und orangen Risiken haben „mittel" bekommen, weil sie lästig sind, nicht weil sie viel kosten. Im Workshop hieß „mittel" „spürbar", in der Vorlage heißt es 250 000 € bis 1 Mio. € je Fall. Fast jeder häufige Fall bleibt unter 50 000 €. Zusammen erwartet Kestner damit rund 170 000 € im Jahr, und die Buchhaltung bestätigt die Größenordnung. Gebucht ist, was in einem einzigen Jahr passiert ist. Die neue Schätzung ist, was Kestner im Schnitt erwartet, seltene Fälle eingerechnet. Dass beide fast gleich sind, zeigt: Nicht das Vorjahr war ein Glücksfall, das Register ist falsch.

Tabelle 5: Was das Register behauptet und was Kestner tatsächlich verliert. Ohne Ransomware, Datenabfluss, Zahlungsbetrug und den versicherten Brand. Jahresergebnis rund 2 Mio. €.

Schaden im Jahr	43 übrige Risiken	davon rot und orange (11)
laut Register, über die Klassengrenzen	rund 4 Mio. €	3,1 Mio. €
gebucht im Vorjahr, kein Einzelfall über 150 000 €	rund 180 000 €	
neu geschätzt, in Euro statt in Stufen	rund 170 000 €	rund 110 000 €

Die drei roten sind genau solche Fälle. Alle drei stehen im selben Feld, W 5 · S 3: fast jedes Jahr, mittlerer Schaden. Das Netz in der Halle ist für ein paar Stunden weg, und die Maschinen warten auf Aufträge. An einer Maschine liegt ein veralteter Zeichnungsstand, und die Teile müssen nachgearbeitet werden. Ein Notebook oder Handy aus Außendienst oder Service geht verloren oder wird gestohlen. Die acht orangen sehen bis auf eines genauso aus: Phishing an Sammelpostfächer, ein Angebot an den falschen Empfänger, Schadsoftware über den USB-Stick eines Servicetechnikers, der CAD-Lizenzserver fällt aus und die Konstruktion wartet.

Laut Register kosten die elf roten und orangen zusammen 3,1 Millionen Euro im Jahr, die drei roten allein 1,4 Millionen. Neu geschätzt kommt jeder Fall auf einige tausend bis 30 000 €, nur die Lieferantenstörung auf bis zu 150 000 €. Zusammen erwartet Kestner für die elf rund 110 000 € im Jahr, für die drei roten rund 30 000 €. Rot und Orange hieß bei Kestner: häufig, nicht teuer. Darum kümmern sich die IT und die Abteilungen mit kleinen Maßnahmen aus dem laufenden Budget, etwa Notebook-Verschlüsselung mit Fernlöschen, einer Zeichnungsfreigabe, die alte Stände sperrt, und einer redundanten Anbindung der Halle. Aus den 120 000 € kommt dafür nichts.

Nach dem oberen Rand gehören diese Risiken in die Abteilungen und in die Sicherheitsrunde, nicht zu Dr. Hesse (wie die Ebenen funktionieren, zeigt Szene 6). Die Ausnahme ist die Lieferantenstörung, das eine orange Risiko mit größerem Schaden: In zwei von drei Jahren kostet sie 20 000 bis 150 000 €, weil Sonderschichten den Großteil der Montage nachholen. Mit diesem oberen Rand geht sie als eigener Antrag über den Einkauf an Dr. Hesse, eine Million erreicht sie aber nicht.

Warum ist das niemandem aufgefallen? Stufen lassen sich nicht addieren. „Passiert ständig" und „mittel" ergeben in Euro Unsinn, aber das sieht erst, wer in Euro rechnet. Euro lassen sich zusammenzählen und mit der Buchhaltung abgleichen.

> **Was Nora mitnimmt:** Stufen lassen sich nicht addieren. Darum fiel niemandem auf, dass sie nicht stimmen.

Zwei Kandidaten und ein Vergleich, alle grün

Die 120 000 € gehören dorthin, wo ein einzelnes Jahr teuer werden kann. Daraus folgt Noras Auswahlregel: Einzeln simuliert sie, was allein ein Millionenjahr auslösen kann, ungeplant und unversichert. Nach der neuen Schätzung bleiben Ransomware und Datenabfluss. Den Zahlungsbetrug nimmt sie zum Vergleich dazu, weil er im Vorjahr fast passiert wäre. Der Brand reicht weit über eine Million, aber die Versicherung deckt ihn. Der Ausfall der Fertigungssteuerung reichte in der Schätzung von Herrn Demir bis 2,5 Millionen. Nach dem Streit aus dem Juli spielt der Dienstleister in den sechs Wochen vor dem Saisonstart keine Updates mehr ein. Damit reicht der Ausfall der Fertigungssteuerung nur noch bis 400 000 €.

Nora schätzt alle drei in Prozent und Euro, mit Bandbreite. Ransomware in der Produktion tritt mit 8 Prozent im Jahr ein und kostet 250 000 € bis 4 Millionen, typisch 1 Million. Dafür setzt sie sich mit Herrn Kübler, Herrn Demir und Frau Brandt noch einmal zusammen, und die 950 000 € von Herrn Demir aus dem Juni liegen mitten in der neuen Bandbreite. Die Cyberversicherung deckt den Ransomware-Stillstand noch nicht, Nora rechnet deshalb ohne sie. Der Ransomware-Schutz wäre zugleich die Mindestmaßnahme, die der Versicherer noch verlangt. Der Abfluss der Konstruktionsdaten, also der Zeichnungen, tritt mit 5 Prozent ein und kostet 100 000 € bis 2 Millionen, genauer geschätzt als im Juli. Zahlungsbetrug, also eine gefälschte Mail eines Gussteil-Lieferanten mit neuer Bankverbindung, tritt mit 25 Prozent ein und kostet 20 000 bis 400 000 €. Im Vorjahr hat die Buchhaltung so einen Fall erst beim Rückruf bemerkt. Er ist häufig, aber eine Million erreicht er nicht.

Tabelle 6: Noras drei Szenarien. „90 %“ heißt: Der Schaden eines Falls liegt mit 90 Prozent Sicherheit in dieser Bandbreite.

Szenario	Wahrscheinlichkeit im Jahr	Schaden je Fall (90 %)	Konzernvorlage
Ransomware Produktion	8 %	250 000 € bis 4 Mio. €	1 × 8 = 8, grün
Abfluss Konstruktionsdaten	5 %	100 000 € bis 2 Mio. €	1 × 4 = 4, grün
Zahlungsbetrug	25 %	20 000 bis 400 000 €	2 × 2 = 4, grün

In der Konzernvorlage zählt der typische Wert: Ransomware 8, Datenabfluss 4, Zahlungsbetrug 4. Datenabfluss und Zahlungsbetrug sind damit gleich wichtig, alle drei Felder sind grün. Nach der Vorlage müsste Kestner nichts tun, und die 120 000 € könnten irgendwohin. Die Millionenrisiken liegen dort, wo im Prolog niemand hingesehen hat: unten rechts, im Grünen.

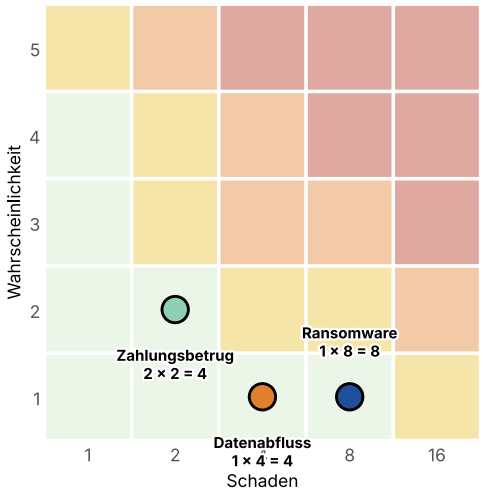


Abbildung 14: Wo die Konzernvorlage die drei Szenarien einordnet: alle im grünen Bereich.

100 000 Jahre Kestner

Nora spielt 100 000 Jahre Kestner durch. In jedem Jahr bestimmt ein Zufallszug je Szenario, ob es eintritt, und ein zweiter, wie teuer es wird. Im Mittel kostet Ransomware 112 000 € im Jahr, mehr als dreimal so viel wie Zahlungsbetrug mit 34 000 und Datenabfluss mit 33 000 €. So weit liegt die Vorlage richtig. Dann fragt Nora, wie oft ein Szenario allein ein Jahr mit mehr als einer Million Verlust verursacht.

Bei Ransomware sind es 4,0 Prozent, fast vierzigmal so oft wie beim Zahlungsbetrug mit 0,1 Prozent. Beim Datenabfluss sind es 0,9 Prozent.

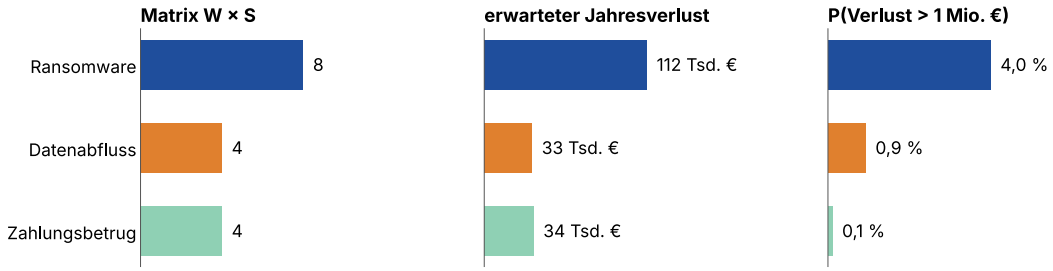


Abbildung 15: Drei Maße, drei Rangfolgen: Matrixwert, erwarteter Jahresverlust und Wahrscheinlichkeit eines Millionenjahrs.

„Datenabfluss und Betrug standen bei uns gleichauf?“, fragt Dr. Hesse. Ja: Sie haben in der Vorlage denselben Wert und fast denselben erwarteten Verlust, aber das Millionenrisiko des Datenabflusses ist neunmal so hoch. Das zeigt weder die Matrix noch der erwartete Verlust allein. Hätte Nora die Punktschätzung von Herrn Demir übernommen, 950 000 statt 1 Million, stünde auch Ransomware in der Vorlage bei 4, gleichauf mit den beiden anderen.

> **Was Nora mitnimmt:** Gleicher Wert in der Vorlage, aber neunfaches Millionenrisiko beim Datenabfluss.

Eine Toleranz, die sich prüfen lässt

Die Holding will als Gesellschafterin wissen, wie viel Verlust Kestner verkraftet. Frau Brandt übersetzt die Frage in eine Zahl: „Eine Million, das ist unser halbes Jahresergebnis.“ Ein Verlust über eine Million soll höchstens in einem von zwanzig Jahren vorkommen, also mit höchstens 5 Prozent Wahrscheinlichkeit.

Die Verlustüberschreitungskurve zeigt, wie oft ein Jahr mehr kostet als ein bestimmter Betrag. Man liest sie von unten nach oben: Über jedem Betrag steht, mit welcher Wahrscheinlichkeit der Verlust eines Jahres ihn übersteigt. Links ist jede Kurve flach. Dort lässt sich nur ablesen, wie oft ein Szenario überhaupt eintritt, denn wenn es eintritt, kostet es gleich Hunderttausende. Steil fällt sie erst im Bereich der Schadensbandbreiten. Für alle drei Szenarien zusammen zeigt sie bei einer Million gut 5 Prozent. Die Toleranz reißt knapp.

Dann nimmt Nora das ganze Register dazu: die drei Szenarien und die 43 übrigen Risiken von Frau Brandt, in Euro neu geschätzt. Die übrigen Risiken kosten fast jedes Jahr etwas, im Mittel 170 000 €, in 19 von 20 Jahren zwischen 70 000 und 330 000 €. Darum kommt ein Ransomware-Fall schneller über die Million. Mit dem ganzen Register liegt ein Millionenjahr bei 6,5 Prozent, die Toleranz reißt deutlicher. Eine Einschränkung nennt Nora gleich mit: Sie hat die Szenarien als unabhängig voneinander simuliert. Eine doppelte Erpressung, bei der Angreifer verschlüsseln und zugleich Daten abziehen, macht große Verluste wahrscheinlicher.

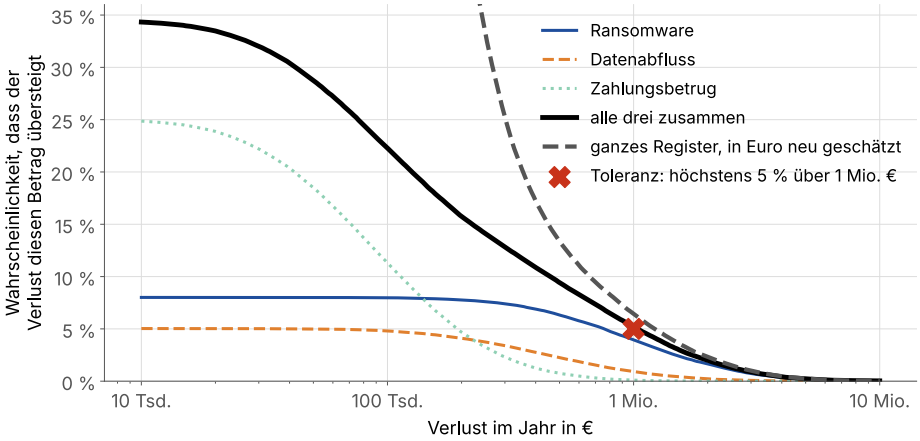


Abbildung 16: Verlustüberschreitungskurve: Wie wahrscheinlich übersteigt der Verlust eines Jahres einen Betrag? Durchgezogen schwarz die drei Szenarien, grau gestrichelt das ganze Register. Das Kreuz ist die Toleranz der Holding.

Statt „Grün ist akzeptabel“ steht jetzt eine Toleranz im Protokoll, die sich prüfen lässt. Dr. Hesse hat damit einen Maßstab für ihre 120 000 €: Jede Maßnahme lässt sich daran messen, wie weit sie die Kurve unter das Kreuz drückt.

Was Nora mitnimmt: Eine prüfbare Toleranz gibt dem Budget einen Maßstab. Die 120 000 € sollen die Kurve unter das Kreuz drücken.

Genauer hingeschaut: Hält die Toleranz? Das hängt an einer Schätzung. Der Übersicht halber steht für jedes Szenario eine einzige Wahrscheinlichkeit. Wie stark das Ergebnis an der Ransomware-Wahrscheinlichkeit hängt, prüft Nora getrennt: Ihre Bandbreite reicht von 4 bis 12 Prozent im Jahr. Mit dem ganzen Register liegt ein Millionenjahr dann bei 4,1, 6,5 oder 8,9 Prozent, nur mit den drei Szenarien bei 3,2 bis 7,3 Prozent. Bei 4 Prozent hält die Toleranz knapp, bei 8 und 12 Prozent reißt sie. Die Grenze liegt bei 5,6 Prozent Ransomware-Wahrscheinlichkeit. Genau diese Schätzung lohnt es vor der nächsten Budgetrunde zu verbessern.

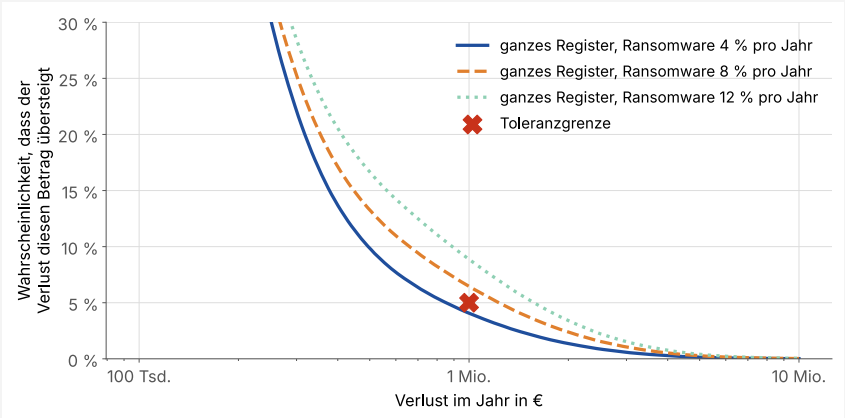


Abbildung 17: Hält die Toleranz? Verlustüberschreitungskurven des ganzen Registers für eine Ransomware-Wahrscheinlichkeit von 4, 8 und 12 Prozent im Jahr.

Verteilung statt Ordinalzahl

Was sich bei Kestner geändert hat, liegt unter der Haube. Ein Risiko ist keine Stufe mehr, sondern eine Verteilung möglicher Jahresverluste. Der erwartete Verlust, das Millionenjahr und die Toleranz der Holding sind drei Blicke auf dieselbe Verteilung. Eine Ordinalzahl wirft alle drei weg.

Der Ansatz hat einen Namen: Open FAIR, ein Standard der Open Group, mit der Taxonomie O-RT und der Analysemethode O-RA. Er zerlegt Risiko in Häufigkeit und Schadenshöhe, schätzt beide als Band-

breiten und simuliert daraus die Verlustverteilung. Kestner nutzt nur die oberste Ebene, Häufigkeit mal Schaden. Für den Anfang reicht das. Die Matrix verschwindet dadurch nicht. Sie wird zur Darstellung für das Management und die Holding, abgeleitet aus den Verteilungen. Wie genau, zeigt Szene 8.

> **Was Nora mitnimmt:** Eine Verteilung beschreibt ein Risiko besser als eine Ordinalzahl. Gerechnet wird mit Verteilungen, die Matrix bildet das Ergebnis ab.

Lohnt es, genauer zu wissen?

Herr Kübler schlägt einen Schutz vor, der die Ransomware-Wahrscheinlichkeit auf 3 Prozent senkt, und will dafür Geld aus den 120 000 €. Bevor er es beantragt, will er für 15 000 € eine externe Bedrohungsanalyse einholen. Sie soll klären, ob die Wahrscheinlichkeit heute eher bei 4 oder bei 12 Prozent liegt.

Nora rechnet nach. Eine Infektion kostet im Mittel 1,4 Millionen. Kostet der Schutz 10 000 € im Jahr, lohnt er sich ab 3,7 Prozent, also in der ganzen Bandbreite. Die Analyse würde an der Entscheidung nichts ändern. Kostet er 50 000 € im Jahr, liegt die Schwelle bei 6,5 Prozent, mitten in der Bandbreite. Gemeint ist die Ransomware-Wahrscheinlichkeit, ab der sich der Schutz rechnet, nicht das Millionenjahr von eben. In diesem Fall kann die Analyse die Entscheidung ändern, aber sie ist höchstens so viel wert, wie eine Fehlentscheidung im Mittel kostet: rund 5 600 €.

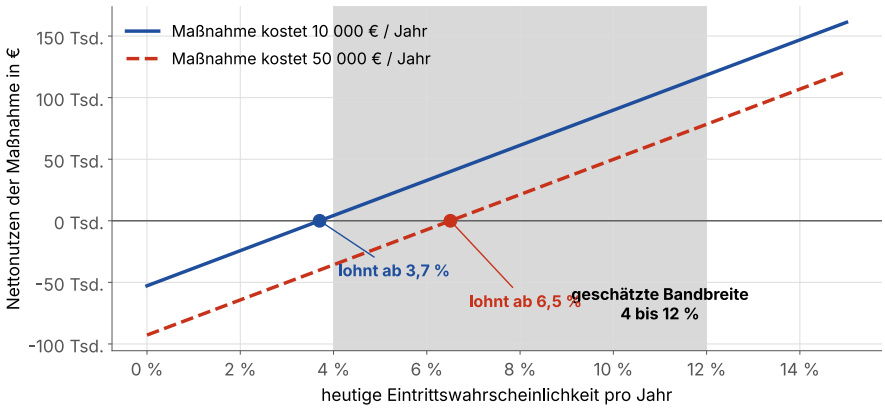


Abbildung 18: Nettonutzen des Schutzes über der heutigen Wahrscheinlichkeit. Grau: Noras Bandbreite von 4 bis 12 Prozent. Über der Nulllinie lohnt sich der Schutz.

„Die Analyse kostet mehr, als sie uns erspart“, sagt Nora. „Die 15 000 € behalten wir.“ Das ist auch die Antwort auf den Einwand, all das sei viel zu aufwendig: Die meisten Risiken brauchen keine genauere Schätzung.

> **Was Nora mitnimmt:** Genauer schätzen lohnt nur, wenn es die Entscheidung ändern kann.

Szene 5: Wie gut schätzt Kestner? (Oktober)

In der Budgetrunde hat sich gezeigt, wie viel an einzelnen Schätzungen hängt. Ob die Toleranz hält, steht und fällt mit einer Zahl wie „4 bis 12 Prozent“. Im Oktober lädt Nora zu zwei Stunden Schätztraining ein.

Fünf von zehn statt neun von zehn

Herr Kübler kommt mit einem Einwand, den Nora schon oft gehört hat: „Für so etwas haben wir keine Daten. Eine Wahrscheinlichkeit kann man doch nur aus einer Statistik ablesen.“ Nora schreibt einen Satz an das Whiteboard: „Wahrscheinlichkeit ist ein Maß für die Unsicherheit einer schätzenden Person.“ So

hat es der Mathematiker Bruno de Finetti 1974 in seiner *Theory of Probability* ausgearbeitet. Im Vorwort spitzt er es in Großbuchstaben zu: „PROBABILITY DOES NOT EXIST“.

Eine Wahrscheinlichkeit ist damit keine Eigenschaft der Welt wie das Gewicht eines Würfels, die man nur genau genug messen müsste. Sie ist der Grad der Gewissheit, mit dem jemand ein Ereignis erwartet, gestützt auf alles, was diese Person weiß. Frank Ramsey hat diese Sicht 1926 begründet, de Finetti hat sie ausgearbeitet, Leonard Savage hat 1954 eine Entscheidungstheorie darauf gebaut. Die Bayes-Statistik rechnet bis heute damit.

Für Kestner ist das eine gute Nachricht. Niemand muss auf objektive Zahlen warten, denn es gibt sie nicht, auch nicht mit noch so vielen Daten. Wo Häufigkeiten vorliegen, etwa Ausfallraten, fließen sie in die Schätzung ein. Eine Ransomware-Infektion bei Kestner im nächsten Jahr ist aber ein Einzelfall, für den es keine Häufigkeit gibt, nur begründete Gewissheit. Jedes „selten“ im alten Register war schon eine subjektive Wahrscheinlichkeit, nur eine unausgesprochene, und deshalb hat jeder im Raum etwas anderes darunter verstanden. Eine Zahl macht sie prüfbar. Herr Kübler und Herr Demir haben im Juli beide nicht falsch geschätzt. Sie waren verschieden gewiss, weil sie Verschiedenes wussten.

Subjektiv heißt aber nicht beliebig. Ob jemand gut schätzt, lässt sich messen. Im Training gibt jede Person zu zwanzig Fragen mit bekannter Antwort eine 90-%-Bandbreite an. Ihre Ränder sind P5 und P95: Nur in 5 Prozent der Fälle liegt der wahre Wert darunter, nur in 5 Prozent darüber. Für den unteren Rand fragt Nora: „Ich wäre überrascht, wenn ein Fall weniger als … kostet. Das passiert nur in einem von zwanzig Fällen.“ Für den oberen Rand fragt sie ebenso. Das Training macht genau diese Ränder messbar: Wer kalibriert schätzt, trifft mit neun von zehn Bandbreiten. Bei Herrn Kübler enthalten nur zehn der zwanzig Bandbreiten die Antwort, fünf von zehn statt neun von zehn. Es ist derselbe Herr Kübler, der im Juli die enge Bandbreite genannt hat. Er war sich zu sicher, wie fast alle beim ersten Mal. Das lässt sich trainieren, zwei bis drei Stunden reichen für den Einstieg.

Danach geht es ums Verengen. Neues Wissen verschiebt eine Schätzung, und der Satz von Bayes beschreibt, um wie viel. In der Fachsprache heißt das Bayes-Update, von a priori zu a posteriori. Herr Demir sagt dazu: „Ich hab mal nachgefragt.“ Über die Wahrscheinlichkeit lernt Kestner am meisten von außen: aus dem Lagebild und aus Vorfällen bei anderen Zulieferern. Über den Schaden lernt die Firma von innen, etwa aus der Stillstandsrechnung von Herrn Demir für die Cyberversicherung. Natürliche Streuung bleibt, abbauen lässt sich nur fehlendes Wissen. Das Unwissen von Herrn Demir über die Updates aus dem Juli kann Herr Kübler ihm abnehmen. Den Saisoneffekt kann niemand wegschätzen. Eine gute Frage für den Workshop lautet: Wie weit lägen zwei Vorfälle noch auseinander, wenn wir alles über unser Werk wüssten?

> **Was Nora mitnimmt:** Subjektiv heißt nicht beliebig. Objektiv wird eine Wahrscheinlichkeit nie, prüfbar schon.

Schlechte Schätzer, und trotzdem simulieren?

Nach dem Training fragt Herr Demir, was viele im Raum denken: „Wenn wir nur fünf von zehn treffen, was taugt dann die Simulation?“ Es ist der wichtigste Einwand gegen alles Bisherige, und Nora antwortet in drei Schritten.

1. **Schätzen lässt sich üben.** In der zweiten Runde, nach Rückmeldung zur ersten, enthalten bei Herrn Kübler schon 16 von 20 Bandbreiten die Antwort.
2. **Eine Bandbreite zeigt, wie unsicher eine Eingabe ist.** Eine weite Bandbreite ist eine ehrliche Eingabe, und das Ergebnis wird entsprechend breit, wie in Szene 3. Die Simulation rechnet mit dieser Unsicherheit, statt sie zu übergehen, und zu enge Ränder fallen im Abgleich mit den tatsächlichen Vorfällen auf.
3. **Die Matrix ist keine Alternative mit besseren Eingaben.** Sie bekommt dieselben Schätzungen von denselben Köpfen und presst sie in Stufen. Dort fällt nie auf, wer sich zu sicher war.

Was Nora mitnimmt: Schlechte Eingaben sprechen nicht gegen die Rechnung, sondern gegen das Verstecken.

Szene 6: Wer entscheidet was? (Oktober)

Eine gute Schätzung hilft wenig, wenn unklar ist, wer entscheidet. Das ist die dritte Hürde, der Ablauf.

Freitag, 15 Uhr. Ein Administrator findet an der Firewall eine offene Verwaltungsschnittstelle. Ein Maschinenlieferant wartet darüber seine Anlagen fern. Der Administrator lässt sie deshalb offen und schreibt ins Ticket: „Mittel, akzeptiert." Geht es schief, steht die Produktion. Der Schaden geht dann zulasten des Budgets von Herrn Demir, schlimmstenfalls um Millionen.

Für Nora ist das kein persönliches Versagen: Die Vorlage lässt jeden selbst einstufen, die Lücke liegt im Ablauf. Der Administrator hat den Fund selbst eingestuft und damit für Kestner entschieden, wozu er nicht befugt ist. Die Schnittstelle kennt er besser als alle anderen. Ob Kestner das Risiko trägt, muss aber entscheiden, wer für die Folgen einsteht. ISO/IEC 27001 verlangt dasselbe: Nach 6.1.3 genehmigen die Risikoeigentümer den Behandlungsplan und akzeptieren das Restrisiko.

Was Nora mitnimmt: Ein Risiko akzeptieren darf nur, wer für die Folgen einstehen muss.

Nora trennt deshalb zwei Rollen. Fachleute aus IT, Produktion und Sicherheit schätzen ab, wie wahrscheinlich ein Ereignis ist und wie viel Schaden es an den Zielen anrichtet, als Bandbreite in Prozent und Euro. Bewerten muss, wer für die Folgen einsteht und über Budget und Haftung entscheiden darf. Diese Person wählt, ob Kestner das Risiko akzeptiert, mindert, überträgt oder meidet, und wägt dabei Kosten, Termine und den Saisonstart ab. Abwägen kann sie nur, weil die Schätzungen in Euro vorliegen. Eine Farbe lässt sich nicht gegen Kosten aufrechnen. Bei 200 Beschäftigten hat eine Person oft mehrere Rollen. Die Trennung verlangt dann kein zusätzliches Personal, nur Klarheit darüber, in welcher Rolle jemand spricht.

Der obere Rand bestimmt die Ebene

Kestner legt drei Ebenen fest, die Schwellen richten sich nach dem Jahresergebnis. Wie viel Befugnis eine Entscheidung braucht, hängt an der Größe des Risikos, nicht an einem festen Instanzenweg.

Oberer Rand des Schadens	Wer entscheidet	Nachweis
bis 10 000 €	Team- oder IT-Leitung	Ticket
bis 100 000 €	Sicherheitsrunde: Nora, Herr Kübler, Herr Demir, Frau Brandt	Register
darüber oder bei Organhaftung	Dr. Hesse	Register, Protokoll

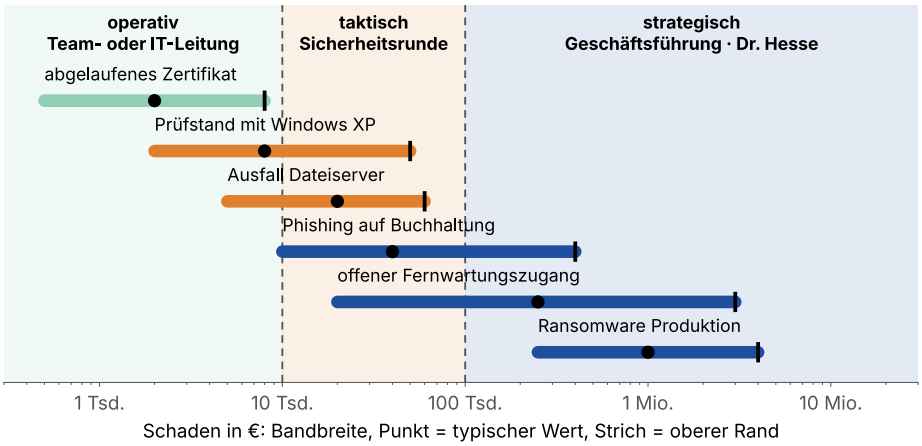


Abbildung 19: Drei Ebenen. Maßgeblich ist der obere Rand der Bandbreite, nicht der typische Wert. Der offene Fernwartungszugang vom Freitag reicht bis 3 Mio. € und gehört wie Ransomware auf die strategische Ebene.

Maßgeblich ist der obere Rand der Bandbreite, denn erst der ungünstige Fall zeigt, wer für die Folgen einstehen müsste. Der Prüfstand in der Endkontrolle läuft noch mit Windows XP. Patchen lässt er sich nicht, ein Ersatz kostet, und die Fertigung braucht ihn jeden Tag. Typisch kostet ein Vorfall 8 000 €, schlimmstenfalls 50 000 €. Ob Kestner ihn abschottet, ersetzt oder das Risiko trägt, wägt deshalb die Sicherheitsrunde ab. Die Entscheidung betrifft mehrere Abteilungen. Ransomware in der Produktion reicht bis in die Millionen, deshalb entscheidet Dr. Hesse über die 120 000 €. Der offene Fernwartungszugang vom Freitag reicht bis 3 Millionen. Auch er gehört nicht ins Ticket, sondern zu Dr. Hesse. Akzeptieren ist auf jeder Ebene legitim, wenn die Zuständigen entscheiden und es dokumentieren.

Damit hängt viel am oberen Rand, und gerade den ziehen Menschen oft zu eng, wie sich im Schätztraining gezeigt hat. Kestner sichert ihn deshalb mit drei Regeln ab. Den oberen Rand schätzen immer zwei, und die zweite Person kommt aus einem anderen Team und bringt einen anderen Blick mit. Risiken nahe einer Schwelle gehen eine Ebene höher: Im Zweifel entscheidet die Ebene mit mehr Befugnis, damit nichts Großes unten liegen bleibt. Und der Abgleich mit den tatsächlichen Vorfällen zeigt wie im Schätztraining, wo Ränder regelmäßig zu eng ausfallen.

> **Was Nora mitnimmt:** Fachleute schätzen, die zuständige Ebene bewertet. Der obere Rand bestimmt die Ebene.

Szene 7: Ordnung per Software? (Oktober)

Die vierte Hürde ist das Werkzeug. Ebenfalls im Oktober meldet sich der Dienstleister der Holding. Er führt dort ein GRC-Werkzeug ein und bietet an, Kestners Register zu übernehmen: „Wir übernehmen Ihr Register eins zu eins, Ampel inklusive.“ Hinter jedem solchen Projekt steht die Hoffnung auf eindeutige, auditfeste Werte. Ankommen würde das alte Register, migriert, mit Arbeitsablauf und Übersichtsseite, nur revisionssicher. Das Risikomanagement bliebe, wie es war.

Nora fragt zurück: Welcher Schritt des Ablaufs, den Kestner gerade festgelegt hat, braucht überhaupt neue Software? Sie geht ihn mit Herrn Kübler durch und findet keinen.

Ablauf	Werkzeug bei Kestner
Fund, Maßnahme, Entscheidung bis 10 000 €	Ticket im vorhandenen Ticketsystem
Glossar, Methode, Schätzhilfen	Wiki
Register, Vier-Augen-Freigabe, Änderungsnachweis	Markdown-Dateien in Git, Merge-Request, Historie
Berichte für Runde, Holding und Audit	erzeugte Seite, Matrix für die Holding aus den Verteilungen

Das Ticketsystem nutzt die IT ohnehin, und im Wiki schlagen schon heute alle nach. Das Register führt Nora als Markdown-Dateien in Git, ein Szenario je Datei, mit Bandbreite, Begründung und Entscheidung. Jede Änderung ist ein Merge-Request, den jemand aus der Sicherheitsrunde freigibt. Das ist die Vier-Augen-Freigabe, und die Historie ist der Änderungsnachweis: wer wann was warum geschätzt hat. Bei jedem Merge baut ein Static-Site-Generator daraus eine lesbare Seite, die Pipeline rechnet dabei die Simulation neu, und die Verlustkurve ist immer aktuell.

Die Holding bekommt, was sie braucht: einmal im Quartal ihre Matrix, abgeleitet aus den Verteilungen. Jedes Szenario landet in dem Feld, das seine Bandbreite und sein Beitrag zur Verlustkurve rechtfertigen, nicht in dem, das ein Produkt zweier Stufen ergibt. Ein GRC-Werkzeug kann sinnvoll werden, wenn viele Gesellschaften, mehrere Regelwerke und Berichte an die Aufsicht zusammenkommen. Aber erst nach dem Ablauf, nicht statt seiner. Kestner bildet den Ablauf mit Werkzeugen ab, die schon im Haus sind und die alle bedienen können. Auch die Folien zu diesem Vortrag liegen als Markdown in Git.

Git sehen dabei die wenigsten. Fachleute wie Herr Demir arbeiten im Ticket und im Wiki, Merge-Requests stellen Nora und die Sicherheitsrunde. Dr. Hesse und Frau Brandt lesen die erzeugte Seite und die Quartalsmatrix. Wo niemand Git kennt, tut es auch ein Wiki mit Versionsgeschichte und Freigabe. Die Simulation ist ein Skript von einer Seite, das Herr Kübler einmal geprüft hat, und jede Änderung daran ist selbst ein Merge-Request. Ein Skript dieser Art steht im Anhang. Als Gegenprobe rechnet die Pipeline den erwarteten Verlust zusätzlich direkt aus, Wahrscheinlichkeit mal mittlerer Schaden. Weichen beide voneinander ab, bricht der Bau ab.

> **Was Nora mitnimmt:** Ein Werkzeug bildet einen Ablauf ab. Es ersetzt ihn nicht. Oft reicht, was schon im Haus ist.

Szene 8: Das Audit (November)

„Wo ist denn Ihre Risikomatrix?“

Im November kommt der Auditor zum Stufe-2-Audit. „Wo ist denn Ihre Risikomatrix?“, fragt er. Vor dieser Frage hat Nora sich das ganze Jahr gefürchtet. ISO/IEC 27001 lässt die Methode offen. Nora geht die Anforderungen aus 6.1.2 durch. Ihr Verfahren erfüllt jede davon, einige besser als die alte Vorlage.

Der Auditor fragt nach 6.1.2	Nora zeigt
Kriterien für die Risikoakzeptanz	Toleranz der Holding, Schwellen je Ebene
konsistente, gültige, vergleichbare Ergebnisse	Glossar, Schätztraining, Begründung je Bandbreite
Folgen, realistische Wahrscheinlichkeit, Risikohöhe	in Prozent und Euro, addierbar
Risikoeigentümer, Behandlungsplan, Erklärung zur Anwendbarkeit	unverändert

„Addierbar“ ist kein Detail: Mit Stufen ist monatelang niemandem aufgefallen, dass das Register doppelt so viel Schaden ergab, wie Kestner verdient. Erst die Gegenprobe von Frau Brandt in Euro hat es gezeigt.

„Woher kommen die 8 Prozent im Jahr für Ransomware in der Produktion?“, fragt der Auditor. Nora öffnet die Datei des Szenarios und zeigt Begründung und Historie. Weil ein Risiko eine Einschätzung ist, kann ein Auditor nur prüfen, ob sie begründet und nachvollziehbar ist. Die alte Vorlage hinterließ eine Stufe. Kestners Register hinterlässt in der Git-Historie, wer was geschätzt hat und warum.

> **Was Nora mitnimmt:** Der Auditor prüft die Begründung einer Einschätzung, nicht ihre Farbe.

Die Matrix musste bei Kestner niemand abschaffen. Die Holding will sie im Quartalsbericht, und als Seite im Bericht an den Beirat steht sie weiter. Als Sortier- und Kommunikationsmittel bleibt sie legitim.

Zulässig ist an ihr ein einfacher Schluss: Liegt ein Risiko in beiden Dimensionen mindestens so hoch wie ein anderes, ist es mindestens so groß. Unzulässig ist die Rechnung, die aus zwei Stufen eine Zahl macht, und jede Entscheidung, die auf dieser Zahl beruht. Gerechnet wird unter der Haube mit Verteilungen. Die Matrix bildet das Ergebnis für das Management ab: Feld und Farbe folgen aus Bandbreite und Toleranz, nicht umgekehrt.

Wie aus der Verteilung ein Matrixfeld wird

Wie genau, will der Auditor wissen. Die Regel steht im Wiki und passt auf eine Seite, eine Fassung davon findet sich im Anhang. Die Zeile ergibt sich wie bisher aus der geschätzten Wahrscheinlichkeit im Jahr, die Spalte aus dem typischen Schaden, dem Median. Die Bandbreite steht als Balken über den Nachbarfeldern. Die Farbe kommt nicht mehr aus dem Produkt zweier Stufen, sondern aus der Simulation: Wie oft macht dieses Szenario allein ein Jahr über 1 Mio. € teuer? Die Toleranz der Holding erlaubt 5 Prozent für alle zusammen. Rot ist ein Szenario, das allein die Hälfte davon verbraucht, also 2,5 Prozent, gelb ab 0,5 Prozent. Die Schwellen sind Kestners Entscheidung, nicht Mathematik.

Regel bei Kestner	Ransomware	Datenabfluss	Zahlungsbetrag
Zeile: Wahrscheinlichkeit im Jahr	8 %	5 %	25 %
Spalte: typischer Schaden, Bandbreite als Balken	1 Mio. €	450 000 €	90 000 €
Farbe: Jahre über 1 Mio. € durch das Szenario allein	4,0 %, rot	0,9 %, gelb	0,1 %, grün
zum Vergleich: Produkt der Stufen	8, grün	4, grün	4, grün

Nach der alten Rechnung waren alle drei grün, und Datenabfluss und Betrug standen gleichauf. Jetzt trennt die Farbe sie, wie in Szene 4. Die Prozentwerte in der Farbzeile sind absolute Wahrscheinlichkeiten: der Anteil der Jahre, in denen dieses eine Szenario allein mehr als eine Million kostet.

Auf dem Bildschirm sieht die Holding-Matrix aus wie immer, nur die Felder sind grau. Ein Feld enthält Risiken mit sehr verschiedener Breite, und eine Feldfarbe würde wieder nahelegen, die Lage bestimme die Farbe. Ransomware steht als roter Punkt im Feld „1–5 Mio.“, ihr Balken reicht von 250 000 € bis 4 Mio. €. Der Balken des Datenabflusses reicht über drei Felder bis in die Millionen. Damit ist die Frage aus Szene 3 beantwortet, ob ein Risiko in ein Feld gehört oder in drei. Wer fragt, warum Ransomware rot ist, bekommt eine Zahl: 4 von 5 Prozent der Toleranz.

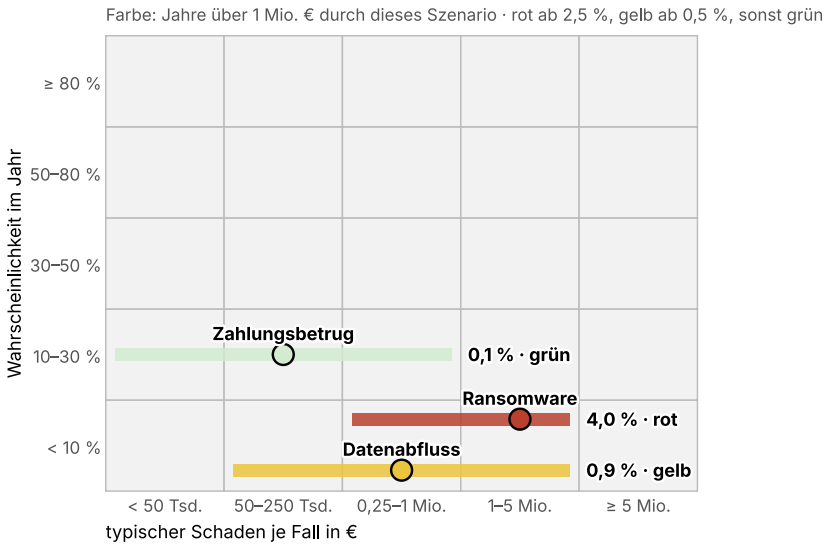


Abbildung 20: Kestners Holding-Matrix: graues Raster, Balken für die 90-%-Bandbreite des Schadens, Farbe je Risiko aus der Toleranz.

Werden nach dieser Regel die drei roten Risiken aus dem April und die Lieferantenstörung grün? Ja. Allein erreichen sie kein Millionenjahr. Um sie kümmern sich die Ebenen aus Szene 6, bezahlt aus dem

laufenden Budget. Die Farbe zeigt jetzt den Beitrag zum Millionenjahr, nicht mehr, wie lästig ein Risiko ist.

> **Was Nora mitnimmt:** Die Matrix darf bleiben. Als Abbild der Verteilung, nicht als Rechnung. Das Raster bleibt, die Farbe gehört dem Risiko und lässt sich nachrechnen.

Auflösung: Die 120 000 €

Tabelle 11: Ein Jahr bei Kestner: Umdenken statt Abhaken.

	Frühjahr	November
Begriffe	drei Bedeutungen von Risiko, 40 Minuten Streit um die 12	Glossar, 6.1.2 als Frage gelesen
Rechnung	Stufen multipliziert, eine Farbe je Risiko	Verteilung unter der Haube, Matrix als Abbild
Ablauf	ein Millionenrisiko per Ticket akzeptiert	Fachleute schätzen, die zuständige Ebene bewertet
Werkzeug	Excel-Vorlage per Mail, Stand unklar	erst den Ablauf geklärt, dann Ticket, Wiki und Git

Die Frage von Dr. Hesse aus dem April hat jetzt eine Antwort. Die 120 000 € gehen zuerst in den Ransomware-Schutz der Produktion, weil er die Verlustkurve am stärksten unter die Toleranz drückt. Rund 80 000 € kosten einmalig drei Maßnahmen: die Trennung der Produktions-IT vom Büronetz, Sprungserver für Fernzugänge und eine Offline-Datensicherung. Die Trennung ist zugleich die Mindestmaßnahme des Versicherers, die Sprungserver führt Kestner Lieferant für Lieferant ein (siehe Epilog). Die übrigen rund 40 000 € gehen in den Schutz der Konstruktionsdaten, das gelbe Szenario: Rechte im Produktdatensystem und eine Protokollierung von Exporten. Die Lieferantenstörung läuft als eigener Antrag über den Einkauf, Rot und Orange aus dem April über das laufende Budget.

Sinkt die Ransomware-Wahrscheinlichkeit von 8 auf 3 Prozent, fällt die Wahrscheinlichkeit eines Millionenjahrs für das ganze Register von 6,5 auf 3,5 Prozent. Die Toleranz hält. Auch die 3 Prozent sind eine Schätzung, denn die Wirkung einer Maßnahme ist so unsicher wie das Risiko selbst. Herr Kübler gibt sie deshalb als Bandbreite an, 2 bis 5 Prozent. Selbst am oberen Rand liegt ein Millionenjahr bei 4,7 Prozent, knapp unter der Grenze. Die Toleranz reißt, sobald der Schutz die Wahrscheinlichkeit nur auf 5,6 Prozent drückt. Der Abstand ist knapp, und genau diese Schätzung lohnt es zu verbessern.

Schlussbemerkung: Kestner hatte Glück

Diese Geschichte ist glatt verlaufen, und das war Absicht. Kestner ist das optimistische Szenario. Kestner hatte Glück: eine ISB, die dranbleibt, eine Geschäftsführerin, die nachfragt, eine Holding, die eine Zahl festlegt, und einen Auditor, der Begründungen liest. Jede dieser Personen hätte das Vorhaben stoppen können.

Wo Kestner hätte scheitern können

Die meisten Organisationen, die ich begleitet habe, kommen über Bandbreiten in der Diskussion nicht hinaus. Die Gründe sind selten technisch:

- **Skepsis gegenüber Mathematik:** „Das versteht der Beirat nicht."
- **Gewohnheit:** Die Berichte des Vorjahres sollen vergleichbar bleiben.
- **Druck von außen:** Holding, Versicherer und Großkunde fragen im Matrixformat.
- **Scheu vor Zahlen:** „Mittel" legt niemanden fest, „8 Prozent" schon.

- **Eine Person:** Geht Nora, kommt die Vorlage zurück.
- **Angst vor dem Audit,** obwohl die Norm die Methode offenlässt.

Organisationen scheitern selten an der Mathematik. Deshalb lohnt es, klein anzufangen.

Wenn Sie sich wiedererkannt haben: drei erste Schritte

Vielleicht kam Ihnen beim Lesen einiges bekannt vor: das Register, das formal vollständig ist und trotzdem keine Budgetfrage beantwortet, der Streit um ein Feld, die Ampel, die alle Szenarien grün malt. Dann ist dieser Abschnitt ein Vorschlag, wie Ihre Organisation die Hürden aus der Geschichte angehen kann, ohne alles auf einmal umzubauen. Dafür genügen drei Schritte, und keiner davon braucht neue Software:

1. **Ein halber Workshoptag für die Begriffe.** Am Ende steht ein Glossar, das Bedrohung, Schwachstelle, Szenario und Risiko trennt. Eine Kurzfassung steht im Anhang.
2. **Für die wichtigsten Risiken eine Bandbreite** auf der vorhandenen Farbskala: günstig, typisch, ungünstig.
3. **Die drei Szenarien, über die bei Ihnen am meisten geredet wird,** in Prozent und Euro schätzen, simulieren und neben die Matrix legen. Wo beide auseinanderliegen, beginnt das Gespräch, um das es im Risikomanagement gehen soll.

Für den dritten Schritt stehen im Anhang eine Schätzvorlage und ein Simulationsskript von einer Seite. Nora hat ihre Simulation an einem Nachmittag mit einem Sprachmodell gebaut. Prüfen muss die Simulation jemand, der den Code und seine Annahmen versteht.

Epilog: Grenzen der Analyse

Nicht jede Frage bei Kestner lässt sich durch Analyse beantworten. Das Cynefin-Modell von Dave Snowden unterscheidet, welche Art Frage man vor sich hat.

Bereich	Beispiel bei Kestner	Vorgehen
klar	Passwortrichtlinie	Lösung bekannt, bewährte Praxis anwenden
kompliziert	Häufigkeit von Ransomware bei Zulieferern dieser Größe	mit Fachwissen analysieren, schätzen, rechnen
komplex	Fernwartung durch 30 Lieferanten	erst bei einem über Sprungserver, beobachten, nachsteuern
chaotisch	Die Verschlüsselung läuft gerade.	erst handeln, dann analysieren

Noras Simulation hilft im Komplizierten. Ist Ransomware nicht komplex? Der einzelne Angriff schon, mit einem Gegner, der dazulernt. Die Häufigkeit über viele Firmen lässt sich aber schätzen, und Nora schätzt die Häufigkeit, nicht den Verlauf. Komplex ist die Fernwartung durch 30 Lieferanten mit unterschiedlichen Werkzeugen und Verträgen: Ursache und Wirkung zeigen sich erst hinterher, und die Beteiligten reagieren auf jede Maßnahme. Snowden nennt das Vorgehen dort „probe, sense, respond“: ausprobieren, beobachten, nachsteuern. Kestner beginnt mit einem Lieferanten und einer Maschine. Der Zugang läuft über einen Sprungserver mit zweitem Faktor, und Herr Demir gibt jede Sitzung frei. Vier Wochen lang beobachtet Nora, ob der Techniker hineinkommt, ob der Service langsamer wird und ob jemand die Regel umgeht. Dann folgt der nächste Lieferant, oder die Regel ändert sich. Die größte Gefahr ist ein Techniker, der ein eigenes Mobilfunkmodem an die Maschine schraubt. Scheitert der Versuch, steht schlimmstenfalls eine Maschine einen Tag still, nicht die Fernwartung von 30 Lieferanten auf einmal. Es ist derselbe Zugang, den der Lieferant in Szene 6 brauchte. Und wenn die Verschlüsselung gerade läuft, ist die Lage chaotisch: erst handeln, dann analysieren.

In der Mitte des Modells liegt ein fünfter Bereich: Man weiß nicht, in welchem der vier man steckt. Wer das nicht erkennt, greift zum vertrauten Werkzeug. Oft ist das die Matrix.

Ob kompliziert oder komplex, eines bleibt gleich:

Der Wert einer Risikoanalyse liegt nicht in der genaueren Zahl, sondern in der Einsicht, wie viel wir nicht wissen.

Anhang

A 1 Glossar

Kestners zwei Seiten, auf das Nötigste gekürzt. Wer ein eigenes Glossar schreibt, sollte Beispiele aus der eigenen Organisation nehmen.

Risiko Auswirkung von Unsicherheit auf Ziele (ISO 31000, übernommen in ISO/IEC 27000). Bei Kestner beschrieben als Verteilung möglicher Jahresverluste eines Szenarios. Eine Risikoeinschätzung ist eine begründete Aussage, die sich mit neuem Wissen ändert. Eine Zahl wie „12“ misst ein Risiko, ist aber keines. Ausführlicher: SRA-Glossar (A 5).

Bedrohung Mögliche Ursache eines unerwünschten Ereignisses, etwa Ransomware, ein Brand, ein gefälschter Zahlungsauftrag.

Schwachstelle Schwäche eines Werts oder einer Maßnahme, die eine Bedrohung ausnutzen kann, etwa die alten Steuerungsrechner, der Prüfstand mit Windows XP, eine offene Verwaltungsschnittstelle.

Szenario Konkreter Ablauf, in dem eine Bedrohung eine Schwachstelle trifft und ein Ziel verfehlt wird. Beispiel: „Ransomware verschlüsselt die Produktions-IT, die Fertigung steht neuneinhalb Tage.“ Geschätzt wird je Szenario, nicht je Bedrohung.

Bandbreite Unterer und oberer Wert, zwischen denen eine Größe mit angegebener Sicherheit liegt, bei Kestner mit 90 Prozent. Je 5 Prozent der Fälle liegen darunter und darüber. Der obere Rand bestimmt die Ebene, die entscheidet.

P5, P95, 90-%-Bandbreite P5 ist der Wert, den nur 5 Prozent der Fälle unterschreiten, P95 der Wert, den nur 5 Prozent überschreiten. Zusammen bilden sie die 90-%-Bandbreite. Gefragt wird wie in Szene 5: „Ich wäre überrascht, wenn ein Fall weniger als … kostet.“

Logarithmische Normalverteilung Kurz Lognormalverteilung. Verteilung für Größen, die nie negativ und rechtsschief sind: viele kleine, wenige sehr große Werte. Bei Kestner das Modell für den Schaden je Fall, festgelegt durch P5 und P95. Der Median ist √(P5 × P95), der Mittelwert liegt darüber. Eine Annahme, keine Tatsache: Bei sehr weiten Bandbreiten wird sie bei einem plausiblen Höchstwert gekappt.

Toleranz Wie viel Verlust wie oft verkraftbar ist, festgelegt von denen, die den Verlust tragen. Bei Kestner: über 1 Mio. € höchstens in einem von zwanzig Jahren, also mit höchstens 5 Prozent.

Verlustüberschreitungskurve Zeigt für jeden Betrag, mit welcher Wahrscheinlichkeit der Verlust eines Jahres ihn übersteigt. An ihr lässt sich die Toleranz prüfen und die Wirkung einer Maßnahme ablesen.

Erwarteter Jahresverlust Mittelwert der Jahresverluste über viele simulierte Jahre, seltene teure Fälle eingerechnet. Er liegt bei rechtsschiefen Schäden deutlich über „typische Wahrscheinlichkeit mal typischer Schaden“.

Kalibrierung Übereinstimmung zwischen angegebener und tatsächlicher Trefferquote. Wer kalibriert schätzt, trifft mit 90-%-Bandbreiten in neun von zehn Fällen.

A 2 Schätzvorlage

Ein Blatt je Szenario. Die Felder entsprechen dem, was das Simulationsskript braucht, plus dem, was ein Auditor sehen will: Begründung, Quellen und wer wann geschätzt hat.

Tabelle 13: Schätzvorlage, leer.

Feld	Eintrag
Szenario	Bedrohung, Schwachstelle, Folge für ein Ziel, in einem Satz
Wahrscheinlichkeit im Jahr (Bandbreite)	von … bis … %, typisch … %
Schaden je Fall, 90 %	von … € (P5) bis … € (P95), Fragetechnik wie in Szene 5
Begründung	Wovon hängen Häufigkeit und Schaden ab? Was spricht für den unteren, was für den oberen Rand?
Quellen	eigene Vorfälle, Buchhaltung, Lagebild, Branchenzahlen, Rechnungen der Fachabteilung
Wer hat geschätzt	… (Fachabteilung) und … (nicht aus dem Team, das die Arbeit hätte)
Datum	…

Ein ausgefülltes Beispiel, so wie es bei Kestner in der Datei des Szenarios stehen könnte:

Tabelle 14: Schätzvorlage, ausgefüllt für Ransomware in der Produktion.

Feld	Eintrag
Szenario	Ransomware Produktion: Schadsoftware verschlüsselt die Produktions-IT über das Büronetz, die Fertigung steht still. Betriebsunterbrechung derzeit nicht versichert.
Wahrscheinlichkeit im Jahr (Bandbreite)	4 bis 12 %, typisch 8 %
Schaden je Fall, 90 %	250 000 € bis 4 Mio. € (typisch 1 Mio. €)
Begründung	Produktions-IT noch nicht vom Büronetz getrennt. Wiederanlauf laut Test nach 9,5 Tagen, ein Stillstandstag kostet rund 100 000 € Deckungsbeitrag, dazu Nacharbeit und Vertragsstrafen. Unterer Rand: Angriff früh erkannt, nur Teile der Fertigung betroffen. Oberer Rand: Angriff in den sechs Wochen vor dem Saisonstart, längerer Wiederanlauf.
Quellen	Wiederanlauftest im Frühjahr, Stillstandsrechnung von Herrn Demir für den Fragebogen der Cyberversicherung, Lagebild und Vorfälle bei anderen Zulieferern, Buchhaltung
Wer hat geschätzt	Herr Kübler (IT) und Herr Demir (Produktion), mit Frau Brandt und Nora
Datum	September 2026, nächste Prüfung vor der Budgetrunde 2027

Hinweise zum Ausfüllen:

- **In Euro und Prozent schätzen, nicht in Stufen.** Wer nur „mittel“ sagen mag, darf das zuerst tun. Dann fragen: Welcher Betrag wäre überraschend niedrig, welcher überraschend hoch?
- **Die Bandbreite so weit ziehen, dass sie zu 90 Prozent stimmt.** Ungeübte ziehen sie fast immer zu eng. Die Gegenprobe lautet: Würde ich eine Wette eingehen, dass der wahre Wert mit neun zu eins drinliegt?
- **Den oberen Rand schätzen immer zwei.** Die zweite Person kommt nicht aus dem Team, das die Arbeit hätte.
- **Wahrscheinlichkeit von außen, Schaden von innen.** Für die Häufigkeit helfen Lagebild und Branchenvorfälle, für den Schaden die eigenen Zahlen aus Controlling und Fachabteilung.
- **Begründung vor Zahl.** Ein Auditor prüft, ob die Einschätzung nachvollziehbar ist.

A 3 Simulationsskript

Das Skript braucht nur Python 3 und numpy. Es spielt 100 000 Jahre durch. In jedem Jahr bestimmt für jedes Szenario ein Zufallszug, ob es eintritt (mit der geschätzten Wahrscheinlichkeit), und ein zweiter, wie teuer es wird. Der Schaden folgt einer Lognormalverteilung, deren 5- und 95-%-Punkte die geschätzte Bandbreite bilden. Das Skript gibt je Szenario den erwarteten Jahresverlust aus, seinen Anteil am gesamten erwarteten Verlust und wie oft das Szenario allein ein Jahr über die Schwelle der

Toleranz bringt. Danach folgt der Wert für alle zusammen. Ist matplotlib installiert, speichert das Skript zusätzlich die Verlustüberschreitungskurve als `verlustkurve.png`.

Eigene Szenarien tragen Sie oben in `SZENARIEN` ein, Schwelle und Toleranz darunter. Für die Bandbreite der Wahrscheinlichkeit lassen Sie das Skript je einmal mit dem unteren und dem oberen Wert laufen, wie Nora mit 4 und 12 Prozent. Das Skript nimmt die Szenarien als unabhängig an. Die Datei liegt als `handout/simulation.py` neben diesem Handout.

```
"""Monte-Carlo-Simulation für wenige Risikoszenarien (Handout „Ein Jahr bei Kestner“).

Je Szenario: Wahrscheinlichkeit im Jahr (Eintritt ja/nein) und eine 90-%-Bandbreite
für den Schaden je Fall (Lognormalverteilung). Benötigt nur numpy; ist matplotlib
installiert, speichert das Skript zusätzlich die Verlustüberschreitungskurve.
Aufruf: python simulation.py
"""
import numpy as np

# Name: (Wahrscheinlichkeit im Jahr, Schaden je Fall 5 %, Schaden je Fall 95 %)
SZENARIEN = {
    "Ransomware Produktion": (0.08, 250_000, 4_000_000),
    "Abfluss Konstruktionsdaten": (0.05, 100_000, 2_000_000),
    "Zahlungsbetrug": (0.25, 20_000, 400_000),
}
JAHRE = 100_000
SCHWELLE = 1_000_000      # Betrag der Toleranz in Euro
TOLERANZ = 0.05           # höchstens in einem von 20 Jahren

# Lognormalverteilung aus der 90-%-Bandbreite: unten = P5, oben = P95.
# Der Logarithmus des Schadens ist normalverteilt, P5 und P95 liegen 1,645 sigma
# unter und über seiner Mitte. Daraus folgt:
#   mu    = (ln P5 + ln P95) / 2
#   sigma = (ln P95 - ln P5) / (2 * 1,645) = (ln P95 - ln P5) / 3,29
# Der Median ist exp(mu) = Wurzel aus P5 * P95, der Mittelwert liegt darüber.
rng = np.random.default_rng(2027)
verluste = {}
for name, (p, unten, oben) in SZENARIEN.items():
    mu = (np.log(unten) + np.log(oben)) / 2          # Mitte der Bandbreite (log)
    sigma = (np.log(oben) - np.log(unten)) / 3.29    # 90 % liegen in ±1,645 sigma
    eintritt = rng.random(JAHRE) < p
    verluste[name] = np.where(eintritt, rng.lognormal(mu, sigma, JAHRE), 0.0)
gesamt = sum(verluste.values())


def de(x, stellen=0):
    return f"{x:,.{stellen}f}".replace(",", " ").replace(".", ",")


print(f"{'Szenario':28} {'erw. Verlust':>14} {'Anteil':>7} {'allein > Schwelle':>18}")
for name, v in verluste.items():
    anteil = 100 * v.mean() / gesamt.mean()       # Anteil am erwarteten Verlust
    print(f"{name:28} {de(v.mean()):>12} € {de(anteil):>5} %"
          f" {de(100 * np.mean(v > SCHWELLE), 2):>16} %")
p_ueber = np.mean(gesamt > SCHWELLE)
urteil = "hält" if p_ueber <= TOLERANZ else "reißt"
print(f"\nErwarteter Jahresverlust, alle zusammen: {de(gesamt.mean())} €")
print(f"Jahre über {de(SCHWELLE)} €: {de(100 * p_ueber, 1)} % "
      f"(Toleranz {de(100 * TOLERANZ, 0)} %: {urteil})")
for q in (0.9, 0.95, 0.99):
    print(f"In {de(100 * q, 0)} % der Jahre bleibt der Verlust unter "
          f"{de(np.quantile(gesamt, q))} €")

try:
    import matplotlib
    matplotlib.use("Agg")
    import matplotlib.pyplot as plt
```

```
except ImportError:
    print("\nmatplotlib nicht installiert, keine Grafik.")
    raise SystemExit
betraege = np.logspace(4, 7, 200)
fig, ax = plt.subplots(figsize=(8, 4.5))
ax.plot(betraege, [np.mean(gesamt > b) for b in betraege], lw=2.5)
ax.plot([SCHWELLE], [TOLERANZ], "x", ms=12, mew=3, color="firebrick",
        label="Toleranz")
ax.set(xscale="log", xlabel="Verlust eines Jahres in €",
       ylabel="P(Verlust > Betrag)")
ax.grid(alpha=0.3)
ax.legend()
fig.savefig("verlustkurve.png", dpi=150, bbox_inches="tight")
print("\nGespeichert: verlustkurve.png")
```

Aufruf ohne eigene Python-Installation, etwa mit Docker aus dem Ordner mit dem Skript:

```
docker run --rm -v $PWD:/h -w /h python:3.12-slim-trixie \
  sh -c 'pip -q install numpy && python simulation.py'
```

Ausgabe mit Kestners drei Szenarien:

```
Szenario                       erw. Verlust  Anteil  allein > Schwelle
Ransomware Produktion             112 276 €    63 %             3,95 %
Abfluss Konstruktionsdaten         32 968 €    18 %             0,92 %
Zahlungsbetrug                     34 034 €    19 %             0,10 %

Erwarteter Jahresverlust, alle zusammen: 179 278 €
Jahre über 1 000 000 €: 5,2 % (Toleranz 5 %: reißt)
In 90 % der Jahre bleibt der Verlust unter 459 043 €
In 95 % der Jahre bleibt der Verlust unter 1 036 375 €
In 99 % der Jahre bleibt der Verlust unter 2 827 230 €

matplotlib nicht installiert, keine Grafik.
```

Die Zahlen sind dieselben wie im Vortrag: 4,0, 0,9 und 0,1 Prozent Millionenjahre je Szenario, gut 5 Prozent für alle drei zusammen. Mit einem anderen Startwert des Zufallsgenerators weichen sie in der letzten Stelle leicht ab. Als Gegenprobe wie in Kestners Pipeline: Der erwartete Verlust eines Szenarios ist Wahrscheinlichkeit mal mittlerer Schaden, bei Ransomware 8 % × 1,43 Mio. € ≈ 114 000 €. Die Simulation liegt mit 112 000 € nahe daran.

Das Skript ist bewusst kurz, damit jemand es vollständig prüfen kann. Wer es mit einem Sprachmodell erweitert, sollte jede Änderung genauso prüfen.

A 4 Die Zuordnungsregel: von der Verteilung ins Feld

So füllt Kestner die Matrix für die Holding. Die Regel passt auf eine Seite, die Schwellen sind eine Entscheidung der Organisation, keine Mathematik.

Voraussetzungen

□ Die Toleranz ist festgelegt, von denen, die den Verlust tragen. Kestner: über 1 Mio. € höchstens in 5 Prozent der Jahre.
□ Für jedes Szenario liegt eine Schätzvorlage vor: Wahrscheinlichkeit, 90-%-Bandbreite des Schadens, Begründung, zwei Schätzende.
□ Die Simulation ist gelaufen, die Gegenprobe des erwarteten Verlusts stimmt.

Zeile: Wahrscheinlichkeit im Jahr

□ Die geschätzte (typische) Wahrscheinlichkeit bestimmt die Zeile, nach den gewohnten Klassen: unter 10 %, 10 bis 30 %, 30 bis 50 %, 50 bis 80 %, 80 % und mehr.

Spalte: typischer Schaden

□ Der typische Schaden ist der Median der Bandbreite: die Wurzel aus unterem mal oberem Rand. Ransomware: √(250 000 × 4 000 000) = 1 Mio. €.
□ Er bestimmt die Spalte: unter 50 000 €, 50 000 bis 250 000 €, 250 000 € bis 1 Mio. €, 1 bis 5 Mio. €, 5 Mio. € und mehr.
□ Die 90-%-Bandbreite steht als Balken über den Nachbarfeldern. Ein Balken über drei Felder heißt: Die Schätzung ist unsicher, nicht falsch.

Farbe: Anteil an der Toleranz

□ Aus der Simulation: In wie viel Prozent der Jahre bringt dieses Szenario allein den Verlust über den Betrag der Toleranz (1 Mio. €)?
□ **Rot** ab der halben Toleranz (bei Kestner 2,5 %), **gelb** ab einem Zehntel (0,5 %), sonst **grün**.
□ Die Felder bleiben grau. Die Farbe gehört dem Punkt, nicht dem Feld.

Prüfen

□ Alle Szenarien zusammen: Hält die Toleranz? Den Wert neben die Matrix schreiben.
□ Auf die unsicherste Eingabe prüfen: Hält die Toleranz auch am oberen Rand der Wahrscheinlichkeit?
□ Wo Matrix und Simulation auseinanderliegen, beginnt das Gespräch.
□ Niemals zwei Stufen miteinander multiplizieren und mit dem Produkt weiterrechnen.

Tabelle 15: Die Regel angewandt auf Kestners drei Szenarien.

Kestner, September 2026	Zeile	Spalte	Balken	Farbe
Ransomware Produktion	unter 10 %	1 bis 5 Mio. €	250 000 € bis 4 Mio. €	4,0 %, rot
Abfluss Konstruktionsdaten	unter 10 %	250 000 € bis 1 Mio. €	100 000 € bis 2 Mio. €	0,9 %, gelb
Zahlungsbetrug	10 bis 30 %	50 000 bis 250 000 €	20 000 bis 400 000 €	0,1 %, grün

A 5 Zum Weiterlesen

- Louis Anthony Cox Jr.: What's Wrong with Risk Matrices? *Risk Analysis*, 2008.
- Douglas W. Hubbard, Richard Seiersen: *How to Measure Anything in Cybersecurity Risk.* Wiley, 2023.
- Bruno de Finetti: *Theory of Probability: A Critical Introductory Treatment.* Wiley, 1974.
- Philip E. Tetlock, Dan Gardner: *Superforecasting: The Art and Science of Prediction.* Crown, 2015.
- Tom Chivers: *Everything Is Predictable: How Bayesian Statistics Explain Our World.* Atria/One Signal, 2024.
- David J. Snowden, Mary E. Boone: A Leader's Framework for Decision Making. *Harvard Business Review*, 2007.

- Stanley Smith Stevens: On the Theory of Scales of Measurement. *Science*, 1946.
- Society for Risk Analysis (Terje Aven u. a.): *Society for Risk Analysis Glossary.* 2018. https://www.sra.org/risk-analysis-introduction/risk-analysis-glossary/
- The Open Group: Open FAIR, Risk Taxonomy (O-RT) 3.1 und Risk Analysis (O-RA) 2.1, 2025.
- kailibrate, quelloffene App zum Kalibrieren eigener Wahrscheinlichkeitsschätzungen: https://github.com/kaijen/kailibrate

Kontakt

Kai Jendrian, Secorvo Security Consulting
kai.jendrian@secorvo.de
https://blog.0x2e6b6169.de