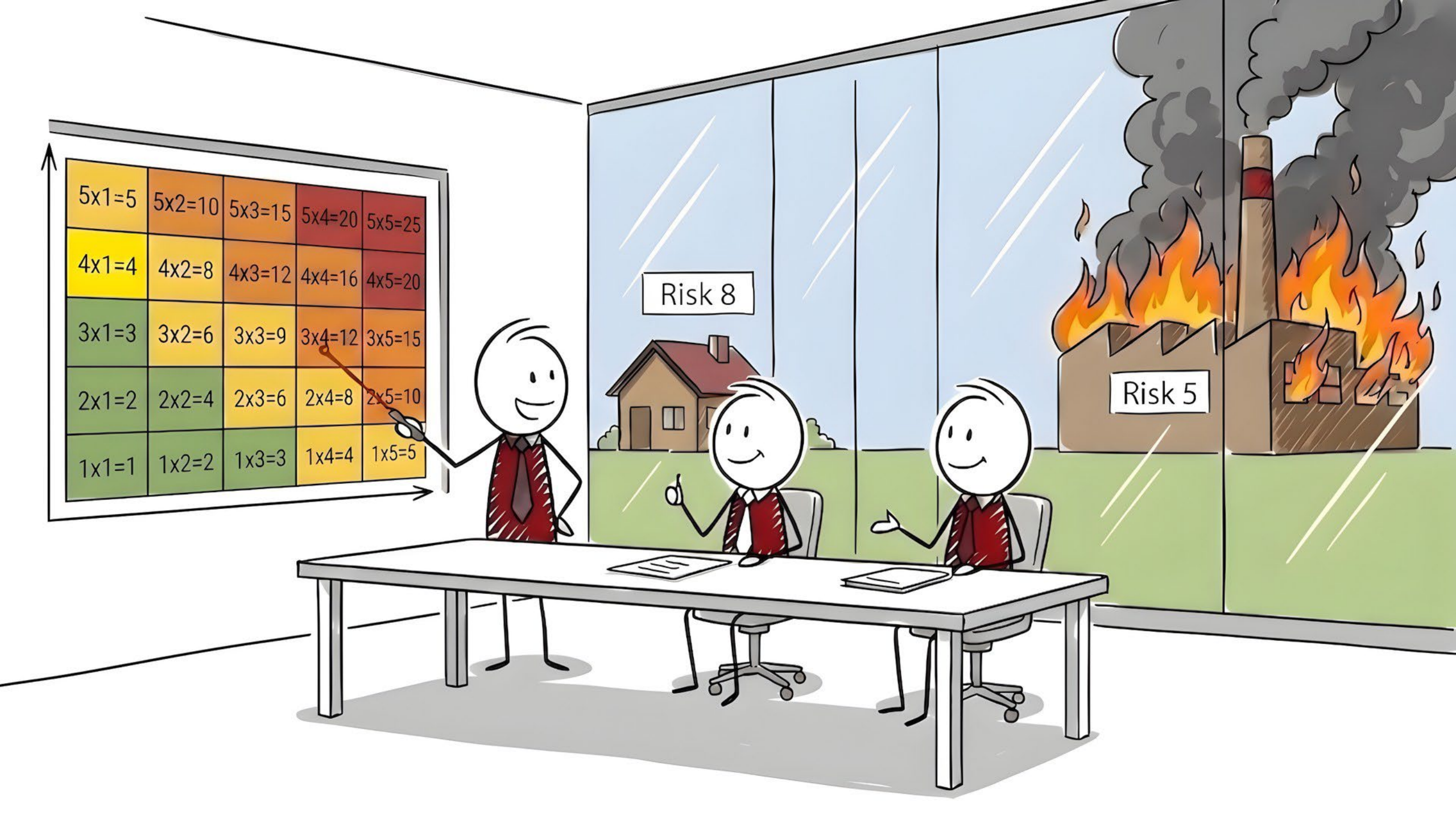
T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

Umdenken statt Abhaken: Informationssicherheit jenseits ausgetretener Pfade

Kai Jendrian, secorvo


5x1=5
5x2=10
5x3=15
5x4=20
5x5=25
4x1=4
4x2=8
4x3=12
4x4=16
4x5=20
3x1=3
3x2=6
3x3=9
3x4=12
3x5=15
2x1=2
2x2=4
2x3=6
2x4=8
2x5=10
1x1=1
1x2=2
1x3=3
1x4=4
1x5=5
Risk 8
Risk 5

Kestner Antriebstechnik GmbH

Getriebe für Landmaschinen und Fördertechnik

rund 200 Beschäftigte, ein Werk, 48 Mio. € Umsatz

Ein Großkunde verlangt bis Jahresende ein
Zertifikat nach ISO/IEC 27001

DIE PERSONEN

Nora Albrecht · ISB, seit acht Monaten

Winfried · Werkstudent bei Nora

Herr Kübler · IT-Leitung

Herr Demir · Produktionsleitung

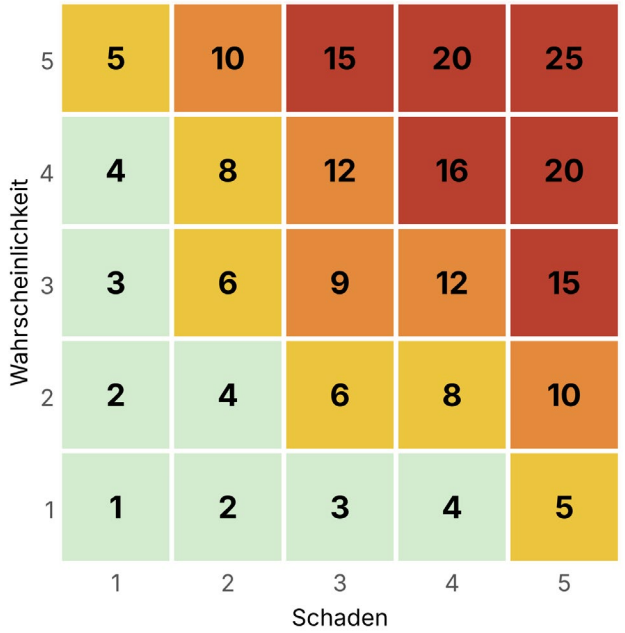
Frau Brandt · Controlling

Dr. Hesse · kaufmännische Geschäftsführerin

dazu: die Holding, ein Auditor

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.

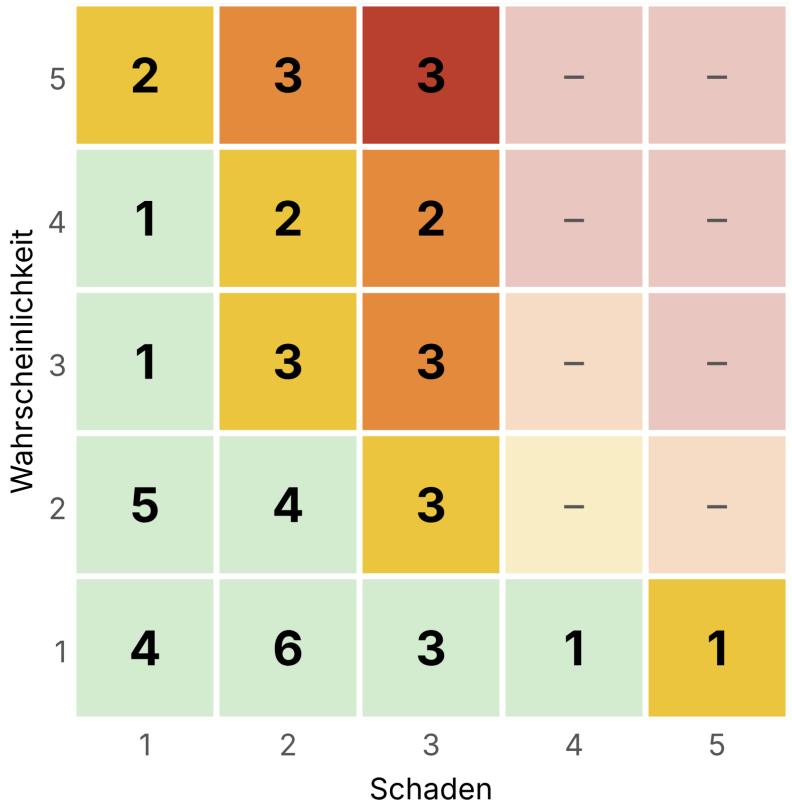
Die Vorlage



Die Excel-Vorlage für die Risikobewertung: Wahrscheinlichkeit mal Schaden, je fünf Stufen. Akzeptiert ist alles bis 8.

> Der Berater: „Füllen Sie das aus, dann sind Sie fürs Audit gerüstet.“

Das Ergebnis



Anzahl Risiken je Feld

47 Risiken: 3 rot, 8 orange, 11 gelb

✓

Dr. Hesse: „Schön. Wir haben 120 000 € frei. Wofür?“

Nora blättert im Register. Die Antwort steht nicht darin.

Ein vollständiges Register enthält noch keine Antwort auf die Budgetfrage.

Vier Hürden in einem Jahr

Begriffe · Rechnung · Ablauf · Werkzeug

Alle sagen Risiko

Und was meinen sie damit?

Drei Sätze in derselben Stunde

Herr Demir: „Das **Risiko** ist Ransomware.“ — eine Bedrohung

Herr Kübler: „Die alten Steuerungsrechner sind ein **Risiko**.“ — eine Schwachstelle

Nora: „Das **Risiko** ist 12.“ — ein Maß für das Risiko

Danach streiten sie 40 Minuten, ob die 12 **richtig** ist.

Was Risiko ist, sagt keiner. Deshalb reden alle aneinander vorbei.

Nora liest ISO/IEC 27001 noch einmal

ABHAKEN

„6.1.2 verlangt eine Risikobewertung. Die Vorlage hat eine Matrix. Fertig.“

UMDENKEN

„6.1.2 verlangt konsistente, gültige und vergleichbare Ergebnisse. Liefert die Vorlage das?“

Vergleichbar wird nur, was alle gleich verstehen. Vor der Matrix steht deshalb ein gemeinsames Verständnis der Begriffe, allen voran von Risiko.

Ein halber Tag, zwei Seiten Glossar.
Erster Satz: ***Risiko ist die Auswirkung von Unsicherheit auf Ziele*** (ISO 31000).

Neue Zahlen aus der Holding

Dieselben Risiken, andere Rangfolge?

Die Holding schickt ihre eigene Vorlage

Ab jetzt berichtet Nora im Format des Konzerns.

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

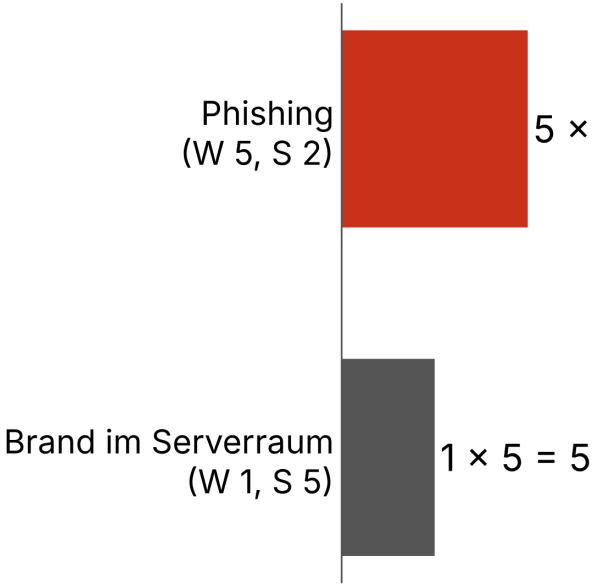
> Die Holding: „Schaden wächst nicht linear. Jede Stufe höher kostet ein Vielfaches.“

Nur die Schadensklassen bekommen neue Zahlen. Winfried, der Werkstudent, rechnet die 47 Risiken an einem Nachmittag neu, die Einstufungen übernimmt er unverändert.

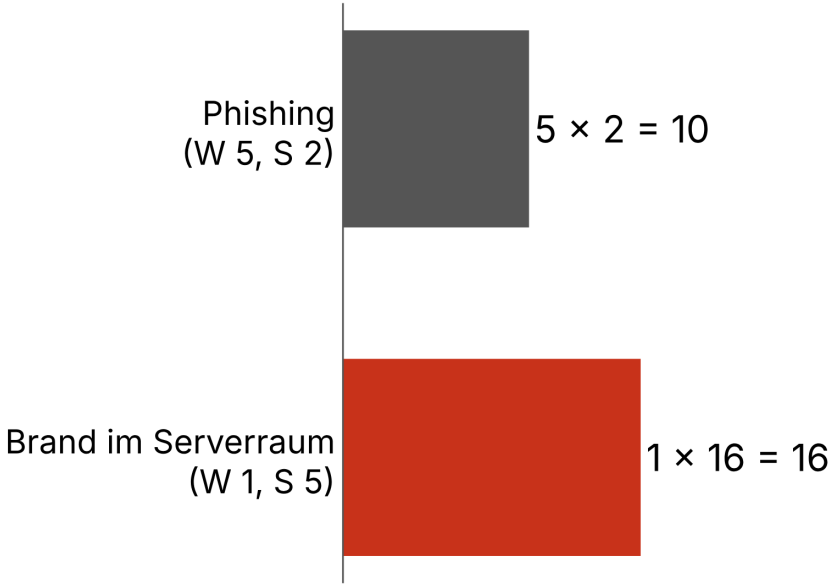
> Am nächsten Morgen hat das Register eine andere Reihenfolge.

Gleiche Einstufung, andere Reihenfolge

Kestner: Schaden 1 · 2 · 3 · 4 · 5



Holding: Schaden 1 · 2 · 4 · 8 · 16

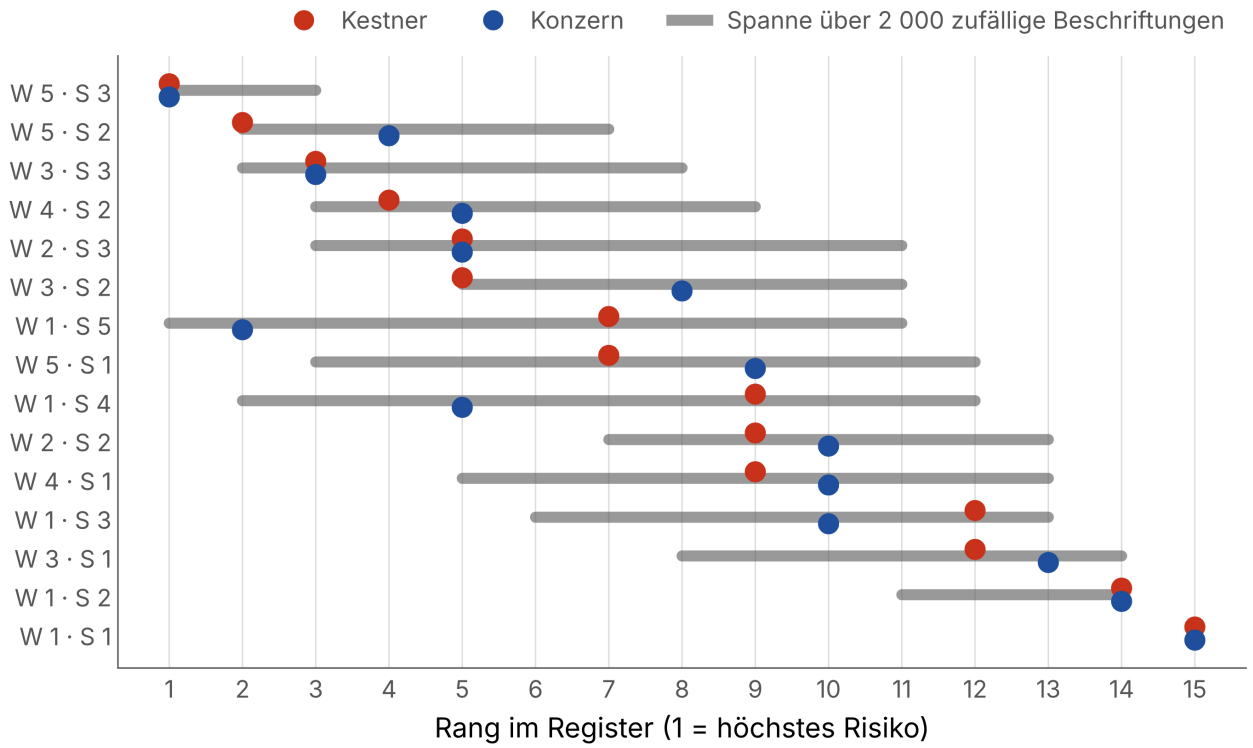


> Winfried: „Ich habe nur neu gerechnet. Warum steht der Brand jetzt vor Phishing?“

Die Rangfolge hängt an den Zahlen für die Stufen, nicht an den Risiken.

Ordinalskala: Jede streng steigende Beschriftung ist gleich gültig (Stevens 1946).

15 Risiken, 2 000 zufällige Beschriftungen



Im Mittel wandert ein Risiko um gut sechs Plätze. Über die Rangfolge entscheidet, wer die Vorlage gebaut hat.

„Was heißt Risiko 8 in Euro?“

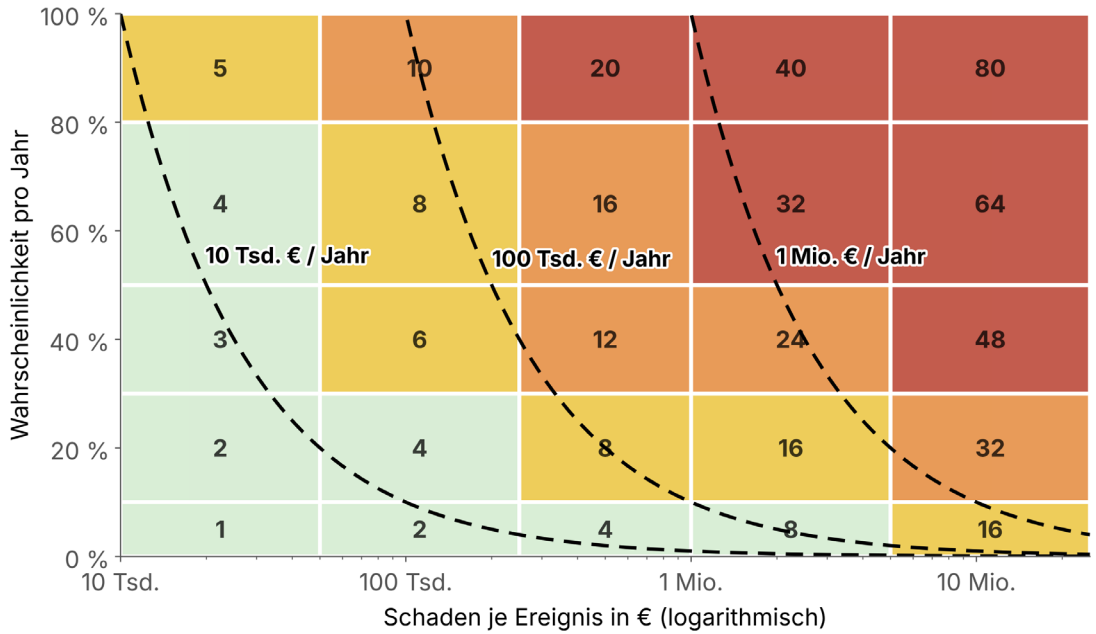
Bei Ransomware steht im Register eine 8. Nora sucht alle Felder mit diesem Wert und rechnet mit den Klassengrenzen nach.

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

Risiko 8 heißt irgendwo zwischen fast null und 500 000 € im Jahr.

> Frau Brandt: „Dann zeichne ich das mal maßstabsgetreu.“

Die Felder sind nicht gleich groß



Gestrichelt: gleicher erwarteter Jahresverlust. ***Gleiche Farbe heißt nicht gleiches Risiko.***

> Frau Brandt: „Bei uns im Controlling wäre das ein Fehler im Berichtswesen.“

Schaden logarithmisch. Bei gleichmäßig verteilten Risiken unterscheidet sich jedes sechste Paar gleicher Farbe um mehr als den Faktor 10.

50 000 € weniger, ganz andere Priorität

Ransomware-Stillstand in der Produktion. Nach dem Wiederanlauftest 9½ statt 10 Tage: Herr Demir rechnet 950 000 statt 1 Mio. €.



50 000 € weniger: Der Matrixwert halbiert sich, Ransomware rutscht im Register weit nach hinten.
Der Verlust sinkt um 5 %.

300 000 €, also 650 000 € weniger: Der Matrixwert bleibt 4, der Verlust sinkt auf ein Drittel.

> Herr Demir: „Wir sind doch nur einen halben Tag schneller.“

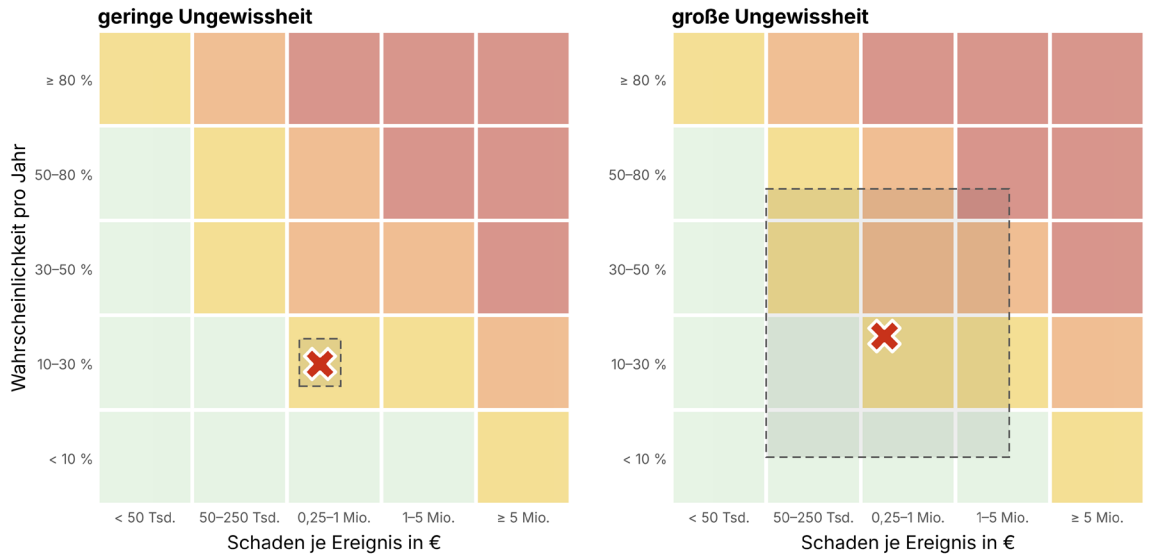
Ein kleiner Schritt über die Klassengrenze kippt die Priorität. Ein großer innerhalb der Klasse ändert nichts.

Wofür die Vorlage kein Feld hat

Zwei Fachleute, ein Feld, wieder Streit

Zwei Schätzungen, ein gelbes Feld

Szenario: Ein fehlerhaftes Update des Dienstleisters legt die Fertigungssteuerung lahm.

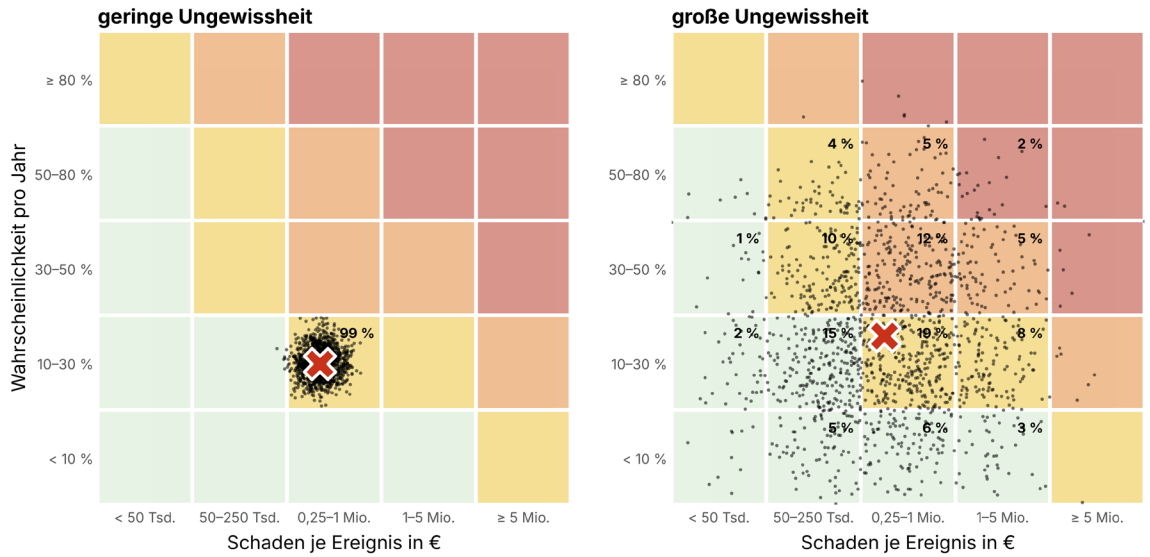


> Herr Kübler: „Drei Updates habe ich begleitet. Nach zwei Tagen läuft es wieder.“
> 15–25 % im Jahr · 300–550 Tsd. €

> Herr Demir: „Wie oft das passiert, weiß ich nicht. Aber in den sechs Wochen vor dem Saisonstart kostet jeder Tag das Fünffache.“
> 5–60 % im Jahr · 50 Tsd. bis 2,5 Mio. €

Was die beiden wissen

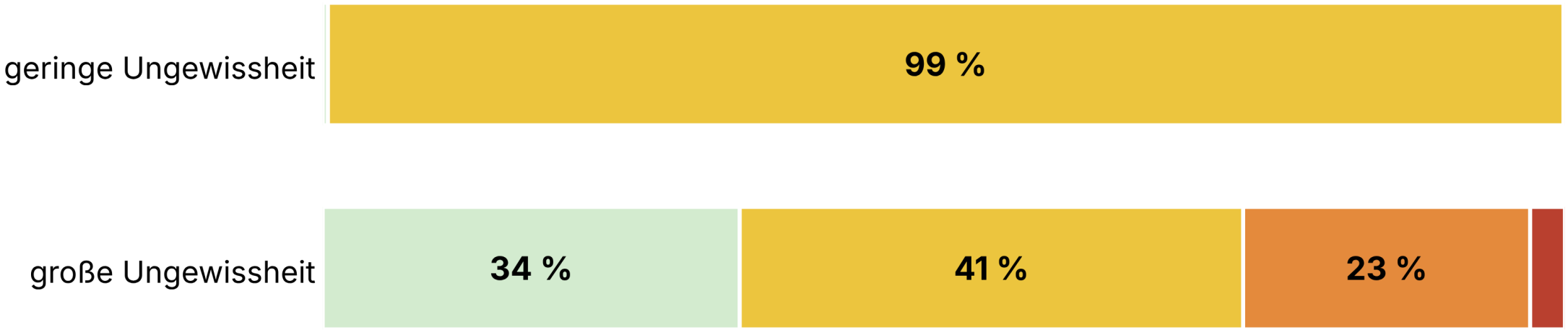
Nora zieht aus beiden Bandbreiten Tausende mögliche Ausfälle. Jeder Punkt ist einer davon.



- Herr Kübler: fast alles im gelben Feld.
- Herr Demir: verteilt über 14 der 25 Felder.

Wieder Streit, diesmal über Gelb oder Rot. Recht hatten beide: In einem Feld steht nicht, wie unsicher die Schätzung ist.

Meistens gelb, manchmal grün, zur Saison rot



Neue Spalten im Register: günstig · typisch · ungünstig

Ins Register gehört die Bandbreite, nicht nur der typische Wert.

BSI-Standard 200-3 zeichnet solche Bandbreiten im Anhang selbst als Balken in die Matrix (Abb. 6).

Wohin mit den 120 000 €?

Naheliegend: in die drei roten aus dem Prolog.

Laut Register 4 Mio. € Schaden im Jahr

Szene 4 · Frau Brandt rechnet das Register in Euro um

Schaden im Jahr	43 Risiken	davon rot und orange (11)
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 Stufen je Risiko: wie oft, wie teuer je Fall	rund 170 000 €	rund 110 000 €

Ohne Ransomware, Datenabfluss, Zahlungsbetrug, versicherten Brand. Jahresergebnis 2 Mio. €.

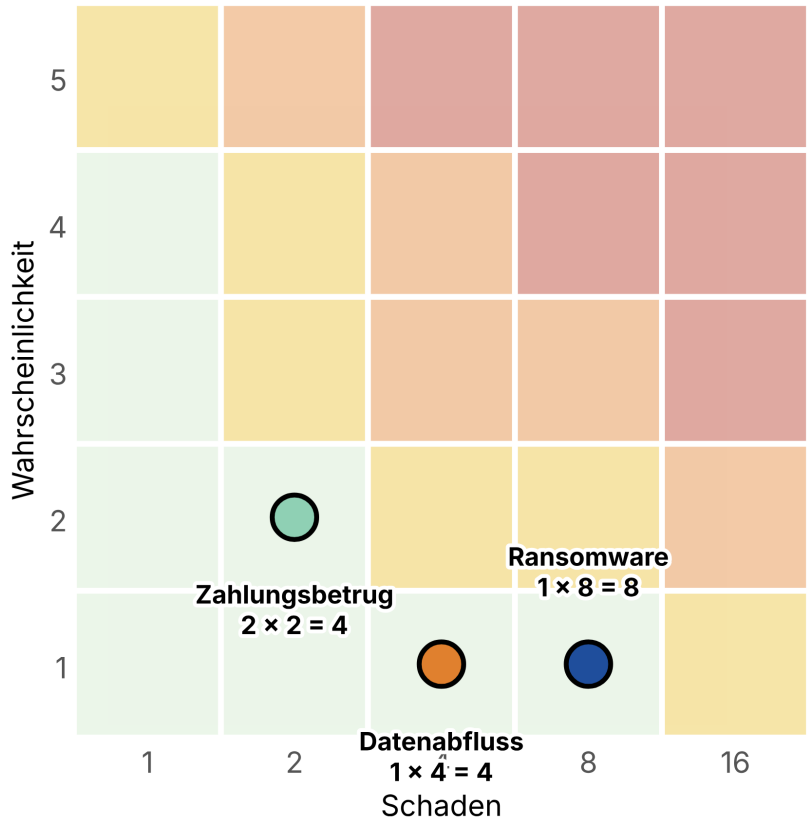
Rot: Netz in der Halle stundenweise weg, alter Zeichnungsstand, verlorene Notebooks. Orange genauso, etwa Phishing an Sammelpostfächer. Je Fall bis 30 000 €; nur die Lieferantenstörung (IT-Ausfall beim Gussteil-Lieferanten) reicht bis 150 000 € und geht als eigener Antrag an Dr. Hesse. **Rot und Orange hieß bei Kestner: häufig, nicht teuer.**

> Frau Brandt: „Laut Register verlieren wir jedes Jahr doppelt so viel, wie wir verdienen. Das Register kann nicht stimmen."

Allein ein Millionenjahr auslösen können nur wenige. Dorthin gehören die 120 000 €. Die simuliert Nora.

Stufen lassen sich nicht addieren. Darum fiel niemandem auf, dass sie nicht stimmen.

Zwei Kandidaten und ein Vergleich, alle grün



	W/Jahr	Schaden (90 %)
Ransomware Produktion Stillstand laut Herrn Demir, nicht versichert	8 %	250 Tsd. bis 4 Mio. €
Abfluss Konstruktionsdaten die Zeichnungen, nicht versichert	5 %	100 Tsd. bis 2 Mio. €
Zahlungsbetrug zum Vergleich: im Vorjahr fast passiert	25 %	20–400 Tsd. €

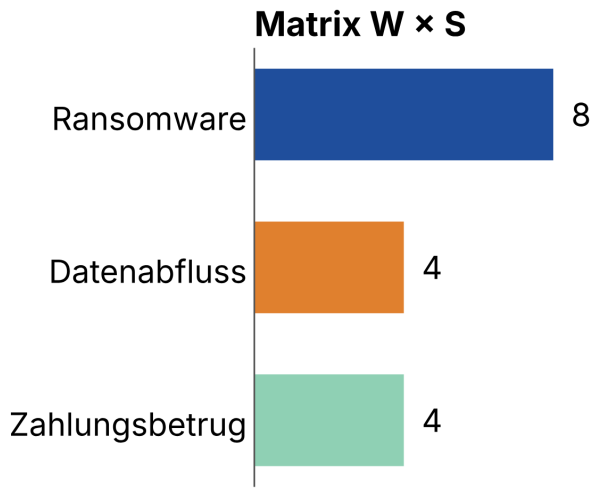
Nicht dabei: Brand (versichert)

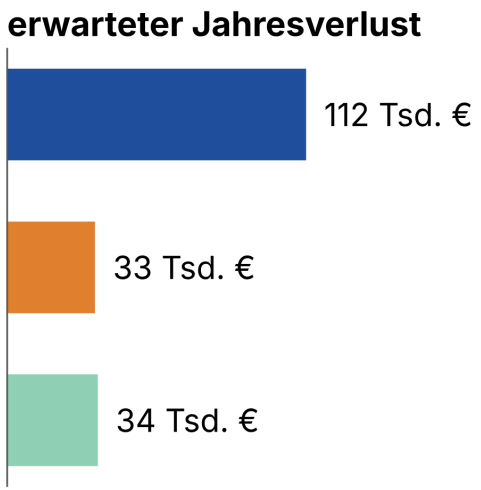
Fertigungssteuerung: keine Updates mehr vor Saisonstart, nur bis 400 000 €

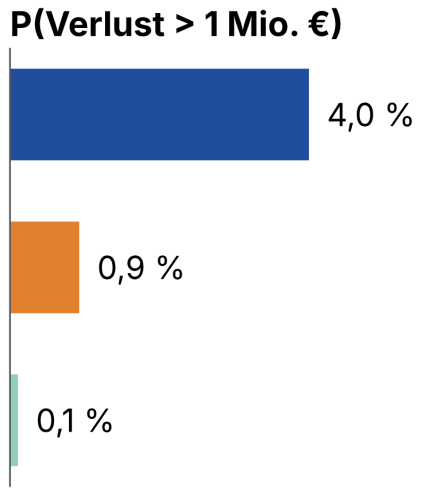
> Laut Vorlage: Ransomware 8, Datenabfluss und Betrug je 4, also gleich wichtig. Alle grün, nichts zu tun.

Drei Maße, drei Rangfolgen

In jedem simulierten Jahr entscheidet der Zufall, ob ein Szenario eintritt und wie teuer es wird.







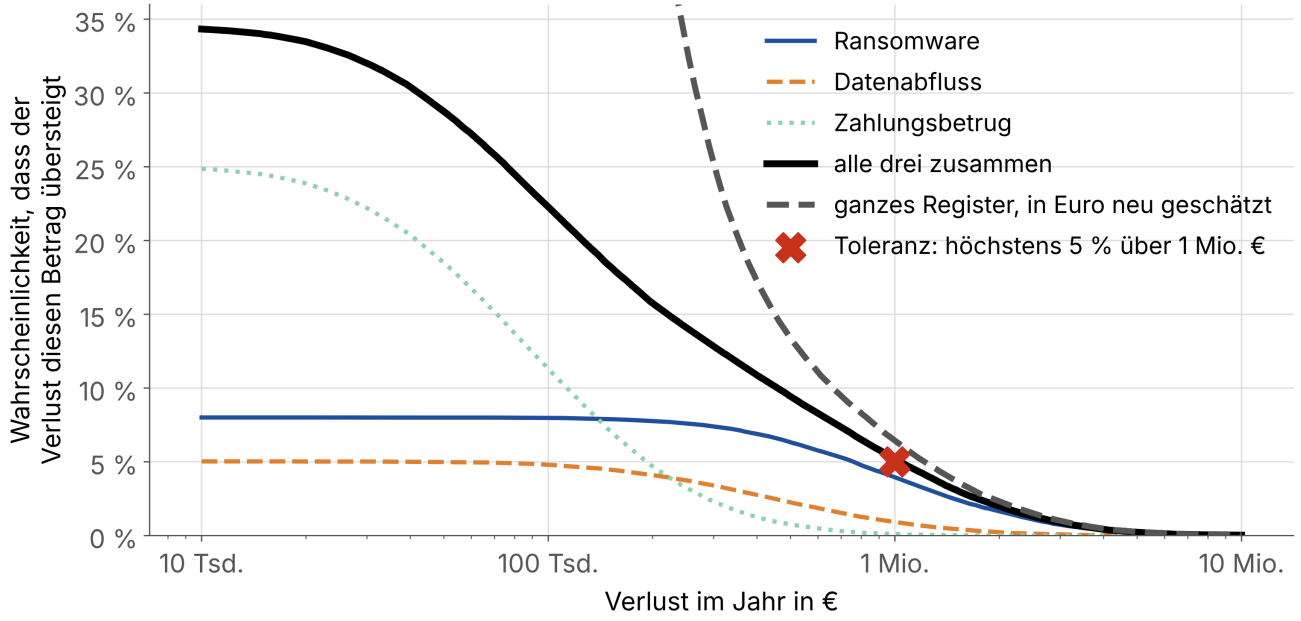
- Vorlage: Ransomware vorn, die anderen gleichauf
- Im Mittel kostet Ransomware dreimal so viel
- Millionenjahre kommen vor allem von Ransomware

Dr. Hesse: „Datenabfluss und Betrug standen bei uns gleichauf?“

Gleicher Wert in der Vorlage, aber neunfaches Millionenrisiko beim Datenabfluss.

„Über 1 Mio. € in einem Jahr: höchstens 5 %“

Frau Brandt: „Eine Million, das ist unser halbes Jahresergebnis.“



Die Kurve zeigt, wie oft ein Jahr mehr kostet als der Betrag darunter. Weiß: alle drei Szenarien zusammen.

Bei 1 Mio. € zeigt sie gut 5 %. Die Toleranz reißt knapp.

Grau: dazu die 43 übrigen Risiken von Frau Brandt. Mit dem ganzen Register: 6,5 %, die Toleranz reißt deutlicher.

Jetzt hat Dr. Hesse einen Maßstab: Die 120 000 € sollen die Kurve unter das Kreuz drücken.

Ganzes Register je nach Ransomware-Wahrscheinlichkeit (4–12 %): 4 bis 9 %.

Eine Verteilung beschreibt ein Risiko *besser als eine Ordinalzahl.*

Gerechnet wird mit Verteilungen. Die Matrix bildet das Ergebnis für das Management ab.

Der Ansatz hat einen Namen: Open FAIR (The Open Group, O-RT und O-RA).

Wie gut schätzt Kestner?

Herr Kübler, Herr Demir und die anderen auf dem Prüfstand

Fünf von zehn statt neun von zehn

Ob die Toleranz hält, hängt an Schätzungen wie der Ransomware-Wahrscheinlichkeit: „4 bis 12 % im Jahr“. Nora beginnt mit Bruno de Finetti (1974):

> Wahrscheinlichkeit ist ein Maß für die Unsicherheit einer schätzenden Person.

KALIBRIEREN

Zwanzig Schätzfragen mit bekannter Antwort, je eine 90-%-Bandbreite.

Bei Herrn Kübler enthalten nur zehn der zwanzig Bandbreiten die Antwort. Er war sich zu sicher, wie fast alle beim ersten Mal.

VERENGEN

Wahrscheinlichkeit von außen: Lagebild, Vorfälle bei anderen Zulieferern.

Schaden von innen: die Stillstandsrechnung für die Cyberversicherung.

Fachsprache: Bayes-Update von a priori zu a posteriori. Herr Demir: „Ich hab mal nachgefragt.“

Subjektiv heißt nicht beliebig. Objektiv wird eine Wahrscheinlichkeit nie, prüfbar schon.

Schlechte Schätzer, und trotzdem simulieren?

> Herr Demir: „Wenn wir nur fünf von zehn treffen, was taugt dann die Simulation?“

1. Schätzen lässt sich üben. In der zweiten Runde trifft Herr Kübler 16 von 20.
2. Die Bandbreite zeigt, wie unsicher eine Eingabe ist. Zu enge Ränder fallen auf.
3. Die Matrix bekommt dieselben Schätzungen. Sie verbirgt nur, wie unsicher sie sind.

Schlechte Eingaben sprechen nicht gegen die Rechnung, sondern gegen das Verstecken.

Wer entscheidet was?

Vom Ticket bis zur Geschäftsführung

„Bleibt offen. Der Lieferant braucht den Zugang.“

Freitag, 15 Uhr. Ein Administrator findet an der Firewall eine offene Verwaltungsschnittstelle, über die ein Maschinenlieferant fernwartet. Er lässt sie offen und schreibt ins Ticket: „Mittel, akzeptiert.“ Geht es schief, steht die Produktion: schlimmstenfalls Millionen aus dem Budget von Herrn Demir.

ABSCHÄTZEN

Wie wahrscheinlich? Wie viel Schaden an unseren Zielen?

Fachleute aus IT, Produktion, Sicherheit. Bandbreite in Prozent und Euro.

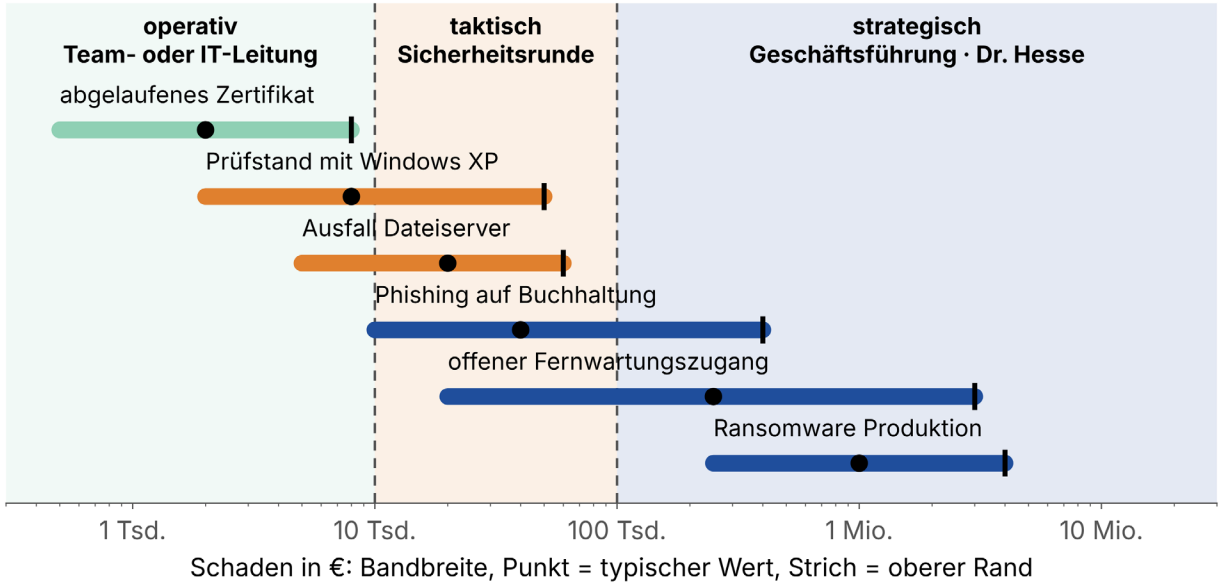
BEWERTEN

Akzeptieren, mindern, übertragen, meiden? Gegen Kosten, Termine, Chancen.

Wer für die Folgen einsteht und die Befugnis hat: Budget, Haftung.

Ein Risiko akzeptieren darf nur, wer für die Folgen einstehen muss.

Der obere Rand bestimmt die Ebene



> Prüfstand mit Windows XP: typisch 8 000 €, schlimmstenfalls 50 000 €. Abschotten, ersetzen oder tragen, das wägt die Sicherheitsrunde ab.

> Ransomware in der Produktion: schlimmstenfalls mehrere Millionen. Über die 120 000 € entscheidet Dr. Hesse.

Schwellen bei Kestner nach dem Jahresergebnis. Risiken nahe einer Schwelle gehen eine Ebene höher. Den oberen Rand schätzen immer zwei.

Ordnung per Software?

Ein GRC-Angebot und das, was schon im Haus ist

Ticket, Wiki und Git reichen

> Der Dienstleister: „Wir übernehmen Ihr Register eins zu eins, Ampel inklusive.“

Nora fragt zurück: Welcher Schritt aus Szene 6 braucht überhaupt neue Software? **Keiner.**

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

Ein Werkzeug bildet einen Ablauf ab. Es ersetzt ihn nicht. Oft reicht, was schon im Haus ist.

Das Audit

Was der Auditor sehen will

„Wo ist denn Ihre Risikomatrix?“

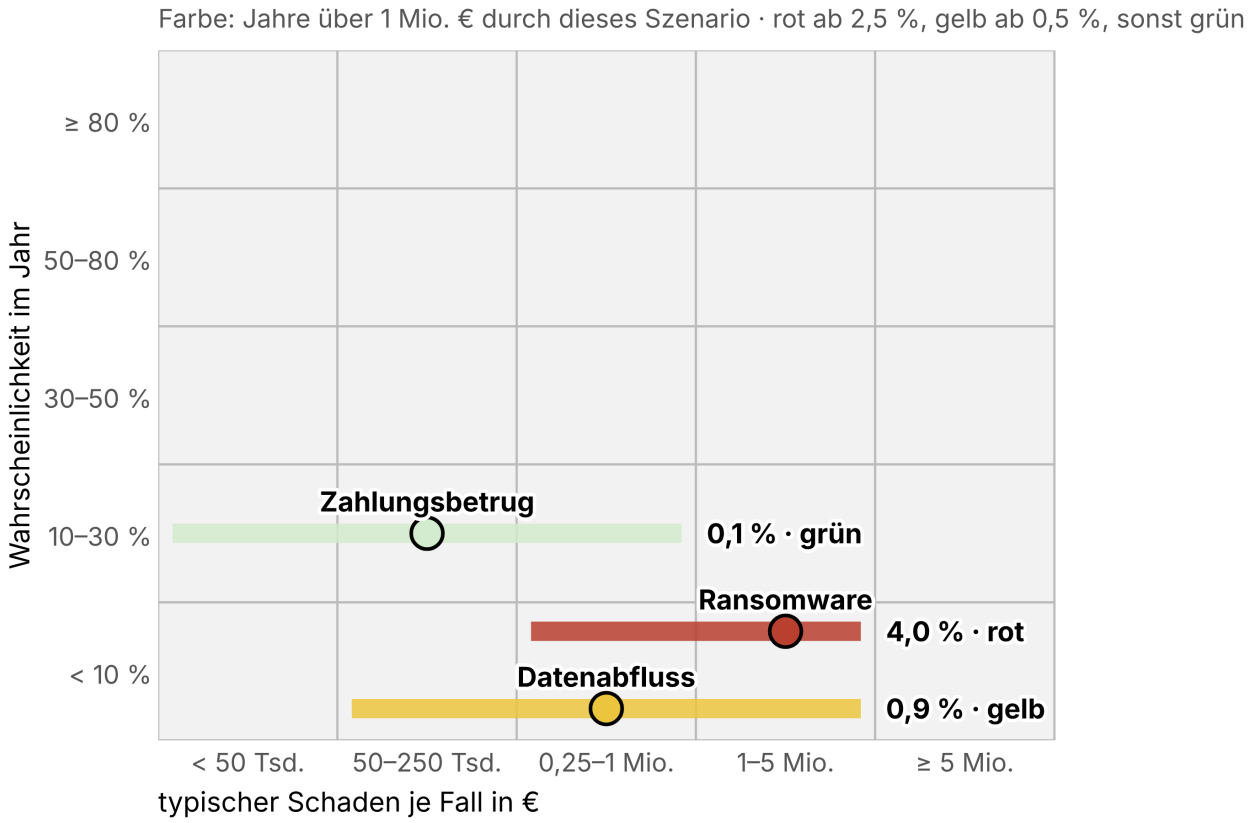
Der Auditor fragt nach 6.1.2	Nora zeigt
Kriterien für Risikoakzeptanz	Toleranz der Holding, Schwellen je Ebene
konsistente, gültige, vergleichbare Ergebnisse	Glossar, Schätztraining, Begründung je Bandbreite
Folgen, realistische Wahrscheinlichkeit, Risikohöhe	in Prozent und Euro, addierbar
Risikoeigentümer,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

> Der Auditor: „Ransomware in der Produktion, 8 % im Jahr. Woher kommt die Zahl?“ Nora zeigt Begründung und Historie im Register.

Der Auditor prüft die Begründung einer Einschätzung, nicht ihre Farbe.

Die Matrix darf bleiben. ***Als Abbild der Verteilung, nicht als Rechnung.***

Wie aus der Verteilung ein Matrixfeld wird



Zeile = Wahrscheinlichkeit im Jahr
Spalte = typischer Schaden

Balken = 90-%-Bandbreite, reicht über mehrere Felder

Farbe = wie oft dieses Szenario allein ein Jahr über 1 Mio. € treibt: rot ab 2,5 % (halbe Toleranz), gelb ab 0,5 % · alte Rechnung: alle drei grün

Das Raster bleibt, die Farbe gehört dem Risiko und lässt sich nachrechnen.

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	Ablauf zuerst, dann Ticket, Wiki, Git

> Und Dr. Hesses 120 000 €? Gehen zuerst in den Ransomware-Schutz der Produktion. Ein Jahr über 1 Mio. € wird von 6,5 auf 3,5 % seltener (Ransomware 3 statt 8 %), die Toleranz hält.

Kestner hatte Glück.

Eine ISB, die dranbleibt. Eine Geschäftsführerin, die nachfragt. Eine Holding, die eine Zahl festlegt. Ein Auditor, der Begründungen liest.

Wo Kestner hätte scheitern können

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 %“ 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 klein anfangen.

Drei Schritte

1 Ein halber Workshoptag für die Begriffe

2 Für die wichtigsten Risiken eine Bandbreite auf der vorhandenen Farbskala

3 Die drei Szenarien, über die bei Ihnen am meisten geredet wird, in Prozent und Euro schätzen, simulieren, neben die Matrix legen

Nicht jede Frage lässt sich durch Analyse beantworten

klar

Passwortrichtlinie: Best Practice anwenden

kompliziert

Ransomware-Häufigkeit: analysieren, schätzen, rechnen

komplex

Fernwartung durch 30 Lieferanten: erst bei einem über Sprungserver, beobachten, nachsteuern

chaotisch

Verschlüsselung läuft gerade: erst handeln, dann analysieren

Noras Simulation hilft im Komplizierten.

Im Komplexen hilft ausprobieren, beobachten, nachsteuern.

Dave Snowden: Cynefin-Modell

Schlusssatz

Der Wert einer Risikoanalyse liegt nicht in der genaueren Zahl,

sondern in der Einsicht, wie viel wir nicht wissen.

Kai Jendrian · kai.jendrian@secorvo.de

blog.0x2e6b6169.de



Reserve

Jede steigende Zahlenreihe ist erlaubt

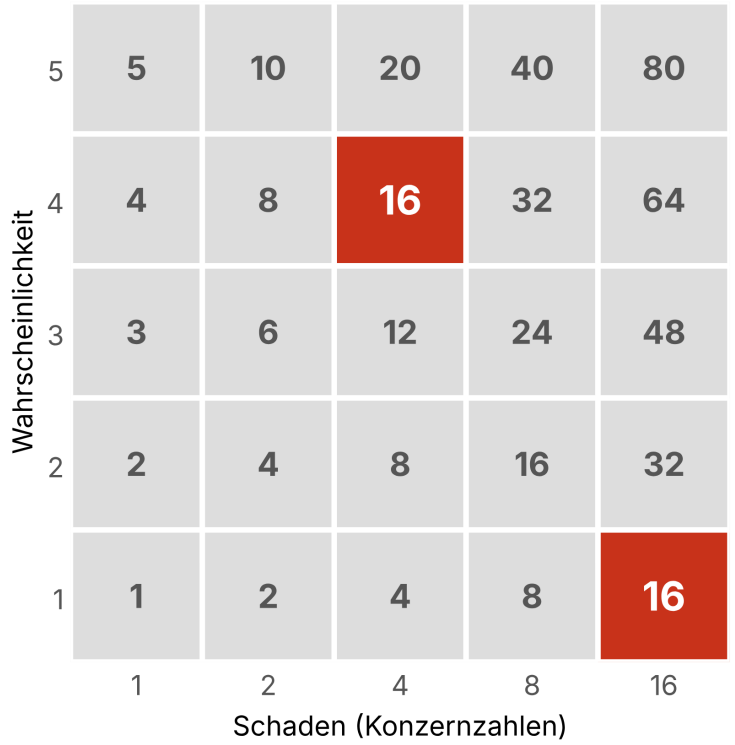
Nora nimmt 15 Risiken aus dem Register, jedes aus einem anderen Feld der Matrix, von W 5 · S 3 bis hinunter zu W 1 · S 1.

Dann lässt sie den Rechner 2 000 Beschriftungen würfeln. Einzige Regel: Jede Stufe bekommt eine größere Zahl als die vorige.

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 → Rang 7
Konzernvorlage	1 · 2 · 3 · 4 · 5	1 · 2 · 4 · 8 · **16**	1 × 16 = 16 → **Rang 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 → **Rang 1**
gewürfelt	1 · 5,4 · 6,3 · 7,8 · 8,6	1 · 1,2 · 1,9 · 2 · **2,2**	1 × 2,2 = 2,2 → **Rang 11**

Alle vier Reihen sind gleich gültig. Der Brand im Serverraum steht auf Platz 1, 2, 7 oder 11.

Zweimal 16



W 4 · S 3: häufiger mittlerer Schaden → Vorbeugung

W 1 · S 5: seltene Katastrophe → Notfallplanung

Im Register nach Konzernformat haben zwei Zeilen den Wert 16:

W 4 · S 3 In zwei von drei Jahren legt ein IT-Ausfall beim Gussteil-Lieferanten, etwa durch Ransomware, die Montage für zwei Tage still.

W 1 · S 5 Der Brand im Serverraum. Einmal in Jahrzehnten, danach steht das Werk.

> Dr. Hesse: „Beide 16. Dann machen wir für beide dasselbe.“

Ein Wert zeigt nicht, ob ein Risiko häufig oder schwer ist. Das eine braucht Vorbeugung, das andere einen Notfallplan.

Drei Abteilungen, zwei Szenarien

Nora fragt: Was kostet es, wenn …

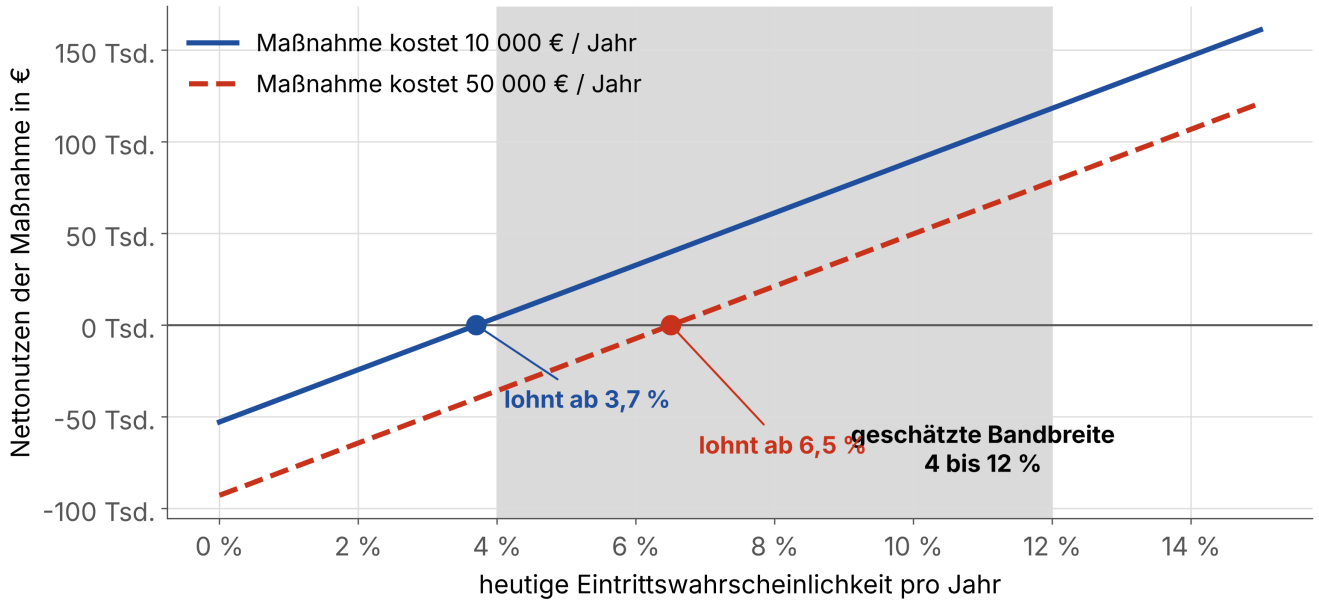
	Konstruktionsdaten abfließen?		**das ERP-System ausfällt?**
Vertrieb	1	„Da sind doch nur Angebote drin.“	3
IT	3	„Je nachdem, welche Zeichnungen.“	3
Konstruktion	5	„Damit baut uns jemand nach.“	3
Excel-Mittelwert	**3**		**3**

Beim ERP sind sich alle einig: „Zwei Tage ohne ERP, dann stehen Einkauf und Versand.“

Auch Uneinigkeit ist Unsicherheit. Der Mittelwert macht aus 1 und 5 eine 3.

Herr Kübler will genauer wissen. Lohnt das?

Ein Schutz senkt die Ransomware-Wahrscheinlichkeit auf 3 %. Vorher soll eine Analyse für 15 000 € klären: Liegt sie heute eher bei 4 oder bei 12 %?



Grau: die heutige Bandbreite. Über der Nulllinie lohnt sich der Schutz.

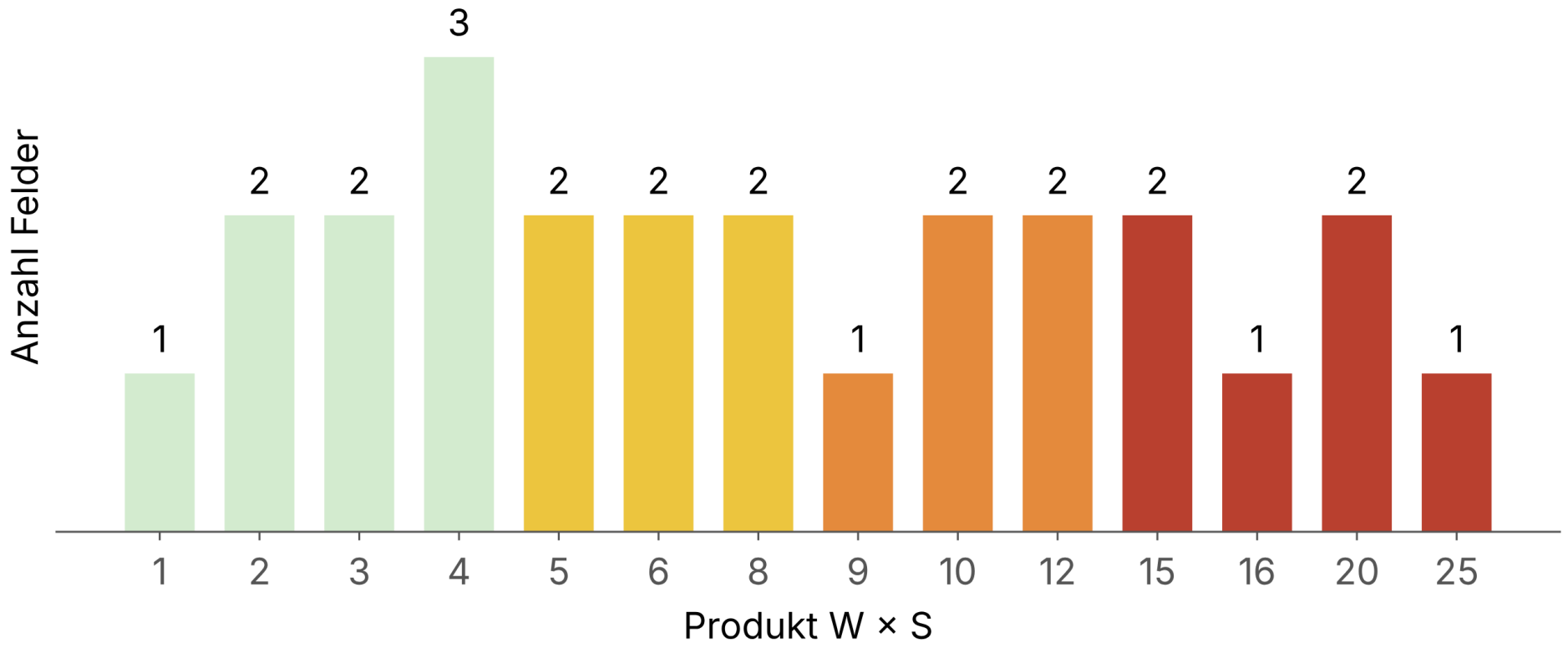
Blaue Linie, Schutz für 10 000 € im Jahr: lohnt in der ganzen Bandbreite. Die Analyse ändert nichts.

Rote Linie, Schutz für 50 000 € im Jahr: lohnt erst ab 6,5 % Ransomware-Wahrscheinlichkeit. Die Analyse wäre höchstens rund 5 600 € wert.

> Nora: „Die Analyse kostet mehr, als sie uns erspart. Die 15 000 € behalten wir.“

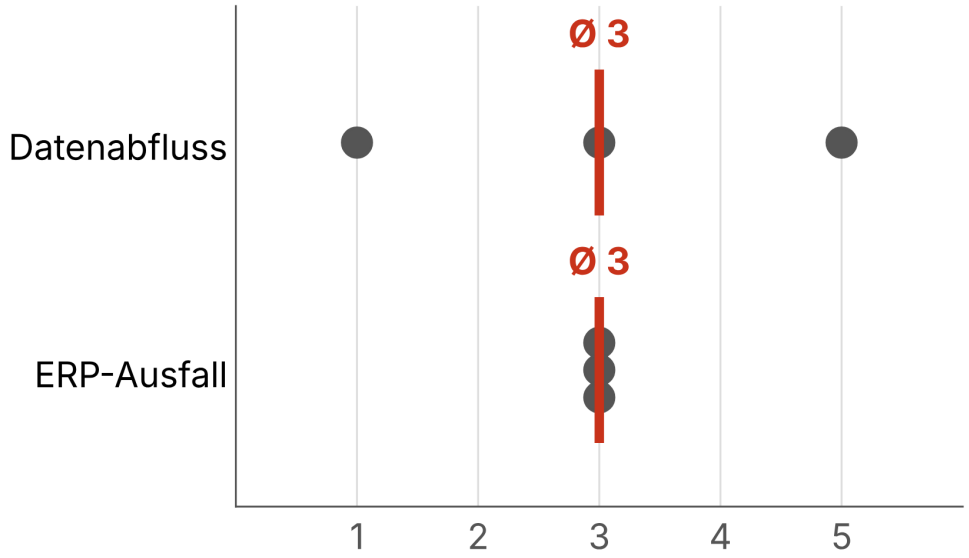
Genauer schätzen lohnt nur, wenn es die Entscheidung ändern kann.

25 Felder, 14 verschiedene Werte

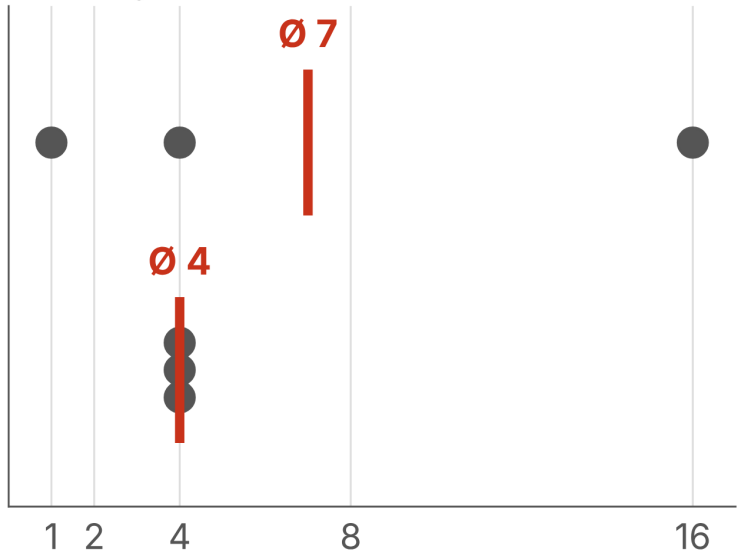


Gleiche Stimmen, andere Mittelwerte

Kestner: Schaden 1 · 2 · 3 · 4 · 5



Holding: Schaden 1 · 2 · 4 · 8 · 16



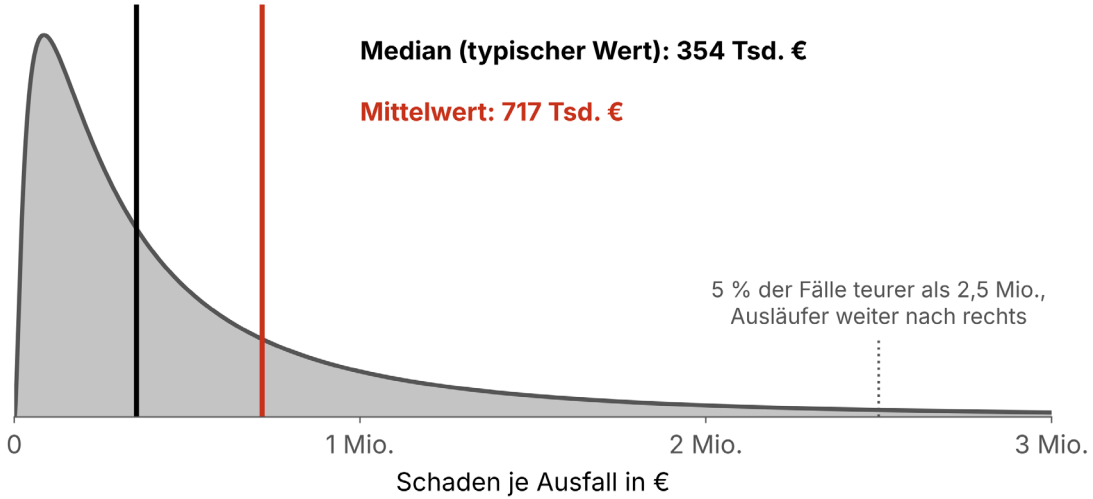
Kestners Stufen: beide Ø 3. Gleichauf.

Zahlen der Holding: Datenabfluss Ø 7, ERP-Ausfall Ø 4. Fast das Doppelte.

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

Der typische Wert unterschätzt

Fertigungssteuerung: Schaden je Ausfall 50 000 bis 2,5 Mio. € (90 %), Wahrscheinlichkeit 5 bis 60 % im Jahr. Die Kurve zeigt, wie sich die möglichen Schäden verteilen.

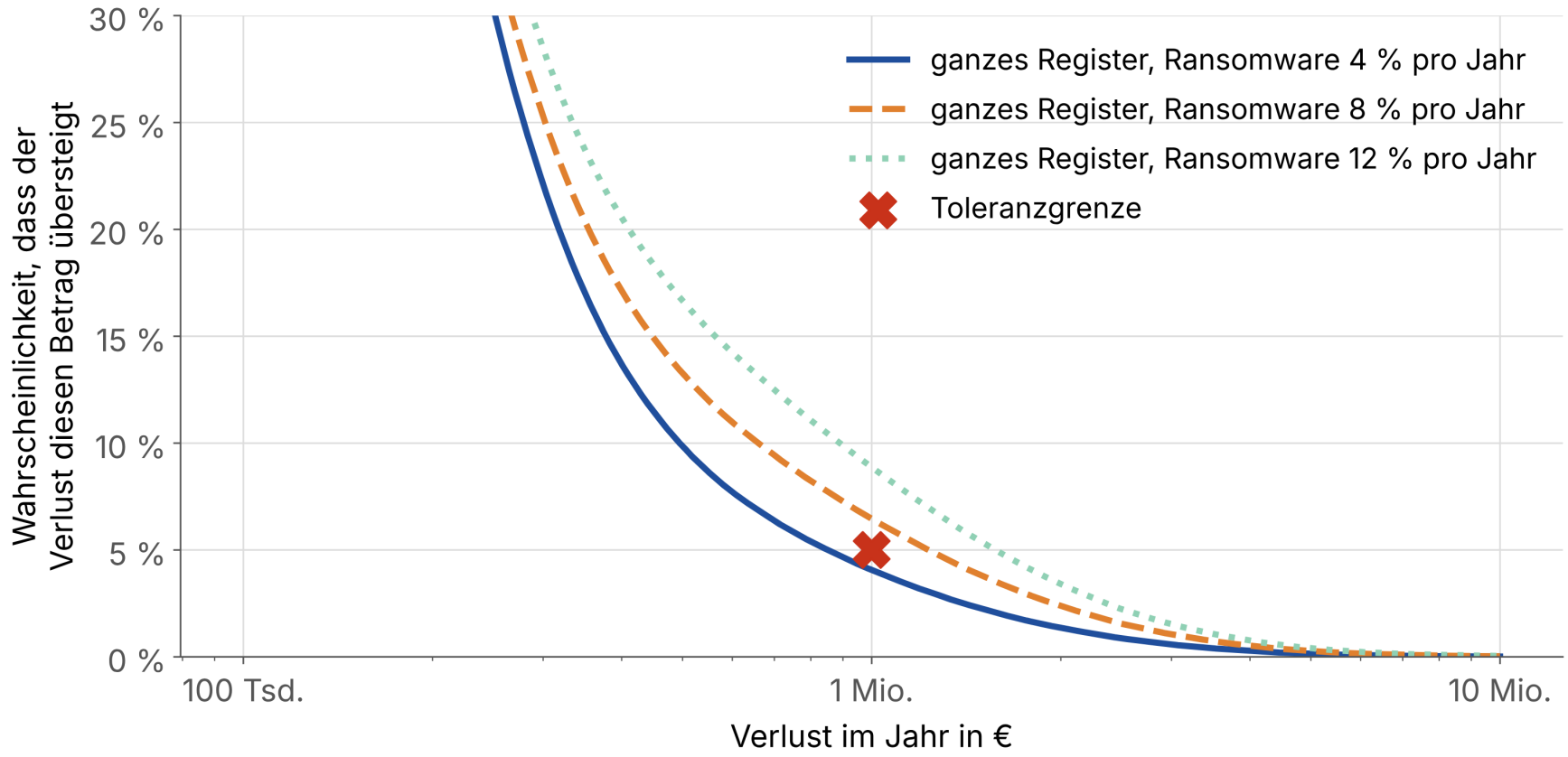


Nach der Vorlage ergeben die typischen Werte rund 90 000 € im Jahr.

Mit allen möglichen Fällen gerechnet: 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.

Hält die Toleranz? Hängt an einer Schätzung



Ganzes Register: drei Szenarien plus die 43 übrigen Risiken von Frau Brandt, in Euro neu geschätzt.