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

Berlin, 10. - 11.11.2026

Der Schnittpunkt von Psychological Safety und Cyber Security - alles rund um Whistleblower und die menschliche Komponente

Felix Rosbach, Crossing Waters

Dienstag, 9:47 Uhr

Ihr Passwort läuft heute ab

Jetzt verlängern



Anna klickt.

„Wird schon nichts gewesen sein.“

„Ich will nicht der Link-Klicker vom Dienst sein.“

Eigene Darstellung

Zwei Firmen, ein Klick

Firma A

9:48	Anna schließt den Tab und hofft
11:30	Das halbe Passwort reicht, der Rest wird erraten
Tag 3	Die IT wundert sich über nächtliche Logins
Tag 9	Niemand weiß, wo es angefangen hat

Firma B

9:51	Anna drückt auf „Melden“
9:52	Antwort: „Danke, gut dass du dich meldest“
9:58	Konto gesperrt, Passwort zurückgesetzt
10:15	Warnung an alle: Diese Mail nicht öffnen

„Eine gemeinsame Überzeugung im Team, dass man hier zwischenmenschliche Risiken eingehen kann.“

Amy C. Edmondson, Harvard, 1999 (sinngemäß übersetzt)

Edmondson, A. (1999): Psychological Safety and Learning Behavior in Work Teams. Administrative Science Quarterly 44(2), 350-383

Psychological Safety ist KEIN Kuschelkurs



Nicht: alle sind nett

Zusammenhalt ist etwas anderes. Er kann Widerspruch sogar senken (Gruppendenken).



Nicht: keine Verantwortung

Wer seinen Fehler erklärt, hilft beim Beheben mit. Er ist nicht „raus“, sondern mittendrin.



Sondern: Fehler werden Information

Ein gemeldeter Fehler ist ein Datenpunkt. Ein verschwiegener ist ein Risiko.

Edmondson (1999), Administrative Science Quarterly; Allspaw, J. (2012): Blameless PostMortems and a Just Culture, Etsy Code as Craft

Wir messen das Falsche.

1,5 %

fallen immer wieder rein. Trotz Training.

5 → 21 %

melden. Training vervierfacht das.

Verizon 2025 Data Breach Investigations Report, S. 49 f. (Phishing-Simulationsdaten; 1,5 % ist dort eine vorsichtige Schätzung für den Median)

247 Tage

bis ein Breach erkannt und eingedämmt ist

5 Min

bis die ersten Meldungen da sind

Melden ist Ihr schnellster Sensor.

IBM Cost of a Data Breach Report 2026 (Mittelwert); Lain, Kostiainen, Capkun (ETH Zürich, 2022): Phishing in Organizations, IEEE S&P, Abschn. VII-B (5 Min ab Eingang der Mail)

Anna meldet einen Klick.
Whistleblower melden einen Missstand.

Eigene Darstellung

Uber, 2016

Ein Jahr geschwiegen.

Vom Sicherheitschef.

U.S. Department of Justice, N.D. California: Pressemitteilungen vom Okt. 2022 und 5. Mai 2023

Wirecard, 2018

Der Meldekanal, der am Ende funktioniert hat:

Mama.

Financial Times (D. McCrum): „They tried to destroy me“, 20.05.2021; SMU: How a whistleblower brought down the House of Wirecard, 23.12.2023; CNBC, 25.06.2020

Snowden, 2012

Fast gescheitert an:

PGP einrichten.

The Intercept (M. Lee), 28.10.2014; G. Greenwald: No Place to Hide (Auszug, openDemocracy); Pulitzer-Preise 2014 (PBS NewsHour, 14.04.2014)

Was das Gesetz verlangt: HinSchG

ab 50

Beschäftigten ist eine interne Meldestelle Pflicht

§ 12

7 Tage

bis zur Eingangsbestätigung

§ 17 Abs. 1

3 Monate

nach Bestätigung: Rückmeldung zu Folgemaßnahmen

§ 17 Abs. 2

mündlich

oder in Textform, auf Wunsch auch persönlich

§ 16 Abs. 3

nur

Zuständige haben Zugriff auf eingehende Meldungen

§ 16 Abs. 2

neu

seit 29.07.2026 auch Verstöße gegen die KI-Verordnung

§ 2 Abs. 1 Nr. 10

Hinweisgeberschutzgesetz (HinSchG) vom 31.05.2023 i.d.F. 2026 (gesetze-im-internet.de); setzt die Richtlinie (EU) 2019/1937 um

Das Gesetz verlangt Vertraulichkeit.
Nicht Anonymität.

§ 8 und § 16 Abs. 1 HinSchG

Technik als Vertrauensbeweis

Keine Spuren

Keine IP-Adressen und Browserdaten speichern (so macht es z. B. SecureDrop)

Verschlüsselt

Nur die zuständigen Personen können Meldungen lesen

Rückkanal ohne Namen

Nachfragen über eine Kennung statt über eine Identität

Status sichtbar

Melder sehen, wie anonym sie gerade sind (so macht es z. B. GlobaLeaks)



Vom Briefkasten zur Paketverfolgung

Wer meldet, sieht: eingegangen, in Prüfung, Maßnahme ergriffen. Das baut mehr Vertrauen als jede Richtlinie.

SecureDrop Documentation (docs.securedrop.org); GlobaLeaks Threat Model (docs.globaleaks.org); § 16 Abs. 2 HinSchG

Luftfahrt, 1975



Die Luftfahrt hat das Problem gelöst.

Meldung an eine neutrale Stelle.

Nicht an die, die bestraft.

NASA Aviation Safety Reporting System: CALLBACK Nr. 435, April 2016 (asrs.arc.nasa.gov)

Positiv statt Strafe



Keine Strafrunden

Pflicht-Nachschulung für Mehrfachklicker wirkte nicht besser als freiwillige oder gar keine.



Sofort-Feedback

Jede Meldung bekommt in Minuten ein Danke und später: was daraus wurde. Auch bei Fehlalarm.



Anerkennung, keine Preise

Eine Schachtel Schokolade für jede richtige Meldung hat das Melden nicht erhöht.



Führung klickt zuerst

Nach Vorfällen fragen wir: wie, nicht wer. Und Führung erzählt offen von eigenen Fehlklicks.

Lain et al. (ETH Zürich, 2024): Content, Nudges and Incentives, ACM CCS; Allspaw, J. (2012): Blameless PostMortems and a Just Culture, Etsy

Sicherheit beginnt dort, wo Melden leichter ist als Schweigen.

Eigene Darstellung

Drei Dinge für Montag

1

Messen

Meldequote und Zeit bis zur Meldung als Kern-KPI. Die Klickrate ist nur die Nebenzahl.

2

Antworten

Jede Meldung in Minuten mit einem Danke beantworten und später sagen, was daraus wurde

3

Testen

Den eigenen Meldekanal selbst ausprobieren: anonym erreichbar? Rückkanal? Status sichtbar?

Eigene Empfehlungen auf Basis der genannten Quellen

Danke. Fragen?

Felix Rosbach | linkedin.com/in/felix-rosbach

Die Quellen zu allen Zahlen stehen auf den jeweiligen Folien.