ASSESSMENT PAPER

FACHLICHE EINORDNUNG DER POINT OF RESOLUTION · AUSGABE 02 / 2026

SICHERHEIT · HUMAN FACTORS · KRITISCHE FUNKTIONEN

Menschliche und organisationale Schwachstellen

Human Factors · Social Engineering · Early Warning · Validation kritischer Funktionen

GEGENSTAND	Fachliche Einordnung menschlicher und organisationaler Verwundbarkeit in kritischen und verteidigungswichtigen Infrastrukturen: Social Engineering, legitimer Zugang, Human Factors, Wissens- und Rollenabhängigkeiten sowie die Frage, wann vorhersehbares menschliches Verhalten eine kritische Funktion beeinträchtigen kann.
STAND	20. September 2026
VERSION	1.3 FINAL
DOKUMENTTYP	Assessment Paper
AUSSAGEEBENE	Strategisch · organisatorisch · operativ
QUELLENBASIS	BSI · BAuA · ENISA · CISA · HRC · Fachliteratur · POR
STATISTIK	Keine Personen- oder Ereignisstatistik

LEITGEDANKE DIESER EINORDNUNG

Der Mensch wird nicht dadurch zur Schwachstelle, dass er menschlich handelt. Zur Schwachstelle wird eine Organisation dort, wo vorhersehbares menschliches Verhalten eine kritische Funktion unkontrolliert beeinträchtigen kann.

00

HINWEISE ZUR INTERPRETATION

Was dieses Dokument leistet – und was nicht

Die Darstellung trennt menschliches Verhalten, organisatorische Exposition, belastbare Beobachtung, systemische Vulnerabilität und funktionale Wirkung. Ziel ist keine Bewertung einzelner Personen.

PUNKT	EINORDNUNG
Kein Personenprofil	Das Paper bewertet keine Persönlichkeit, Loyalität, psychische Verfassung oder vermeintliche Gefährlichkeit einzelner Beschäftigter.
Kein Verhaltensverdacht	Eine Auffälligkeit, ein Fehler oder eine Regelabweichung belegt weder Absicht noch Insider-Handeln. Beobachtung, Ursache und Motiv sind getrennt zu behandeln.
System statt Schuld	Human Factors werden als Zusammenspiel von Mensch, Technik, Organisation, Arbeitsbedingungen und Information betrachtet – nicht als individuelles Defizit.
Quellen mit verschiedener Funktion	BSI beschreibt Informationssicherheit und Social Engineering, BAuA sozio-technische Human Factors, ENISA die Cyber-Bedrohungslage, CISA Insider Risk; Romeike und Mestchian liefern Frühwarn- und Risk-Intelligence-Ansätze.
Schutz der Informationssicherheit	Konkrete Manipulationsskripte, Umgehungsmethoden, objektspezifische Schwachstellen oder nutzbare Angriffspfade werden nicht dargestellt.
Datenschutz und Mitbestimmung	Personenbezogene Auswertungen bedürfen eines klaren Zwecks, der Verhältnismäßigkeit, der Datenminimierung und der Beachtung von Datenschutz-, Arbeits- und Mitbestimmungsrecht. Dieses Paper ist keine Rechtsberatung.

LESESCHLÜSSEL

QUELLENAUSSAGE: was eine Quelle festhält.
POR-EINORDNUNG: Übertragung auf kritische Funktionen.
METHODISCHE FOLGERUNG: abgeleitete Arbeitsregel.
VALIDATION: autorisierte Prüfung einer Kontrollannahme innerhalb eines definierten Scopes.

FORMALE REFERENZ: BEHÖRDLICHE LAGEBILD- UND STATISTIKLOGIK

Datenbasis, Interpretation und Aussagegrenze bleiben getrennt. Bei Human Factors ist das besonders wichtig: Eine beobachtete Handlung darf nicht automatisch in eine Aussage über Motiv, Charakter oder Gefährlichkeit einer Person übersetzt werden.

KURZFASSUNG

Sechs Kernaussagen

Die Auswertung verdichtet sich auf sechs Punkte, die für Betreiber unmittelbar handlungsleitend sind.

01 **Human Vulnerability ist keine Persönlichkeitseigenschaft.**

Sicherheitsrelevant wird menschliches Verhalten erst im Zusammenspiel mit Berechtigungen, Arbeitsbedingungen, Prozessen und der Bedeutung einer kritischen Funktion.

02 **Social Engineering nutzt normales menschliches Verhalten.**

Das BSI nennt unter anderem Hilfsbereitschaft, Vertrauen, Angst und Respekt vor Autorität. Die Schutzaufgabe besteht in verlässlichen Verifikations- und Eskalationswegen – nicht in Misstrauen gegen Beschäftigte.

03 **Legitimer Zugang übersetzt Human Factors in Wirkung.**

Je größer physische, digitale oder informationelle Berechtigungen sind, desto wichtiger werden Least Privilege, unabhängige Verifikation, Rollenklärung und belastbare Rückfallebenen.

04 **Routine kann Abweichungen unsichtbar machen.**

Workarounds, wiederkehrende Ausnahmen und dauerhaft tolerierte Störungen verschieben die gelebte Baseline. Dann wird eine Abweichung nicht mehr als solche wahrgenommen.

05 **Frühwarnung erkennt Expositions- und Kontrollveränderungen.**

Relevante Frühindikatoren liegen in Berechtigungen, Arbeitslast, Prozessdrift, Verifikation, Einzelabhängigkeiten, Kommunikation und externer Manipulationsbelastung – nicht in „gefährlichen Menschen“. Einzelindikatoren beweisen weder Absicht noch Ereignis.

06 **Pentesting ist eine Validierungsstufe, kein Ritual.**

Ein Human-Risk-Pentest ist sinnvoll, wenn eine konkrete Kontrollannahme unter realistischen Bedingungen überprüft werden muss. Der HVVI priorisiert den Validierungsbedarf; ein Decision Gate klärt Informationswert, Remediation, Safety, Legal und Testdesign.

01

QUELLENLAGE

Sieben Perspektiven, unterschiedliche Aussagekraft

Die Quellen beantworten unterschiedliche Fragen – von Social Engineering über Arbeitsgestaltung bis zu Insider Risk und Frühaufklärung.

QUELLE	FUNKTION, STÄRKE UND GRENZE
BSI · Social Engineering, IT-Grundschutz	Offizieller Informationssicherheitsrahmen: menschliche Eigenschaften, Personal, Sensibilisierung, Berechtigungen. Grenze: Cyberfokus, keine vollständige Human-Factors-Systemanalyse.
BAuA · Human Factors, Ergonomie	Arbeitswissenschaftlicher Referenzrahmen: sozio-technische Systeme, kognitive und organisationale Ergonomie, Fehlervermeidung. Grenze: kein Insider- oder Social-Engineering-Lagebild.
ENISA · Threat Landscape	EU-Cyberbedrohungslage: Social Engineering als relevante Bedrohungskategorie, aktuelle Trends. Grenze: keine Aussage über individuelle Verwundbarkeit.
CISA · Insider Threat Mitigation	Praxisrahmen für Insider Risk: autorisierter Zugang, unbeabsichtigte und vorsätzliche Risiken, Programmreife. Grenze: US-Kontext, rechtliche Übertragung erforderlich.
Romeike / Mestchian 2005	Frühwarn- und Risk-Intelligence-Grundlagen: schwache Signale, People Risks, Silos überwinden. Grenze: historische Quellen, methodische Grundlage statt Bedrohungsbild.
Ebrahimi et al. 2022	Wissenschaftliche Risikomodellierung: Trennung von Hazard, Vulnerability und Risk. Grenze: dort populationsbezogen; demografische Indikatoren werden nicht auf Beschäftigte übertragen.
Proofpoint / Human Risk Consulting GmbH (HRC)	Industrie- und Validierungsperspektive: Proofpoint zu kanalübergreifender Social-Engineering-Exposition und Human-Centric Security; HRC zu Vishing-, Remote- und physischen Pentests mit Pre-Engagement und Scope. Grenze: kommerzielle Quellen; Kennzahlen keine Prävalenzwerte; die Nennung von HRC begründet keine Kooperation.

BEWERTUNGSREGEL

Amtliche und wissenschaftliche Quellen tragen Definition und Methodik. Industriequellen ordnen aktuelle Angriffs- und Validierungsformen ein. Je näher eine Aussage an einer konkreten Person, Absicht oder Gefährlichkeitsprognose liegt, desto höher ist die Evidenz- und Rechtfertigungsschwelle.

02

BEGRIFFLICHE EINORDNUNG

Der Mensch ist Teil des Systems – nicht dessen Gegenstück

BEGRIFF	ARBEITSDEFINITION IN DIESER PUBLIKATION
Human Factors	Physische, kognitive und organisationale Einflüsse auf menschliches Handeln in einem sozio-technischen System. Mensch, Technik, Aufgabe und Organisation werden gemeinsam betrachtet.
Human Vulnerability	Systembedingte Verwundbarkeit, bei der vorhersehbares menschliches Verhalten in Verbindung mit Exposition, Berechtigung oder fehlenden Kontrollen eine kritische Funktion beeinträchtigen kann.
Social Engineering	Soziale Manipulation mit dem Ziel, Menschen zu sicherheitswidrigen Handlungen, Informationspreisgabe oder Zugangsgewährung zu bewegen. Die operative Durchführung wird hier nicht beschrieben.
Insider Risk	Risiko aus aktuellem oder früherem legitimem Zugang, Wissen oder Vertrauen – vorsätzlich, fahrlässig, unbeabsichtigt oder extern beeinflusst.
Key-Person Dependency	Abhängigkeit einer kritischen Funktion von Wissen, Berechtigung oder Handlungsfähigkeit einzelner Personen oder sehr kleiner Gruppen.
Normalisierung von Abweichungen	Zustand, in dem wiederkehrende Ausnahmen, Workarounds oder Störungen schrittweise als normal akzeptiert werden und ihre Warnwirkung verlieren.

ABGRENZUNG

Ebrahimi et al. verwenden „human vulnerability" populationsbezogen. Übernommen wird nur die methodische Trennung, nicht die demografische Indikatorik.

POR ARBEITSGRUNDSATZ

Nicht die Person ist der Analyseanker, sondern die kritische Funktion und die Reichweite menschlicher Handlung in diesem System.

03

VERWUNDBARKEITSDIMENSIONEN

Human Risk entsteht zwischen Person, Organisation und Funktion

Die folgenden Dimensionen sind keine Charaktermerkmale. Sie strukturieren Bedingungen, unter denen menschliches Handeln für eine kritische Funktion sicherheitsrelevant werden kann.

DIMENSION	BEOBACHTUNGSGEGENSTAND UND BETREIBERFRAGE
Zugang & Berechtigung	Physischer, digitaler und informationeller Zugriff, privilegierte Rollen. Leitfrage: Welche Wirkung kann eine einzelne legitime Handlung entfalten?
Wissen & Abhängigkeit	Erfahrungswissen, Spezialkenntnisse, Schlüsselrollen, Dienstleister. Leitfrage: Welche Funktion verliert Handlungsfähigkeit, wenn eine Person ausfällt?
Arbeitslast & Zeitdruck	Unterbesetzung, Rufbereitschaft, Alarmdichte, parallele Störungen. Leitfrage: Sind sichere Verifikation und Entscheidung unter realen Bedingungen praktikabel?
Prozess & Workaround	Abweichung zwischen dokumentiertem Verfahren und gelebter Praxis. Leitfrage: Welche Ausnahme ist faktisch zum Normalbetrieb geworden?
Kommunikation & Eskalation	Meldewege, Rückmeldung, Hierarchie, Entscheidungsbefugnis. Leitfrage: Erreicht eine Beobachtung rechtzeitig die entscheidungsfähige Ebene?
Kultur & Lernen	Umgang mit Fehlern, Near Misses, Widerspruch und Unsicherheit. Leitfrage: Werden schwache Signale gemeldet – oder vermieden und normalisiert?
Technik & Schnittstelle	Usability, Alarmierung, Mensch-Maschine-Interaktion, Systemtransparenz. Leitfrage: Unterstützt die Technik sicheres Handeln oder erzeugt sie vermeidbare Fehlermöglichkeiten?

> **QUELLENAUSSAGE BAUA UND BSI**
>
> *Die BAuA betrachtet Human Factors im Kontext sozio-technischer Arbeitssysteme und zielt auf die Vermeidung von Handlungs- und Bedienfehlern. Das BSI betont, dass selbst aufwendige Sicherheitsvorkehrungen wirkungslos werden, wenn sie im Arbeitsalltag nicht verstanden und gelebt werden.*

04

KRITISCHE FUNKTION UND MENSCHLICHE ABHÄNGIGKEIT

Nicht die Person, sondern ihre funktionale Wirkung ist der Anker

Ein Human-Factors-Assessment beginnt bei der Leistung, die erhalten bleiben muss. Erst danach folgen Rollen, Zugänge, Wissen und Rückfallebenen.

01	02	03	04	05	06
Funktion	**Rolle**	**Zugang**	**Wissen**	**Fallback**	**Wirkung**

ANALYSEEBENE	LEITFRAGE UND ERGEBNIS
Funktion	Welche Leistung muss unter welchen Mindestbedingungen erhalten bleiben? Ergebnis: priorisierte kritische Funktion.
Rolle	Welche menschlichen Rollen sind für Betrieb, Freigabe, Diagnose oder Recovery erforderlich? Ergebnis: Rollen- und Verantwortungsmodell.
Zugang	Welche physischen, digitalen oder informationellen Rechte sind damit verbunden? Ergebnis: Expositions- und Berechtigungsbild.
Wissen	Wo liegt kritisches Erfahrungswissen, und wie redundant ist es vorhanden? Ergebnis: Key-Person-Abhängigkeiten.
Fallback	Wer oder was übernimmt, wenn Person, Team, Kommunikationsweg oder Dienstleister ausfällt? Ergebnis: Vertretungs- und Rückfallebene.
Wirkung	Welche Funktion kann durch Fehlhandlung, Manipulation oder Ausfall beeinträchtigt werden? Ergebnis: funktionsbezogene Impact-Bewertung.

POR-EINORDNUNG

Die Aussage „der Mensch ist die Schwachstelle“ greift zu kurz. Relevanter ist die Architektur hinter der Person: Berechtigungen, fehlende Redundanz, unklare Verfahren, Zeitdruck oder Kontrollen, die eine einzelne Fehlhandlung nicht auffangen.

05

SOCIAL ENGINEERING UND BEEINFLUSSBARKEIT

Normales Verhalten darf keine unkontrollierte Wirkung erzeugen

Für Betreiber folgt daraus kein Misstrauensmodell, sondern robuste, kanalübergreifende Verifikation und begrenzte funktionale Reichweite.

FAKTOR	MÖGLICHE SYSTEMWIRKUNG UND SCHUTZPRINZIP
Vertrauen und Hilfsbereitschaft	Eine plausible Bitte ersetzt die formale Prüfung. Schutzprinzip: Identität und Berechtigung unabhängig verifizieren, sichere Rückfragewege vorgeben.
Autorität und Hierarchie	Rang oder vermeintliche Zuständigkeit verkürzt die Prüfung. Schutzprinzip: kritische Freigaben rollenbasiert statt personenbezogen, Vier-Augen-Prinzip wo angemessen.
Zeitdruck und Dringlichkeit	Sicherheitsroutinen werden als Hindernis erlebt. Schutzprinzip: Der Verifikationsweg muss auch unter Zeitdruck schnell und praktikabel sein.
Angst und Unsicherheit	Eine unklare Lage begünstigt vorschnelles Befolgen vermeintlicher Hilfe. Schutzprinzip: klare Eskalationswege und bekannte Ansprechpartner.
Routine und Gewöhnung	Wiederkehrende Ausnahmen senken Aufmerksamkeit und verschieben die Baseline. Schutzprinzip: Ausnahmen erfassen, begrenzen und regelmäßig reviewen.
Kontextwissen	Glaubwürdige Details lassen eine unberechtigte Anfrage plausibel erscheinen. Schutzprinzip: nicht Plausibilität, sondern verifizierte Identität, Zuständigkeit und Zweck entscheiden lassen.

METHODISCHE FOLGERUNG

Awareness ist notwendig, aber nicht hinreichend. Vertrauen ist für den Betrieb unverzichtbar; unverifiziertes Vertrauen ist Exposition. Plausibilität ersetzt keine Verifikation.

06

POR HUMAN VULNERABILITY STRUCTURE

Gefährdung, Exposition und Vulnerabilität sauber trennen

Erst die Kombination aus kritischer Funktion, Rolle, Exposition, unzureichender Kontrolle und auslösendem Ereignis erzeugt funktionale Wirkung.

01 **Critical Function**	02 **Human Role**	03 **Hazard / Threat**	04 **Exposure**
05 **Vulnerability**	06 **Event**	07 **Control Response**	08 **Functional Impact**

SCHRITT	ZWECK
CRITICAL FUNCTION	Festlegen, welche Leistung erhalten bleiben muss und welche Auswirkung ein Verlust hätte.
HUMAN ROLE	Bestimmen, welche Rollen beobachten, freigeben, verändern, diagnostizieren oder wiederherstellen können.
HAZARD / THREAT	HAZARD: nicht notwendigerweise intentionaler, potenziell schädlicher Zustand oder Einfluss. THREAT: potenziell intentionaler und akteursbezogener Einfluss. Beide werden zunächst ohne Attribution erfasst.
EXPOSURE	Zugang, Berechtigung, Wissen, Vertrauensstellung und Entscheidungsmacht der Rolle bestimmen.
VULNERABILITY	Fehlende Kontrolle, Einzelabhängigkeit, Prozessschwäche oder ungünstige Arbeitsbedingung bestimmen.
EVENT / ACTION	Fehler, Beeinflussung, Ausfall oder Regelabweichung als auslösendes Ereignis betrachten.
CONTROL RESPONSE	Prüfen, ob Verifikation, Rollentrennung, technische Begrenzung, Eskalation oder Recovery die Wirkung unterbrechen.
FUNCTIONAL IMPACT	Einordnen, welche Wirkung auf Verfügbarkeit, Integrität, Vertraulichkeit, Steuerungsfähigkeit oder Recovery verbleibt.

07

STATUSSPRACHE UND CONFIDENCE

Systemrisiko bewerten – keine Person prognostizieren

Status beschreibt den Reifegrad einer Information über eine organisatorische oder funktionale Schwachstelle. Confidence beschreibt die Belastbarkeit dieser Bewertung.

STATUS	BEDEUTUNG UND BEISPIELHAFTE AUSSAGEFORM
SIGNAL	Ein möglicher systemischer Risikofaktor ist sichtbar. „Wiederkehrende Prozessabweichung beobachtet; Kontextprüfung läuft.“
VERIFIED	Die Abweichung oder Abhängigkeit ist nachvollziehbar bestätigt. „Kritischer Prozess hängt tatsächlich von einer Einzelrolle ab.“
ASSESSED	Die Bedeutung für eine kritische Funktion wurde eingeordnet. „Einzelberechtigung und fehlende Zweitprüfung erzeugen relevante Exposition.“
DECISION RELEVANT	Die Exposition verlangt eine betriebliche oder organisatorische Entscheidung. „Rollen- und Freigabemodell anpassen.“

CONFIDENCE	ARBEITSDEFINITION
NIEDRIG	Einzelbeobachtung oder indirekte Hinweise; Kontext und Alternativerklärungen weitgehend offen.
MITTEL	Mehrere konsistente Hinweise; Systemzusammenhang plausibel, aber nicht vollständig verifiziert.
HOCH	Mehrere unabhängige Befunde und klare Funktionsbeziehung; wesentliche Alternativerklärungen geprüft.

GOVERNANCE

Confidence bezieht sich auf die Belastbarkeit einer Risikoeinschätzung des Systems. Sie ist kein Prozentwert für die Wahrscheinlichkeit, dass eine bestimmte Person absichtlich schädlich handelt.

08

FRÜHERKENNUNG UND INDIKATOREN

Frühwarnung beginnt vor dem Ereignis

Früherkennung sucht nicht nach „verdächtigen Menschen“, sondern nach Bedingungen, Abweichungen und Abhängigkeiten, die eine kritische Funktion verletzlich machen.

INDIKATORGRUPPE	SYSTEMSIGNALE · BEWERTUNGSPRINZIP
Arbeitslast und Besetzung	Überstunden, Rufbereitschaftslücken, parallele Aufgaben, anhaltende Unterbesetzung. Prinzip: prüfen, ob sichere Handlung unter realer Last möglich bleibt.
Prozessabweichung	Wiederkehrende Workarounds, informelle Freigaben, dauerhafte Ausnahmen. Prinzip: Häufigkeit, Ursache und Wirkung gegen den Soll-Prozess prüfen.
Zugang und Berechtigung	Überbreite Rollen, veraltete Rechte, fehlende Trennung kritischer Freigaben. Prinzip: Notwendigkeit, Reichweite und Gültigkeit gegen die Aufgabe prüfen.
Wissenskonzentration	Einzelne Personen als alleinige Diagnose-, Freigabe- oder Recovery-Instanz. Prinzip: Vertretbarkeit, Dokumentation und Wiederanlauffähigkeit testen.
Verification Discipline	Nicht bestätigte kritische Anweisungen, informelle Identitätsprüfung, Ausnahmen von Zweitprüfung. Prinzip: Verifikationsqualität und Häufung gegen die Baseline prüfen.
Kommunikation und Eskalation	Meldungen ohne Rückmeldung, unklare Zuständigkeit, widersprüchliche Eskalationswege. Prinzip: prüfen, ob ein Signal unter Zeitdruck die richtige Ebene erreicht.
External Manipulation Pressure	Identitätsvortäuschungen, ungewöhnliche Informationsanfragen oder gehäufte Social-Engineering-Kontakte. Prinzip: Druck auf Rolle und Funktion bewerten; keine Personenanfälligkeit ableiten.
Lernen und Near Misses	Wiederkehrende ähnliche Fehler, nicht geschlossene Maßnahmen, geringe Meldedichte trotz bekannter Probleme. Prinzip: Review-Qualität und Maßnahmenabschluss bewerten.

ROMEIKES FRÜHAUFKLÄRUNGSLOGIK

Romeike unterscheidet Frühwarnung, Früherkennung und Frühaufklärung und warnt davor, komplexe Kausalitäten aus einzelnen statischen Indikatoren abzuleiten. Leading Indicators gewinnen ihre Aussage erst durch Baseline, Kontext, Verifikation und Korrelation.

09

HUMAN VULNERABILITY EARLY WARNING

Frühwarnung erkennt steigende Systemverwundbarkeit

Beobachtet wird, ob sich Exposition, Arbeitsbedingungen, Berechtigungen, Prozessdrift und Kontrollqualität einer kritischen Funktion verändern.

01	02	03	04
Baseline	**Indicators**	**Signal Fusion**	**Verify**
05	06	07	08
Function	**Confidence**	**Status**	**Response**

LAYER	ZWECK
BASELINE	Normalzustand der kritischen Funktion, Rollen, Berechtigungen, Verifikation, Besetzung und Rückfallebenen beschreiben.
INDICATORS	Leading Indicators aus Access, Workload, Process Deviation, Verification, Dependency, Communication, External Pressure und Learning erfassen.
SIGNAL FUSION	Mehrere unabhängige Veränderungen zusammenführen; Einzelindikatoren nicht zu Personen- oder Motivannahmen überdehnen.
VERIFY	Datenqualität, Betriebszustand, geplante Änderungen und alternative Erklärungen prüfen.
FUNCTION	Bewerten, welche kritische Funktion durch die veränderte Exposition betroffen sein könnte.
CONFIDENCE	Belastbarkeit der Systembewertung als niedrig, mittel oder hoch ausweisen.
STATUS	SIGNAL, VERIFIED, ASSESSED und DECISION RELEVANT als Informationsreife führen.
RESPONSE	Prozess, Rechte, Besetzung, Training oder Kontrolle anpassen; bei ungeklärter Kontrollwirksamkeit gezielte Validation prüfen.

10

HUMAN VULNERABILITY VALIDATION INDICATOR

HVVI: Wann reicht Monitoring nicht mehr aus?

Der HVVI ist ein von POINT OF RESOLUTION entwickeltes heuristisches Triageinstrument, kein Risiko- oder Personenscore. Gewichtung und Schwellenwerte sind derzeit nicht empirisch validiert; sie dienen der strukturierten Priorisierung und müssen in der Anwendung fortlaufend kalibriert werden. Bewertet wird ausschließlich eine kritische Funktion.

DIMENSION	SKALENANKER
F · Functional Criticality	0 Punkte: keine kritische Funktion, Auswirkung lokal und reversibel. 4 Punkte: Ausfall oder Fehlhandlung kann eine kritische Funktion erheblich beeinträchtigen.
E · Human Exposure	0 Punkte: menschliche Wirkung stark begrenzt. 4 Punkte: wenige Rollen besitzen weitreichenden Zugriff oder Entscheidungsmacht.
C · Control Uncertainty	0 Punkte: Kontrollen aktuell, unabhängig und validiert. 4 Punkte: Kontrollen nur angenommen, ungeprüft oder dauerhaft umgangen.
S · Signal Accumulation	0 Punkte: keine relevanten oder klar erklärte Einzelabweichungen. 4 Punkte: mehrere unabhängige, verifizierte und wiederkehrende Signale mit Funktionsbezug.
D · Change & Drift	0 Punkte: stabile Baseline ohne wesentliche Änderungen. 4 Punkte: Baseline durch Änderungen, Ausnahmen oder Prozessdrift nicht mehr belastbar.

PUNKTWERT	TRIAGE-STATUS
0 – 5	BASELINE · Monitoring und reguläres Review ausreichend.
6 – 9	OBSERVE · Prozess- und Berechtigungsreview, Tabletop oder gezielte Kontrollprüfung.
10 – 13	VALIDATION CANDIDATE · externe oder unabhängige realitätsnahe Validierung fachlich prüfen.
14 – 17	STRONG INDICATION · Human-Risk-Pentest angezeigt, sofern Decision Gate und Safety erfüllt sind.
18 – 20	INTEGRATED VALIDATION · mehrdimensionale Validierung erwägen; keine automatische Eskalation.

KEIN AUTOMATISMUS

Kein HVVI-Wert löst automatisch einen Pentest aus. Ein Test ist nur sinnvoll, wenn eine konkrete Annahme über eine Kontrolle offen ist. Bekannte Lücken werden zuerst behoben – nicht nochmals bewiesen.

11

VALIDATION DECISION GATE

Wann ein Human-Risk-Pentest sinnvoll wird

Der HVVI markiert möglichen Validierungsbedarf. Vor einem Auftrag wird geprüft, welche Kontrollannahme offen ist, ob ein Test Erkenntniswert liefert und welche Testform die Frage mit vertretbarem Risiko beantwortet.

GATE	LEITFRAGE UND ERGEBNIS
1 · Information Value	Welche konkrete Kontrollannahme soll validiert werden? Ohne prüfbare Hypothese kein Pentest.
2 · Remediation Value	Ist die Schwachstelle bereits eindeutig bekannt? Bekannte Lücke zuerst beheben, danach gezielter Retest.
3 · Safety	Kann die Simulation ohne Gefährdung von Betrieb, Arbeitssicherheit oder Versorgung durchgeführt werden? No-go-Zonen, Stop Rules, Zeitfenster und Notfallkontakt festlegen.
4 · Legal & Governance	Sind Auftrag, Datenschutz, Arbeitsrecht, Mitbestimmung, Berechtigung und Eskalation geklärt? Dokumentiertes Pre-Engagement vor Testbeginn.
5 · Test Design	Welcher Kanal trägt die relevante Kontrollannahme? Vishing bei Telefon, Remote bei E-Mail und Identität, Physical bei Zutritt, Combined bei cyber-physischer Folgewirkung.
6 · Success Criteria	Welche Kontrolle muss unter realistischen Bedingungen funktionieren? Nicht „wer fällt herein?“, sondern Verifikation, Eskalation, Begrenzung, Detektion und Recovery messen.

HRC ALS PRAXISREFERENZ

HRC dient hier als fachliche Praxisreferenz für spezialisierte Human-Risk-Validation. Eine operative Einbindung oder Kooperation ist damit nicht verbunden; sie würde gesonderte Abstimmung und Beauftragung voraussetzen.

VALIDATION OUTPUT

Der relevante Befund lautet nicht „Mitarbeiter X hat versagt“, sondern: Welche Kontrolle wurde unter welcher Bedingung umgangen oder bestätigt? Welche funktionale Wirkung wäre möglich gewesen? Wurde das Signal erkannt und eskaliert?

12

INSIDER RISK UND LEGITIMER ZUGANG

Vertrauen ist notwendig – unkontrollierte Reichweite nicht

Insider Risk beginnt dort, wo aktueller oder früherer legitimer Zugang, internes Wissen oder institutionelles Vertrauen besondere Wirkung ermöglicht. Nicht jedes Insider-Risiko ist vorsätzlich.

RISIKOFORM	BEDEUTUNG UND KONTROLLE
Unbeabsichtigt	Fehler ohne schädliche Absicht. Kontrolle: fehlertolerante Prozesse, klare Bedienlogik, sichere Defaults, Training und Recovery.
Fahrlässig	Vorgaben werden aus Bequemlichkeit, Routine oder Zeitdruck nicht eingehalten. Kontrolle: Ursachen prüfen, praktikable Verfahren und Verantwortlichkeit herstellen.
Extern beeinflusst	Legitimer Zugang wird durch Täuschung für eine unzulässige Handlung genutzt. Kontrolle: unabhängige Identitäts- und Auftragsverifikation, begrenzte Berechtigungen.
Vorsätzlich	Autorisierter Zugang wird bewusst gegen Interessen der Organisation eingesetzt. Kontrolle: Need-to-Know, Berechtigungstrennung, Protokollierung; personenbezogene Maßnahmen nur legitimiert.
Dritte und Dienstleister	Externe Rollen erhalten zeitweise Zugang zu Systemen, Orten oder Informationen. Kontrolle: begrenzte Rechte, Zeitfenster, Offboarding und Review.
Ehemaliger Zugang	Berechtigungen, Wissen oder Tokens bleiben nach Rollenwechsel wirksam. Kontrolle: Joiner-Mover-Leaver-Prozess, zeitnahe Entziehung, Berechtigungsinventar.

POR DATA-MINIMISATION-PRINZIP

Das Ziel ist nicht maximale Mitarbeiterüberwachung. Das Ziel ist die minimale, belastbare Kontrolle derjenigen Zugänge, Abhängigkeiten und Entscheidungen, die eine kritische Funktion tatsächlich beeinflussen können.

ABGRENZUNG

POR ersetzt keine arbeitsrechtliche Bewertung, psychologische Begutachtung, interne Ermittlungsstelle oder Strafverfolgung. Das Assessment bleibt auf System-, Prozess- und Funktionsrisiken fokussiert.

13

HUMAN-FACTORS-RESILIENZ

Kontrollen müssen unter realen Bedingungen funktionieren

Wirksame Resilienz reduziert nicht „den Menschen“, sondern die unkontrollierte Wirkung einzelner Entscheidungen.

01 **Understand**	02 **Reduce**	03 **Verify**	04 **Observe**
05 **Validate**	06 **Respond**	07 **Learn**	

PHASE	OPERATIVE KERNFRAGE
UNDERSTAND	Welche kritische Funktion hängt von welchen Rollen, Kenntnissen, Zugängen und Entscheidungen ab?
REDUCE	Welche unnötigen Berechtigungen, Einzelabhängigkeiten oder Prozessausnahmen können strukturell reduziert werden?
VERIFY	Welche sensiblen Handlungen benötigen unabhängige Identitäts-, Auftrags- oder Freigabeprüfung?
OBSERVE	Welche Leading Indicators zeigen zunehmende Exposition, Prozessdrift oder Lernlücken?
VALIDATE	Welche offene Kontrollannahme muss durch Tabletop, Walkthrough, Pentest oder technische Prüfung realitätsnah getestet werden?
RESPOND	Wie wird die kritische Funktion stabilisiert, wenn Rolle, Zugang oder Vertrauenspfad ausfällt oder kompromittiert erscheint?
LEARN	Welche Annahmen, Indikatoren, Berechtigungen und Prozessschritte werden nach Ereignis, Near Miss oder Validation angepasst?

FÜHRUNGSAUFGABE

Mestchian betont, dass Risikomanagement ein organisationsweiter Prozess ist und Unterstützung von oben benötigt. Sicherheitskultur, realistische Ressourcen, klare Verantwortlichkeiten und funktionierende Eskalationswege sind Führungsaufgaben – nicht allein Schulungsthemen.

14

KONSEQUENZEN FÜR BETREIBER

Die belastbare Minimalausstattung

Nicht jeder Betreiber benötigt ein eigenes Insider-Threat-Programm. Jede kritische Funktion benötigt jedoch Rollenklärung, begrenzte Exposition, sichere Verifikation, Redundanz und eine lernfähige Organisation.

01 **Kritische Funktionen und Rollen abbilden.**

Nicht bei Stellenbeschreibungen beginnen, sondern bei der Frage, welche Leistung von welcher menschlichen Handlung oder Entscheidung abhängt.

02 **Berechtigungen und Einzelabhängigkeiten begrenzen.**

Least Privilege, zeitliche Begrenzung, Vertretung und getrennte Freigaben dort einsetzen, wo die mögliche Wirkung dies rechtfertigt.

03 **Verifikation unter Zeitdruck funktionsfähig machen.**

Sichere Rückfragen, Identitätsprüfung und Eskalation müssen auch in Störung, Rufbereitschaft und Krisenlage praktisch nutzbar sein.

04 **Abweichungen sichtbar machen, ohne Schuldlogik.**

Workarounds, Near Misses und wiederkehrende Ausnahmen als Systemsignale behandeln und Ursachen analysieren.

05 **Training mit Prozessdesign verbinden.**

Sensibilisierung schafft Wissen; sichere Prozesse, Technik und Berechtigungen müssen verhindern, dass ein einzelner Fehler unkontrolliert durchschlägt.

06 **Validation und Retest als Lernschleife etablieren.**

Offene Kontrollannahmen risikobasiert validieren, nach Remediation gezielt retesten und die neue Baseline dokumentieren. Pentests nicht nach Kalender, sondern nach Informationsbedarf planen.

SICHERHEITSGRENZE DIESER PUBLIKATION

Diese Einordnung enthält keine Anleitung zur Manipulation von Beschäftigten, keine objektspezifischen Schwachstellen, keine verdeckten Profiling-Methoden und keine Kriterien zur psychologischen Gefährlichkeitsbewertung.

15

POR HUMAN VULNERABILITY ASSESSMENT

System prüfen – Frühwarnung, Validation und Learning verbinden

CAPABILITY	PRIMÄRER BEITRAG UND TYPISCHE OUTPUTS
RISK INTELLIGENCE	Zusammenführung von Rollen, Berechtigungen, Prozessrealität, Abhängigkeiten, Signalen und Funktionswirkung. Outputs: Human-Dependency-Map, Expositionsbild, verifizierte Systemsignale, Confidence, Entscheidungsbedarf.
DIRECT ACTION	Preparedness, Eskalationslogik, Tabletop, Stabilisierung und Recovery bei gestörter oder kompromittierter Rollenstruktur. Outputs: Rollen- und Entscheidungslogik, Übungsbefund, Maßnahmenpriorisierung, After Action Review.
DARK DALOS	Technische oder physische Verifikation dort, wo ein menschlich gemeldeter Befund objektiviert werden muss – nicht zur Personenüberwachung. Outputs: Zustandsdokumentation, zeitlicher Verlauf, Bestätigung oder Widerlegung eines Signals.

01	02	03	04
Signal	**Verified**	**Assessed**	**Decision Relevant**

OPERATIVER GRUNDSATZ

No person scoring. Keine automatisierte Loyalitäts-, Motiv- oder Gefährlichkeitsbewertung. POR bewertet Exposition, Prozess, Evidenz und funktionale Wirkung.

DOMAINS

Das Modell ist sektorübergreifend, aber nie generisch fertig. Für jede Domain werden kritische Funktionen, Rollen, Berechtigungen, Normalbetrieb, Leading Indicators und Rückfallebenen neu erhoben.

16

SCHLUSSFOLGERUNG

Menschliche Verwundbarkeit wird systematisch bewertbar, wenn wir das System beobachten

Menschliches Verhalten ist weder vollständig vorhersehbar noch durch Schulung allein kontrollierbar. Frühwarnung entsteht dort, wo Leading Indicators eine Veränderung von Exposition und Kontrollqualität sichtbar machen.

METHODISCHER KERN

Human Vulnerability entsteht aus dem Zusammenspiel von kritischer Funktion, menschlicher Rolle, Exposition, systemischer Vulnerabilität und auslösendem Ereignis. Wirksame Kontrollen begrenzen die funktionale Wirkung. Frühwarnung beobachtet Veränderungen dieser Faktoren; der HVVI priorisiert den Validierungsbedarf; das Decision Gate entscheidet über Tabletop, Walkthrough oder autorisierten Pentest.

POR-FAZIT

Für Betreiber kritischer Infrastruktur lautet die entscheidende Frage nicht, welcher Mensch „schwach“ ist. Entscheidend ist, ob eine kritische Funktion zunehmender menschlich-organisatorischer Exposition ausgesetzt ist, ob schwache Signale diese Veränderung früh anzeigen und ob vorhandene Kontrollen ihre Wirkung unter realistischen Bedingungen nachweislich begrenzen. Erst wenn diese Wirksamkeit ungeklärt und der Erkenntniswert hoch genug ist, wird ein Human-Risk-Pentest zur fachlich begründeten Validierungsmaßnahme.

Verwendete Quellen

QUELLEN UND DOKUMENTENBASIS

01 Bundesamt für Sicherheit in der Informationstechnik (BSI): Social Engineering - der Mensch als Schwachstelle; IT-Grundschutz-Kompendium, G 0.42 sowie ORP.2 / ORP.3. bsi.bund.de; Abruf 20.09.2026.

02 Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA): Human Factors / Ergonomie - sozio-technische Arbeitssysteme, kognitive und organisationale Ergonomie. baua.de; Abruf 20.09.2026.

03 European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape 2024; ENISA Threat Landscape 2025. enisa.europa.eu; Abruf 20.09.2026.

04 Cybersecurity and Infrastructure Security Agency (CISA): Insider Threat Mitigation Guide; Insider Risk Mitigation Program Evaluation (IRMPE). cisa.gov; Abruf 20.09.2026.

05 Frank Romeike: Frühwarnsysteme im Unternehmen - Nicht der Blick in den Rückspiegel ist entscheidend. RATINGaktuell 02/2005, S. 22-27.

06 Peyman Mestchian: Risk intelligence - from compliance to performance. Journal of Risk Intelligence / SAS EMEA, 2005.

07 H. Ebrahimi, F. Sattari, L. Lefsrud, R. Macciotta: Human vulnerability modeling and risk analysis of railway transportation of hazardous materials. Journal of Loss Prevention in the Process Industries 80 (2022), 104882. DOI: 10.1016/j.jlp.2022.104882.

08 Proofpoint: Social Engineering; Human-Centric Security. proofpoint.com/de; Abruf 20.09.2026.

09 Human Risk Consulting GmbH (HRC): Pentesting und Awareness; Vishing Pentest; Remote Social Engineering Pentesting; physische Pentests; Human Risk Management. hrc-gmbh.com; Abruf 20.09.2026. Fachliche Praxisreferenz; keine Aussage über Kooperation oder Beauftragung.

PUBLIKATION

POINT OF RESOLUTION · Assessment Paper 02/2026 · Version 1.3 FINAL · Stand 20.09.2026. Herausgeber: Ingo Zimmer, POINT OF RESOLUTION, Leipzig. Diese Publikation dient der fachlichen Einordnung und Methodikentwicklung. Sie ersetzt weder Rechtsberatung, arbeitsrechtliche Einzelfallbewertung, psychologische Begutachtung, interne Ermittlungen noch behördliche Lagebilder. Pentests setzen ausdrückliche Autorisierung, definierten Scope sowie Safety-, Datenschutz- und Governance-Regeln voraus.