PERA Pre-Employment Risk Assessment

Präventive Analyse von Personalrisiken bei kritischen Positionen

Das Pre-Employment Risk Assessment (PERA) ist die einzige präventive Risikoanalyse für Schlüsselpositionen, die personaldiagnostische, psychologische und digitale Risikofaktoren kombiniert – und diese in eine klare, managementtaugliche Entscheidungsgrundlage übersetzt.

LEISTUNGSUMFANG

Im Rahmen des Assessments werden relevante Risikodimensionen systematisch analysiert und eingeordnet:

Digitale Risikospuren
Analyse öffentlich zugänglicher digitaler Informationen im Hinblick auf sicherheitsrelevante Auffälligkeiten

Biographische und strukturelle Faktoren
Bewertung von Werdegang, Kontext und möglichen Risikokonstellationen

Interessenkonflikte und Abhängigkeiten
Identifikation potenzieller Einflussfaktoren, die Integrität oder Unabhängigkeit beeinträchtigen könnten

Risikobewertung und Einordnung
Strukturierte Einschätzung identifizierter Faktoren nach Relevanz und Kritikalität

Ergebnis

Das Ergebnis wird in einem kompakten, managementgerechten Bericht zusammengefasst und umfasst:

- eine klare, nachvollziehbare Risikoeinordnung
- eine kontextbezogene Bewertung der identifizierten Faktoren
- eine sachliche Entscheidungsgrundlage für Geschäftsführung, CISO oder Sicherheitsverantwortliche
- Optional erfolgt eine persönliche Ergebnisbesprechung

Methodik & Rahmen

- ausschließlich Nutzung rechtlich zulässiger und öffentlich zugänglicher Informationen
- keine Observationen oder verdeckten Maßnahmen
- diskrete, strukturierte und nachvollziehbare Vorgehensweise
- klare Trennung zwischen Analyse (unsere Leistung) und Entscheidung (Kunde)

Zielsetzung

Reduzierung von Fehlentscheidungsrisiken bei der Besetzung kritischer Positionen durch eine unabhängige, präventive und fachlich fundierte Bewertung potenzieller Risikofaktoren.

IHRE VORTEILE

01

Minimierung existenzieller Risiken in KRITIS-Positionen

Fehlbesetzungen in kritischen Funktionen gefährden Betriebssicherheit, Compliance und im Ernstfall die öffentliche Versorgung. Sie erkennen potenzielle Risiken, bevor sie wirksam werden.

02

Schutz vor Reputations- und Haftungsschäden

Unentdeckte Auffälligkeiten können schnell zur persönlichen Belastung für Geschäftsführung und Gremien werden. Sie schaffen belastbare Entscheidungsgrundlagen und reduzieren Ihr eigenes Risiko.

03

Risikotransparenz dort, wo klassische Verfahren versagen

Lebensläufe, Interviews und Referenzen zeigen Stärken – nicht Schwächen. Sie erhalten eine strukturierte Risikoperspektive auf Kandidaten, die sonst verborgen bleibt.

04

Souveräne Entscheidungen unter Unsicherheit

Gerade bei sensiblen Besetzungen fehlt oft die letzte Sicherheit. Sie gewinnen Klarheit, wo vorher nur Annahmen waren – und treffen Entscheidungen mit Rückendeckung.

Für eine weiterführende Einordnung und ein vertrauliches Gespräch stehen wir Ihnen jederzeit gerne zur Verfügung.

Eingesätzte Kräfte / Berater

1. Senior-Consultant „Digitale Forensik“ Drei Grad
2. Senior Consultant „Sicherheits- und Risikoanalyse“ Drei Grad
3. Psychologe Drei Grad

Unsere Berater verfügen über langjährige Erfahrung in der kriminalistischen Analyse und Bewertung komplexer Risikolagen.

DARSTELLUNG DER METHODIK

Warum Sicherheit beim Recruiting beginnt und wie Geschäftsführer die persönliche Haftung vermeiden.

Das Kernproblem & die Gefahren

Faktor Mensch: Teure Firewalls schützen Systeme, aber der Mensch bleibt die größte, oft vernachlässigte Schwachstelle.

Falscher Fokus: Unternehmen prüfen IT-Technik intensiver als die Personen, die diese bedienen.

Insider-Risiko: Zu weit gefasste Zugriffsrechte und fehlende Sicherheitsüberprüfungen schaffen unkontrollierbare Risiken.

Haftungsfalle: Geschäftsführer, Vorstände und Führungskräfte haften persönlich, wenn bekannte menschliche Risiken organisatorisch ignoriert werden.

Der 5-Punkte-Prüfkatalog (Human Risk Analyse)

1. **Identitätskonsistenz:** Aufdecken von Fake-Profilen, Widersprüchen im Werdegang und Aliasnamen
2. **Risiko-Analyse (Daten & Zugänge):** Abgleich mit Datenpannen (Leaks, Zugangsdaten)
3. **Security-Risiken:** Suche nach versehentlich veröffentlichtem Quellcode (z. B. GitHub-Leaks) oder ungesicherten Admin-Zugängen
4. **Reputations- & Compliance-Risiken:** Erkennung von übergriffigem und diskriminierendem Verhalten, Betrugsindikatoren oder Extremismusbezug
5. **Insider-Risiko-Indikatoren:** Identifikation von Datenabfluss, Teilen von Firmengeheimnissen oder gezielter Security-Umgehung

Methodik, Ethik & Rechtssicherheit

- **Erlaubte Methoden:** Rein analytischer Prozess mittels OSINT (Open Source Intelligence), Exposure-Analyse und technischer Metadatenanalyse
- **Strikte Tabus:** Keine verdeckten Maßnahmen, keine Account-Übernahmen, kein Social Engineering (Phishing) und keine Täuschung
- **Rechtlicher Rahmen:** Volle Compliance nach DSGVO (Art. 6) und BDSG (§ 26). Keine Diskriminierung, keine politischen/religiösen Profile. Es findet kein automatisiertes Profiling statt
- **Datenschutz:** Jede Prüfung erfolgt mit klarer Zweckbindung, Einwilligung/berechtigtem Interesse sowie nach dem Need-to-know-Prinzip, Einhaltung einer strengen Löschrichtlinie nach Besetzung (spätestens nach 6 Monaten)

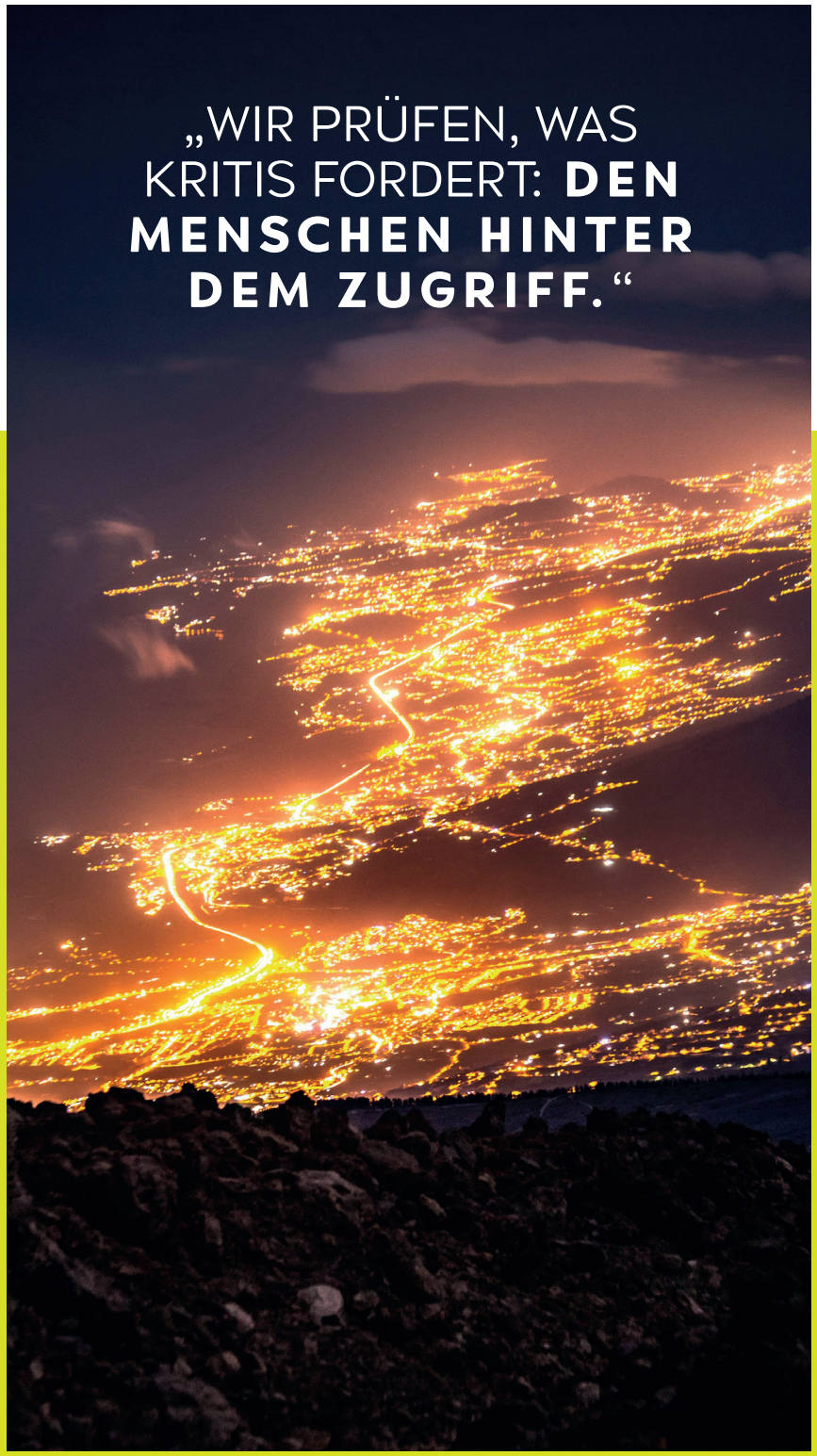

Foto: Marek Piwnicki auf Unsplash

Das Ergebnis: Der Human Risk Report

Objektive Bewertung: Strukturierte Aufbereitung aller Indikatoren aus den fünf Kernbereichen.

Handlungsempfehlungen: Fundierte Entscheidungshilfe für das Onboarding oder die Rechtevergabe.

Revisionssicherheit: Lückenlose Dokumentation als rechtlicher Nachweis für die Erfüllung der organisatorischen Sorgfaltspflicht.

3° | DREI GRAD

Drei Grad GmbH

Freiheitstraße 124, 15745 Wildau
Telefon: +49 (0)3375-246 84 08
info@drei-grad.de, www.drei-grad.de