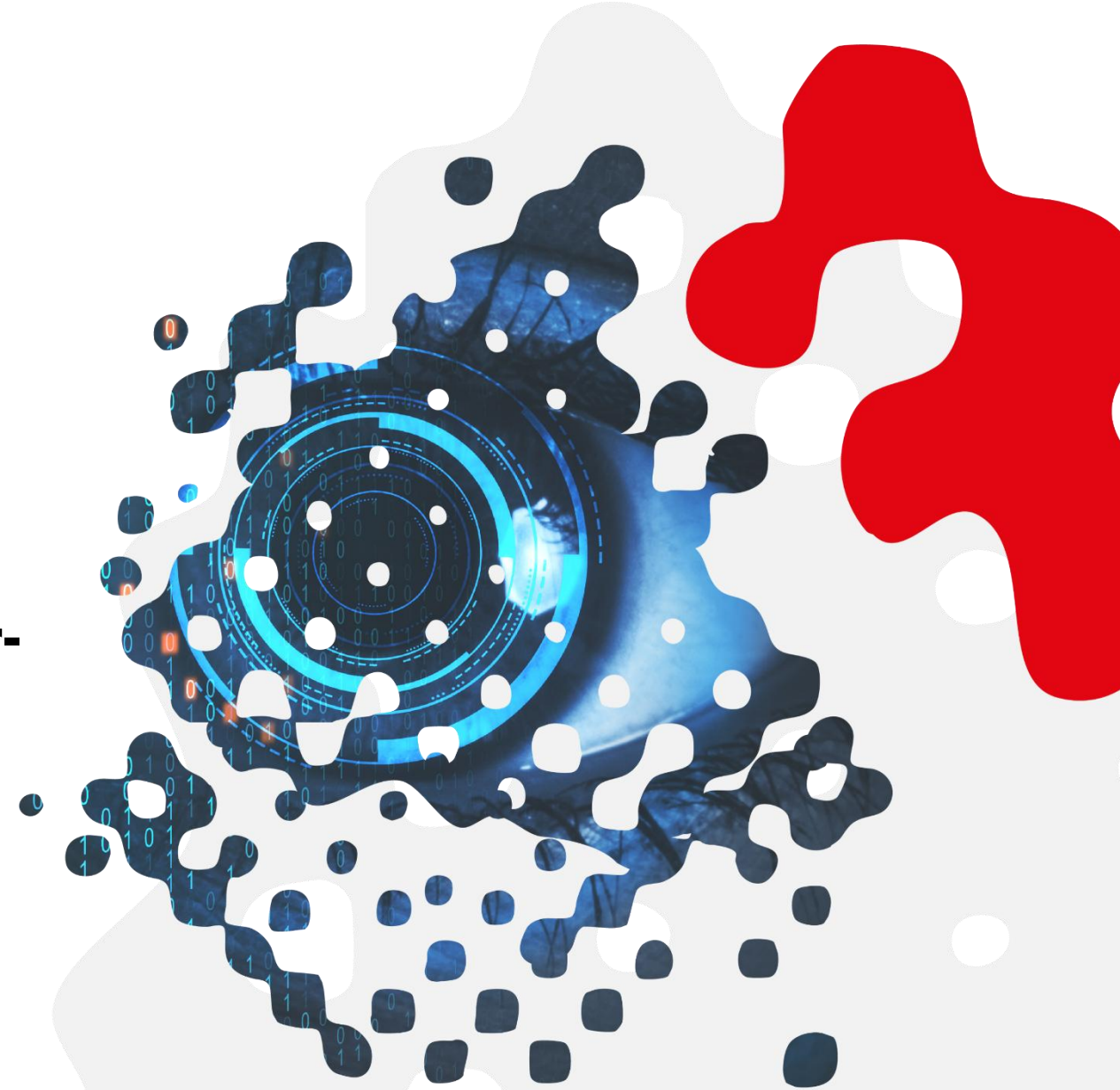
NetEye Conference DACH 2026

Die Sicht der Angreifer verstehen: Wie Threat Intelligence, Exposure Monitoring und Analystenwissen Cyber-Risiken reduzieren

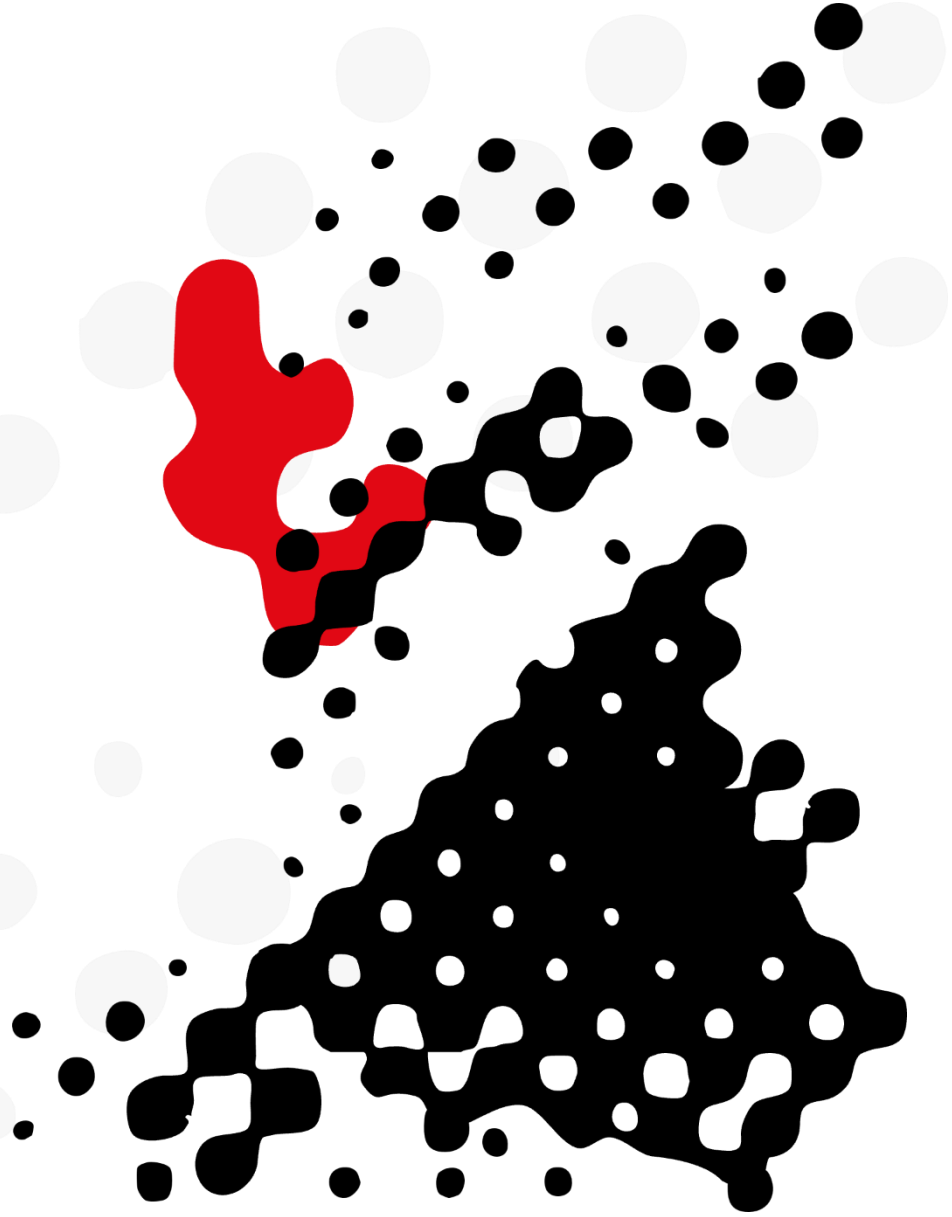
Günter Aigle
Dipl. Ing. Tech. Inf. / CISSP



(mit Hilfe von KI erstellt)

Agenda

- Bedrohungslage
- Threat Intelligence
- Exposure Monitoring
- Die Rolle der Analysten
- KI
- Use Cases / Beispiele
- Empfehlungen und Erfolgsfaktoren



Bedrohunglage 2026



Bedrohunglage 2026 – aktuelle Motivation

Motivation	Anteil / Bedeutung	Ziel der Angreifer	Typische Methoden
Finanzielle Gewinne	Sehr hoch	Geld verdienen	Ransomware, Betrug, BEC, Datendiebstahl
Wirtschaftsspionage	Hoch	Know-how stehlen	APTs, Supply-Chain-Angriffe
Politische / geopolitische Ziele	Hoch	Einflussnahme, Destabilisierung	DDoS, Sabotage, Informationsoperationen
Hacktivismus	Hoch	Aufmerksamkeit erzeugen	DDoS, Website-Manipulationen, Leaks
Technische Neugier / Reputation	Mittel	Anerkennung in der Szene	Exploit-Entwicklung, Schwachstellenforschung
Sabotage	Mittel	Betriebsunterbrechungen	OT-/ICS-Angriffe, Datenlöschung
Aufbau von Botnetzen	Mittel	Ressourcen kontrollieren	Malware, IoT-Kompromittierung

Ganz neu – sehr Gefährlich:
KI - Agenten



Threat Intelligence

Warum Angreifer erfolgreicher werden

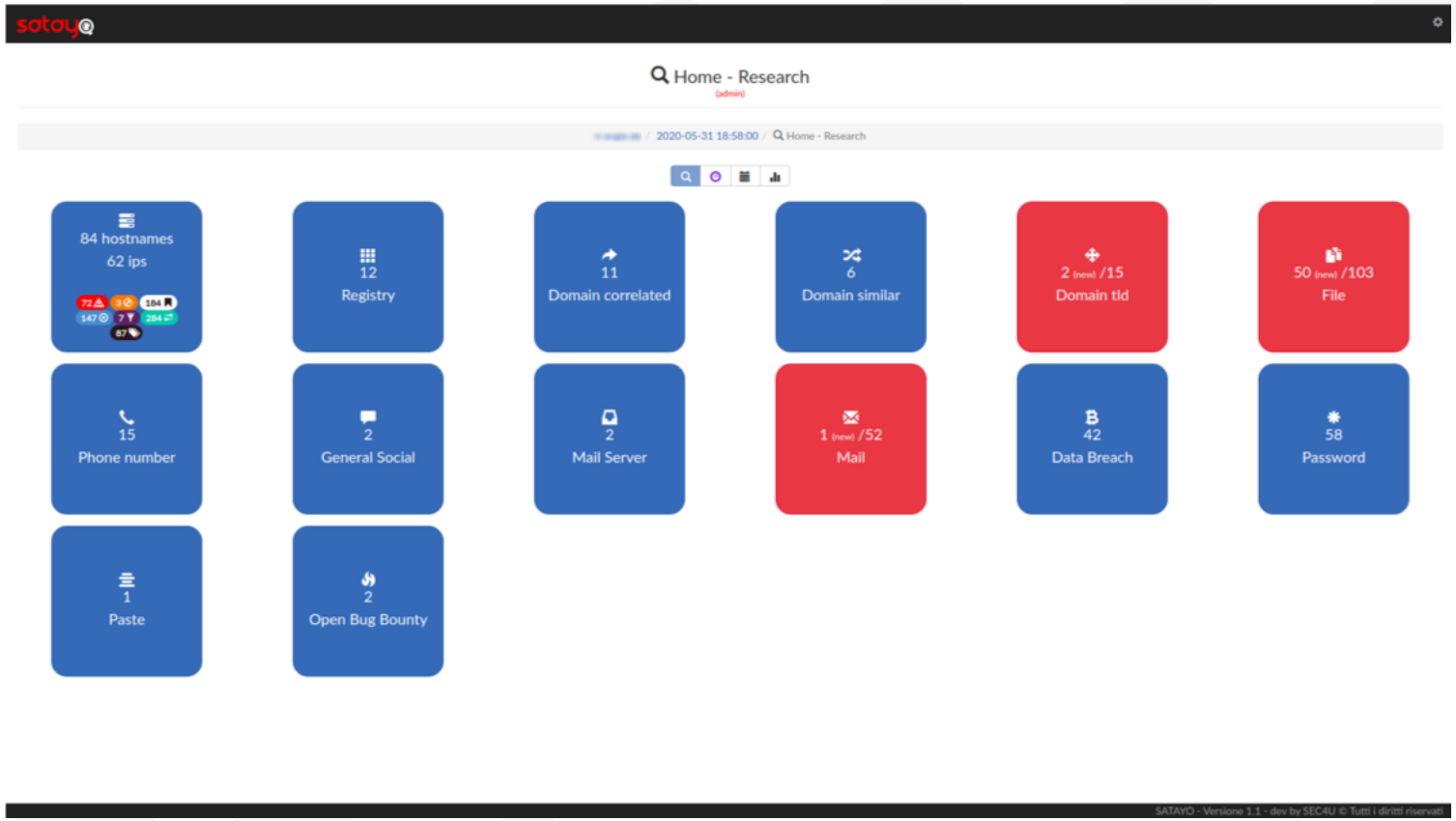
Threat Intelligence (Bedrohungsaufklärung) ist die systematische Sammlung, Analyse und Bewertung von Informationen über aktuelle und potenzielle Cyberbedrohungen.

- Professionalisierung von Cybercrime
- Crime-as-a-Service
- Automatisierung der Angriffe durch KI
- Schnellere Anpassung der Angriffe (KI)
- Ransomware dominant
- Phishing wird durch Einsatz von „deep fake“ zum Problem
- Vereinfachung der Angriffe (durch KI)
- Kürzere Reaktionszeiten -> *„Schnelligkeit ist Trumpf“*

Cyberkriminelle beherrschen das „footprinting“

Quellen für Threat Intelligence

- Open Source Intelligence (OSINT)Darknet-Foren und Underground-Märkte
- CERTs und Sicherheitswarnungen
- Malware-Analysen
- Partnernetzwerke
- Sicherheitsvorfälle anderer Unternehmen



NetEye Conference DACH 2026

Wer sind die Gegner?

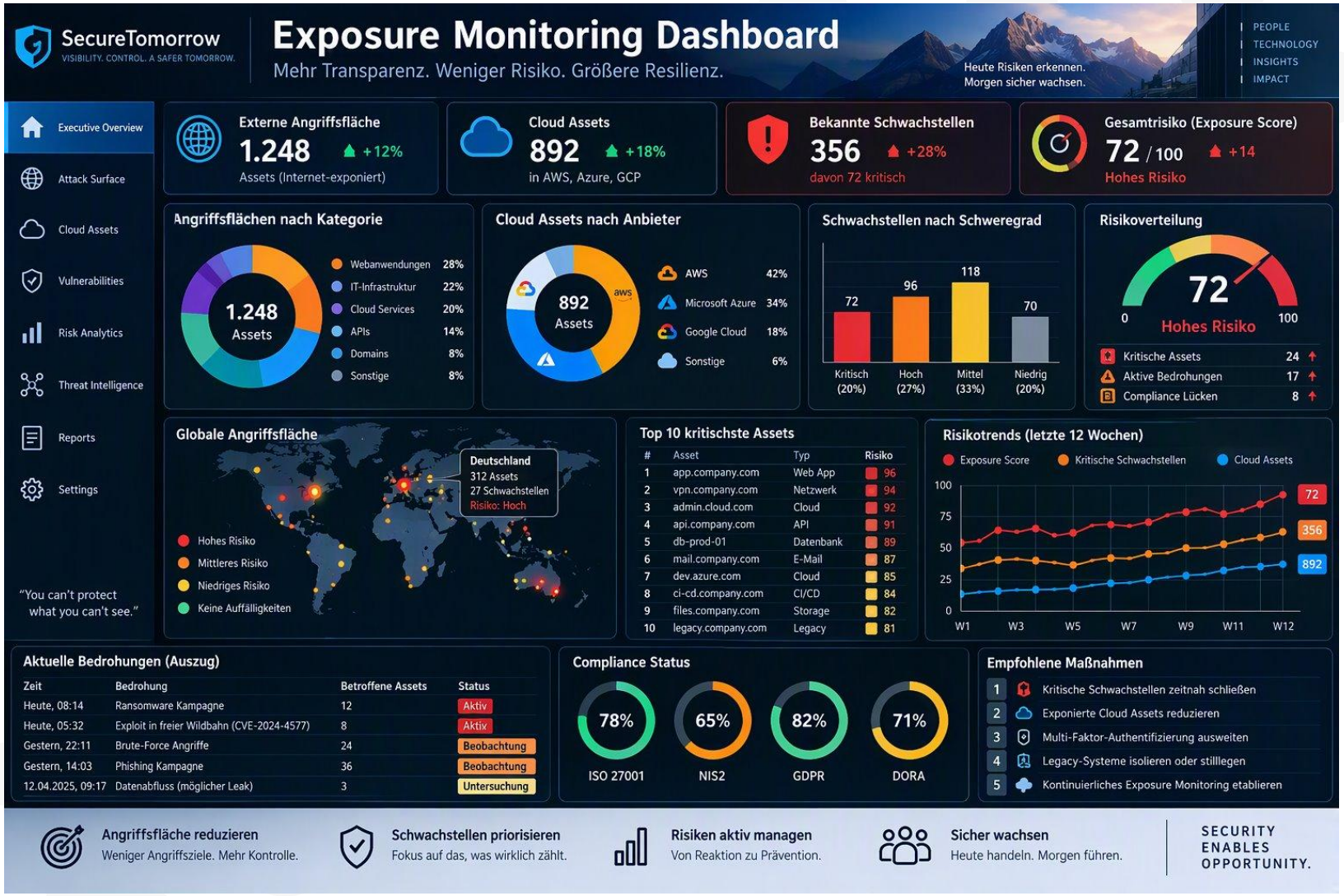
Gruppe	Typ	Hauptangriffsweg	Besondere Merkmale	Typische Ziele	Risikoniveau
LockBit	Ransomware-as-a-Service (RaaS)	Schwachstellen, gestohlene Zugangsdaten, Phishing	Ehemals größte Ransomware-Organisation weltweit, hochgradig professionalisiert, großes Affiliate-Netzwerk [swisscyber...titute.com]	Industrie, Behörden, Gesundheitswesen, Unternehmen aller Größen	Sehr hoch
Cl0p	Datendiebstahl & Ransomware	Ausnutzung von Zero-Day-Schwachstellen in Unternehmenssoftware	Spezialisiert auf Massenangriffe über Lieferketten und File-Transfer-Systeme wie MOVEit & ähnliche Produkte [swisscyber...titute.com], [ransomwarewire.com]	Großunternehmen, Konzerne, Dienstleister	Sehr hoch
Akira	Ransomware	VPN-Zugänge, Schwachstellen, kompromittierte Accounts	Häufige Angriffe auf mittelständische Unternehmen, Fokus auf doppelte Erpressung (Verschlüsselung + Datenveröffentlichung) [deepstrike.io], [dexpose.io]	Mittelstand, Bildung, Fertigung	Hoch
RansomHub	Ransomware-as-a-Service	Phishing, Initial Access Broker, Schwachstellen	Nach dem Rückgang von LockBit stark gewachsen, eines der größten Affiliate-Netzwerke der letzten Jahre [ransomwarewire.com], [deepstrike.io]	Kritische Infrastruktur, Gesundheitswesen, Finanzsektor	Sehr hoch
Play (PlayCrypt)	Ransomware	Schwachstellen, VPNs, kompromittierte Konten	Schnelle Ausbreitung im Netzwerk nach Erstzugriff, professionelle Erpressungskampagnen [dexpose.io]	Mittelstand, Behörden, kritische Infrastrukturen	Hoch

Cybercrime
ist heute eine hoch-organisierte, nach industriellem Beispiel durchorganisierte, höchst effektive Form von Kriminalität!

Exposure Monitoring

- Externe Angriffsfläche erkennen
- Shadow IT identifizieren
- Fehlkonfigurationen aufdecken
- Kontinuierliche Transparenz
- Auch Menschen sind Assets (was macht Ihre Belegschaft so auf Linkedin und Co.? ☺)

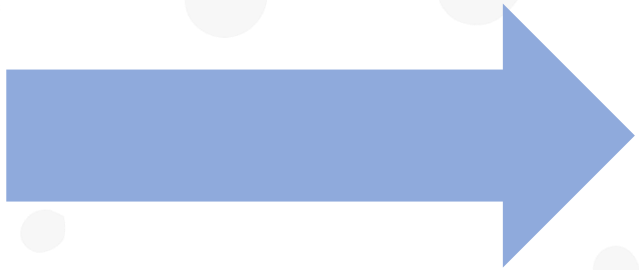
„Sie sollten darüber informiert sein, was in Ihrem Laden so läuft“ ☺



NetEye Conference DACH 2026

Angriffssicht statt Innensicht

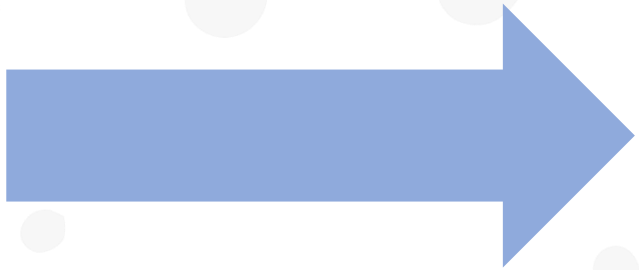
- Was sieht der Angreifer?
- Internet-exponierte Systeme
- Offene Dienste und Schwachstellen
- Ungeschützte Cloud-Ressourcen



- Threat Analyse
- OSINT
- Schwachstellen-Scanner
- Pentests
- Darknet Monitoring

Die Rolle der Analysten

- Korrelation von Informationen
- Priorisierung von Risiken
- Bewertung der Bedrohungsrelevanz
- Ableitung konkreter Maßnahmen



- Prozesse zur weiteren Verarbeitung der Informationen
- Alarmierung
- 24/7 Bereitschaft
- Einleitung und Umsetzung von Maßnahmen

  (Idealerweise 27/7/365 im Minutenbereich)

KI

Warum KI ein Gamechanger ist

- **Angriffe werden schneller, günstiger und skalierbarer**
- **Personalisierte Täuschungen in Sekunden**
- **Sprach-, Bild- und Video-Fälschungen wirken glaubwürdig**
- **Automatisierte Auswertung gestohlener Daten**

Aktuelle Angriffsformen

- KI-generierte Phishing-Mails
- CEO-Fraud mit **synthetischen** Stimmen
- Gefälschte Bewerberprofile und Identitäten
- Automatisierte Social-Engineering-Kampagnen

Deutsche Rentenversicherung

Online-Services › Erstattungsmitteilung

Ihr Erstattungsbetrag (§ 26 Abs. 2 SGB IV)
Abrechnungszeitraum 2024–2026

€ 347,60

Zahlungsfrist: 20.09.2026

Bitte schließen Sie die Kontoaktualisierung bis zu diesem Datum ab, damit die Erstattung fristgerecht bearbeitet werden kann.

Beitragsrückerstattung – Bankverbindung nicht erreichbar

Im Rahmen der Beitragsprüfung für den Zeitraum **2024–2026** wurde festgestellt, dass Ihnen zu Unrecht ein erhöhter Beitragssatz berechnet wurde. Der daraus resultierende Erstattungsanspruch in Höhe von **€ 347,60** wurde gemäß **§ 26 Abs. 2 SGB IV** für die Rücküberweisung freigegeben.

⚠ **Überweisung fehlgeschlagen:** Der Versuch, den Betrag auf die bei uns hinterlegte Bankverbindung zu überweisen, ist gescheitert. Das Konto konnte nicht erreicht werden oder ist nicht mehr aktiv. Bitte geben Sie eine gültige Zahlungskarte an, damit wir die Erstattung auf diesem Weg auszahlen können.

So funktioniert die Auszahlung über Ihre Zahlungskarte:

1. Geben Sie Ihre Debit- oder Kreditkarte an. Zur Echtheitsprüfung wird eine temporäre Autorisierung von **0,01 €** vorgenommen, die umgehend storniert wird.
2. Ihre Bank bestätigt die Karteninhaberin bzw. den Karteninhaber im Rahmen des 3D-Secure-Verfahrens.
3. Der Erstattungsbetrag von **€ 347,60** wird innerhalb von **3–5 Werktagen** auf Ihrem Kartenkonto gutgeschrieben.

Zahlungskarte hinterlegen →

Rechtsgrundlage: § 26 Abs. 2 SGB IV · Aktenzeichen: DRV-2026-336451 · Systembenachrichtigung der Deutschen Rentenversicherung Bund, 10704 Berlin

drv.bit2000.com.br/login/#

Gebärdensprache Leichte Sprache **Mein Kundenportal**

Deutsche Rentenversicherung

Prävention Reha Rente Versicherung Über uns

Online-Services · Erstattungsportal

Sichere Anmeldung mit Ihrer Rentenversicherungsnummer

Deutsche Rentenversicherung › Online-Services › Erstattungsportal

Anmelden

Bitte geben Sie Ihre Rentenversicherungsnummer ein, um auf Ihre persönliche Erstattungsakte zuzugreifen.

Rentenversicherungsnummer (RV-Nr.)

Z. B. 12 120585 M 045

Format: 2 Stellen · 6-stelliges Geburtsdatum · 1 Buchstabe · 3 Stellen

Weiter

Haben Sie keinen Zugang? Wenden Sie sich an Ihre DRV-Geschäftsstelle.

Das Erstattungsportal der DRV

Beitragsdaten einsehen
Rufen Sie Ihre persönliche Storno-Akte und Abrechnungshistorie sicher ab.

Erstattungsanspruch prüfen
Ihren persönlichen Erstattungsbetrag gemäß § 26 SGB IV einsehen und freigeben.

DSGVO-konform & verschlüsselt
256-Bit SSL-Verschlüsselung. Ihre Daten werden gemäß Art. 6 Abs. 1 DSGVO verarbeitet.

Dieses Portal ist nur für den Zeitraum der aktuellen Beitragsüberprüfung 2024–2026 verfügbar.

Phishing E-Mails werden durch KI-Unterstützung immer perfider und sehen immer professioneller aus.

Früher – leicht zu erkennen

Von: support@bankk.com
Betreff: Wichtige Informationen!!!

Sehr geehrter Kunde,

Ihr Konto wurde gesperrt!

Klicken Sie hier, um es zu entsperren:
http://www.bankk.com/login

Mit freundlichen Grüßen
Ihr Bank-Team

OFFENSICHTLICH FAKE

Heute – dank KI täuschend echt

Ihre Bank Vertrauen. Sicherheit. Gemeinsam.

Von: service@ihre-bank.de
Betreff: Wichtige Information zu Ihrem Konto
Heute, 10:24

Sehr geehrte Frau Müller,

im Rahmen unserer aktuellen Sicherheitsüberprüfung bitten wir Sie, Ihre Kontodaten zu bestätigen. Dies dient Ihrer eigenen Sicherheit und ist in wenigen Minuten erledigt.

Jetzt Daten bestätigen →

Bei Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Thomas Berger
Kundenservice
Ihre Bank

www.ihre-bank.de
kundenservice@ihre-bank.de
+49 30 12345678

Ihre Sicherheit ist uns wichtig.



- BESSERE TEXTE
- NATÜRLICHER SCHREIBSTIL
- REALISTISCHE LAYOUTS & LOGOS
- PERSONALISIERTE INHALTE
- KAUM NOCH ZU UNTERSCHEIDEN

KI aus Sicht der Verteidiger

- Anomalie-Erkennung
- Automatisierte Analyse
- Schnellere Korrelation
- Unterstützung statt Ersatz

Praxisbeispiel: Ransomware

- Leak im Darknet erkannt
- Exposure Monitoring findet
- Analyst bewertet RisikoSchwachstelle
- Gegenmaßnahmen vor Angriff

Praxisbeispiel: KI-Phishing

- Täuschend echte E-Mails
- Mitarbeiter schwerer zu sensibilisieren
- Threat Intelligence liefert Indikatoren
- Mehrstufige Verifikation erforderlich

Empfehlungen und Erfolgsfaktoren

- Kontinuierliches Monitoring
- Kombination Mensch + KI
- Klare Prozesse
- Schnelle Reaktion

- Wie Angreifer denken: versetzen Sie sich in die Rolle der Cyberkriminellen
- Transparenz reduziert Risiken
- KI erhöht Tempo auf beiden Seiten
- Threat Intelligence schafft Vorsprung



GESCHWINDIGKEIT IST TRUMPF

KI-Agenten handeln in Sekunden. Ihre Verteidigung auch.

WER SCHNELLER ERKENNT,
SCHNELLER REAGIERT,
BLEIBT SICHER.

- Automatisierte Reconnaissance
- KI-generierte Phishing-Angriffe
- Automatisierte Schwachstellenausnutzung
- Adaptive Angriffsstrategien
- Skalierung in Sekunden



- Echtzeit-Erkennung
- KI-gestützte Analyse
- Automatisierte Reaktion
- Proaktive Abwehr
- Mensch + KI im Team

VOM REAKTIVEN ZUM PROAKTIVEN SCHUTZ – IN ECHTZEIT.

SICHTBARKEIT schafft die Basis → **ERKENNUNG** in Sekunden → **AUTOMATISIERUNG** stoppt Angriffe → **ANPASSUNG** durch kontinuierliches Lernen

Herzlichen Dank!

Für Ihre Aufmerksamkeit!



NetEye

