PROTFORCE
INFORMATION SECURITY

Das ist Protforce

Die fortschreitende Digitalisierung stellt die Informationssicherheit vor immer größere Herausforderungen. Als branchenübergreifender Experte kennen wir den Weg durch den Information Security Dschungel.

PROTFORCE GMBH

Alte Schmelze 20
65201 Wiesbaden
Tel.: +49 611 724 98 130
E-Mail: info@protforce.de

SOCIAL MEDIA

LinkedIn @Protforce GmbH
Instagram @protforce_is
TikTok @protforce_is
YouTube @protforce_is

PROTFORCE
INFORMATION SECURITY

Unsere Dienstleistungen auf einen Blick

Als umfassender Cyber Security Service Provider kennen wir die Herausforderungen, denen Unternehmen im Bereich Informationssicherheit begegnen. Unsere Dienstleistungen umfassen strategische, offensive und defensive Sicherheit, um die Systeme unserer Kunden zuverlässig zu schützen.

STRATEGISCHE SICHERHEIT

- **Beratung:** Wir bieten umfassende Beratung zur Verbesserung Ihrer Sicherheitsstrategie.
- **Planung & Steuerung:** Wir unterstützen Sie bei der Planung und Steuerung Ihrer Sicherheitsmaßnahmen.
- **Implementierung:** Wir setzen effektive Sicherheitlösungen nahtlos in Ihrer Infrastruktur um.
- **Discovery Workshops:** Gemeinsam erarbeiten wir ein ganzheitliches Sicherheitskonzept.

OFFENSIVE SICHERHEIT

- **Angriffsflächenanalyse:** Wir identifizieren potenzielle Schwachstellen in Ihrer IT-Infrastruktur.
- **Penetration Test:** Unsere Penetration Tests simulieren Angriffe, um Ihre Sicherheitslücken aufzudecken.
- **Schwachstellenanalyse:** Wir analysieren Ihre Systeme, um bestehende Schwachstellen zu erkennen.

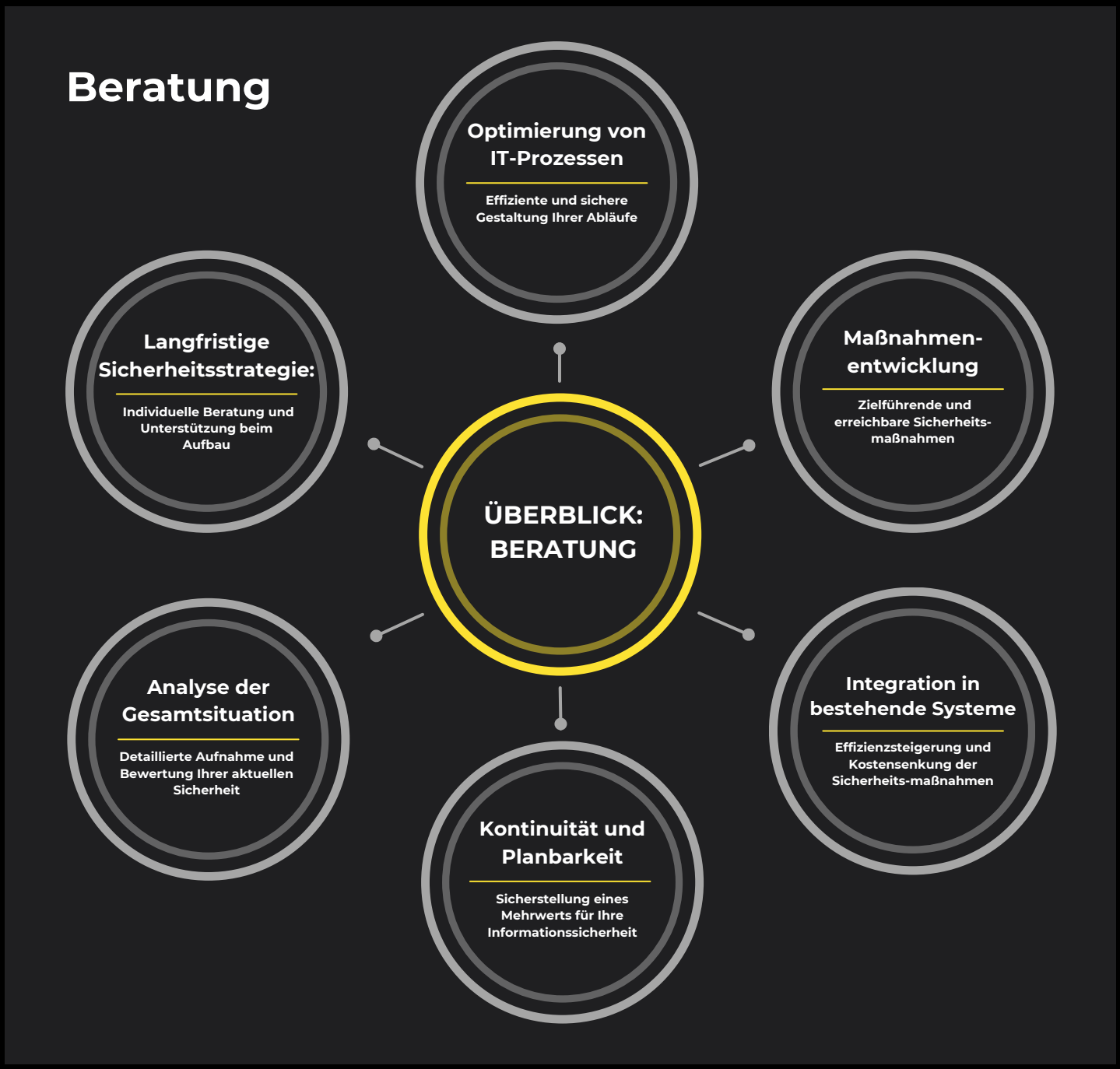
DEFENSIVE SICHERHEIT

- **Notfallmanagement**: Unser Notfallmanagement gewährleistet schnelle Reaktionen in Krisensituationen.
- **Systemhärtung**: Bei der Systemhärtung reduzieren wir Angriffsflächen Ihrer IT-Systeme.

Strategische Sicherheit

Sichere Grundlagen schaffen

Wir unterstützen Sie branchen- und größenunabhängig beim Aufbau einer langfristigen, individuellen Sicherheitsstrategie. Unser Ziel ist es, Optimierungsmöglichkeiten für die sichere und effiziente Gestaltung Ihrer IT-Prozesse und organisatorischen Maßnahmen aufzuzeigen. Wir analysieren Ihre bestehende Gesamtsituation und entwickeln zielführende Maßnahmen, um die Effizienz zu steigern und Kosten gering zu halten.



PROTFORCE
INFORMATION SECURITY

Beratung: Ein Blick in die Praxis

Vorschriften und Regularien

Konzepte zur Informationssicherheit sind zwar grundlegend, doch ohne eine kompetente Umsetzung entfalten sie ihre Wirkung nicht. Im Mittelpunkt stehen diverse, teilweise branchenspezifische, Standards und Richtlinien, wie etwa ISO/IEC 27001, NIS-2, BSI-Grundschutz oder DORA. Wir bieten umfassende Unterstützung bei der praktischen Implementierung dieser Rahmenwerke und optimieren Ihre internen Prozesse.

Unsere Erfahrung zeigt, dass Unternehmen häufig auf unsere Discovery Workshops zurückgreifen, um einen soliden Grundstein für eine effektive Umsetzung von Vorschriften und Richtlinien zu schaffen.

ISO/IEC 27001

ISO/IEC 27001 ist ein internationaler Standard für Informationssicherheits-Managementsysteme (ISMS). Er schützt vertrauliche Daten, sichert die Integrität und Verfügbarkeit von Informationen und unterstützt Unternehmen bei der Zertifizierung. Wir können Unternehmen helfen, ein effektives ISMS zu implementieren.

NIS-2

NIS-2 ist eine EU-Richtlinie zur Verbesserung der Cybersicherheit kritischer Infrastrukturen. Sie verpflichtet Unternehmen in essenziellen Sektoren, Cyberrisiken zu managen und Sicherheitsvorfälle zu melden. Wir unterstützen Unternehmen dabei, die Anforderungen der NIS2 zu erfüllen.

BSI-Grundschutz

Der BSI-Grundschutz ist ein deutscher Standard für Informationssicherheit, der praxisnahe Sicherheitsmaßnahmen bietet. Er hilft Organisationen, ihre IT-Systeme abzusichern und sich an ISO/IEC 27001 zu orientieren. Wir können Unternehmen bei der Umsetzung des BSI-Grundschutzes unterstützen.

DORA

DORA ist eine EU-Verordnung zur Stärkung der digitalen Resilienz im Finanzsektor. Sie fordert von Finanzinstituten, IT-Sicherheitsvorkehrungen zu treffen und Störungen zu bewältigen. Wir helfen Unternehmen, die Anforderungen von DORA erfolgreich zu erfüllen.

Planung und Steuerung

Fehlende Planung und unzureichende Steuerung bei der Umsetzung von Sicherheitsmaßnahmen können die Informationssicherheit erheblich gefährden. Um nachhaltigen Schaden zu vermeiden, ist es entscheidend, dass Sicherheitsziele klar definiert und sorgfältig mit der Wirtschaftlichkeit Ihres Unternehmens abgestimmt werden. Eine erfolgreiche Umsetzung erfordert daher eine durchdachte Planung und kontinuierliche Steuerung aller Maßnahmen. Zusätzlich sind interne Ressourcen, Zeit und oft auch Anpassungen im Geschäftsbetrieb notwendig, um diese Ziele effektiv und fristgerecht zu erreichen.

- **Klare Sicherheitsziele und Ausrichtung auf Wirtschaftlichkeit**
- **Planung und Steuerung als Grundlage erfolgreicher Umsetzung**
- **Anpassung des Geschäftsbetriebs und Einsatz interner Ressourcen**

Implementierung

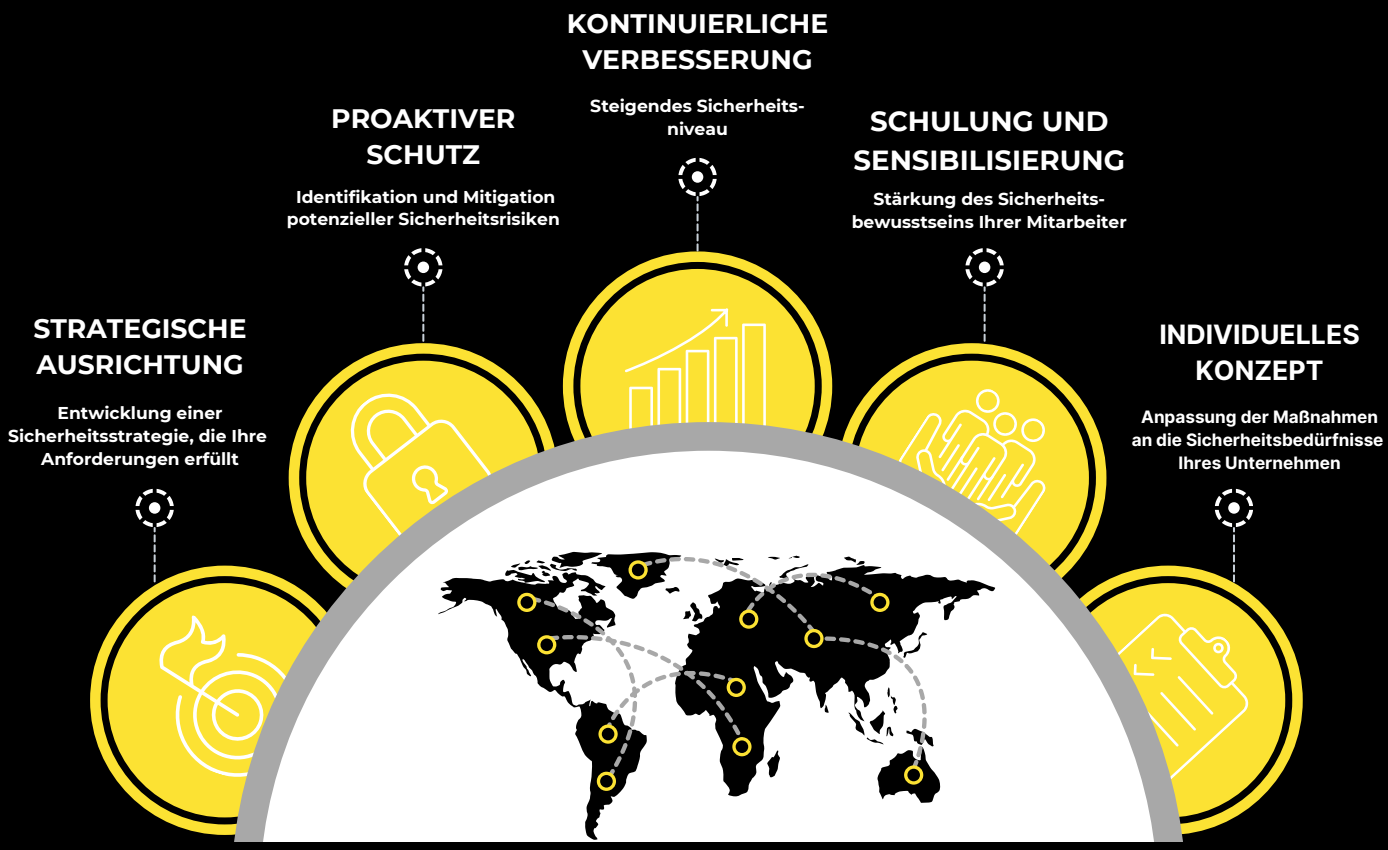
Theorie und Konzeption zur Informationssicherheit sind unverzichtbar, aber ohne kompetente Umsetzung nutzlos. Wir unterstützen Sie nicht nur mit der Theorie, sondern setzen gemeinsam Sicherheitsmaßnahmen praktisch um – vom Systemaufbau bis zur internen Operationalisierung. Zudem begleiten wir Sie bei der Einführung oder Erweiterung von Prozessen und Informationssicherheitsrichtlinien. Dabei achten wir auf effiziente Strukturen und die richtige Kommunikation, um Akzeptanz und Verständnis für Informationssicherheit in der Belegschaft zu fördern.

- **Praktische Umsetzung von Sicherheitsmaßnahmen**
- **Einführung und Erweiterung von Prozessen und Richtlinien**
- **Förderung von Akzeptanz und Verständnis in der Belegschaft**

Discovery Workshops

Unsere Discovery Workshops bilden die Grundlage für ein nachhaltiges IT-Sicherheitskonzept durch individuelle Strategien und Sensibilisierung aller Mitarbeiter. Gemeinsam entwickeln wir eine ganzheitliche Sicherheitsstrategie, identifizieren Risiken und setzen gezielte Maßnahmen zur Risikominderung ein. Regelmäßige Schulungen stärken das Sicherheitsbewusstsein und passen die Maßnahmen flexibel an Ihre Bedürfnisse an.

Unsere Erfahrung zeigt, dass Unternehmen unsere Workshops als Orientierung für zukünftige Projekte nutzen. Durch die Identifikation von Risiken und Verbesserungspotenzialen erhalten Unternehmen eine strukturierte Grundlage für strategische Entscheidungen, was zu einem robusteren Sicherheitskonzept und langfristiger Resilienz führt.



Offensive Sicherheit

Der Angriff als bestes Mittel zur Verteidigung

Trotz Schutzmaßnahmen wie Firewalls und Antivirenprogrammen bleiben Unternehmen oft verwundbar. Schwachstellen, Fehlkonfigurationen und menschliche Fehler öffnen Angreifern Tür und Tor. In der offensiven Sicherheit begeben wir uns in die Rolle des Angreifers, um gezielt Schwachstellen und Angriffsflächen aufzudecken und Ihre IT-Systeme widerstandsfähiger zu machen.

ANGRIFFSFLÄCHEN-ANALYSE	SCHWACHSTELLEN-ANALYSE	PENETRATION TESTS
Wir analysieren Ihre IT-Systeme, um Angriffsflächen zu identifizieren und die Widerstandsfähigkeit Ihrer Infrastruktur zu erhöhen.	Schwachstellen werden identifiziert, um durch uns gezielte Maßnahmen zur Risikominderung zu ermöglichen.	In einem simulierten Angriff identifizieren wir Vulnerabilitäten und zeigen Ihnen Sicherheitslücken, bevor Angreifer diese ausnutzen.

Angriffsflächenanalyse

Viele Unternehmen geben unbewusst Informationen preis, die Angreifern Vorteile verschaffen, um Einblicke in Technologien, Mitarbeiter und Prozesse zu gewinnen. Wir bewerten Ihre externe Sicherheit durch eine Angriffsflächenanalyse und erstellen einen Bericht über potenzielle Bedrohungen sowie Empfehlungen für Gegenmaßnahmen.

Vorgehen

- **Informationsbeschaffung:** Auswertung öffentlich zugänglicher Informationen
- **Analyse:** Bewertung der Informationen aus Sicht eines Angreifers
- **Berichterstattung:** Erstellung eines Berichts über Angriffsvektoren
- **Handlungsempfehlungen:** Optimierung der Angriffsfläche
- **Umsetzung:** Unterstützung bei der Implementierung der Empfehlungen

PROTFORCE
INFORMATION SECURITY

Schwachstellenanlyse

Bekannte Schwachstellen ermöglichen Angreifern einen einfachen Zugang zu IT-Systemen. Wir setzen moderne Testverfahren ein, um diese Schwachstellen gezielt zu identifizieren und entsprechende Gegenmaßnahmen zu entwickeln. Regelmäßige Schwachstellenanalysen verbessern die Sicherheitslage und ermöglichen eine zeitnahe Reaktion auf neue Bedrohungen.

Vorgehen

- **Analyse:** Erfassen der IT-Infrastruktur zur Festlegung des Umfangs
- **Automatisierte Scans:** Identifikation bekannter Schwachstellen
- **Manuelle Prüfungen:** Detaillierte Bewertung durch Sicherheitsexperten
- **Berichtserstellung:** Ausarbeitung von Details und Handlungsempfehlungen
- **Umsetzung:** Unterstützung, Behebung und Anpassung von Prozessen

Penetration Tests

Penetration Tests sind Sicherheitsüberprüfungen, bei denen wir in die IT-Systeme eines Unternehmens eindringen, um Schwachstellen aufzudecken. Unsere Tests simulieren reale Angriffe mit maßgeschneiderten Szenarien und innovativen Analysemethoden. Die identifizierten Schwachstellen werden in einem Bericht zusammengefasst, der technische Informationen und konkrete Handlungsempfehlungen enthält.

Mehrwerte

- Reduzierter Ressourceneinsatz durch lösungsorientiertes Vorgehen
- Erhöhte Erkennungsrate durch softwaregestützte und manuelle Prüfungen
- Verständliche und übersichtliche Kundenberichte
- Prüfungen nach Standards von OWASP, PTES und BSI
- Konkrete Handlungsempfehlungen zur Behebung von Schwachstellen
- Unterstützung bei der Behebung von Schwachstellen

PROTFORCE
INFORMATION SECURITY

Defensive Sicherheit

Perfekt aufgestellt mit geschultem Team und gesichertem System

Die Auswirkungen einer initialen Kompromittierung hängen stark von der Effektivität Ihrer defensiven Sicherheit ab. Ein erfolgreicher Angriff bedeutet nicht zwangsläufig den Verlust der Kontrolle über Ihre Systeme. Wir setzen auf die Planung und Umsetzung bewährter Sicherheitsprinzipien und führen angepasste Gegenmaßnahmen auf Basis spezifischer Bedrohungsanalysen durch. Dazu gehören der Aufbau von Security Awareness, die Minimierung der Informationspreisgabe und die Reduzierung des technischen Funktionsumfangs gemäß etablierter Standards.

SYSTEMHÄRTUNG

Das Erkennen und Schließen von Schwachstellen ist entscheidend für die Sicherheit Ihrer IT-Infrastruktur.

NOTFALL-MANAGEMENT

Eine durchdachte Notfallplanung gewährleistet die Handlungsfähigkeit in kritischen Situationen.

Systemhärtung

Um effektiven Schutz zu gewährleisten, ist eine systematische Optimierung und Härtung der bestehenden Systeme unerlässlich. Standardlösungen allein reichen nicht aus, da sie nicht in der Lage sind, gegen moderne Angriffe und neuartige Schadsoftware zu bestehen. Durch individuelle Härtungskonzepte und die Kombination anerkannter Standards mit Best-Practices können Unternehmen ihre Systeme unattraktiver für Hacker machen und somit die Sicherheit signifikant erhöhen.

- **Gezielte Härtung für komplexe Systeme:** Individuelle Konfiguration und Härtung sind entscheidend angesichts vielfältiger Bedrohungen.
- **Unzureichende Standardlösungen:** Firewalls und Antivirenprogramme bieten oft keinen Schutz gegen moderne Angriffe.
- **Sicherheitsrisiken minimieren:** Individuelle Härtungskonzepte erschweren potenzielle Angriffe.

PROTFORCE
INFORMATION SECURITY

Notfallmanagement

In einer zunehmend vernetzten und digitalisierten Welt sind Unternehmen jeglicher Größe einer Vielzahl von Bedrohungen ausgesetzt, die plötzliche und existenzbedrohende Notfälle hervorrufen können. Ein effektives Notfallmanagement ist daher unerlässlich, um die Resilienz Ihres Unternehmens zu gewährleisten und auf unvorhergesehene Ereignisse angemessen zu reagieren.

Durch die Entwicklung maßgeschneiderter Notfallpläne und die Implementierung von Krisenbewältigungsstrategien stellen wir sicher, dass Ihr Unternehmen optimal vorbereitet ist, um auch in kritischen Situationen handlungsfähig zu bleiben.

UMFASSENDE VORBEREITUNG

Eine gründliche Notfallplanung ist entscheidend, um Unternehmen vor existenzbedrohenden Cyberangriffen zu schützen.

BSI-STANDARDS

Wir entwickeln einen maßgeschneiderten Notfallplan, der Kommunikationswege und Krisenbewältigungsstrategien regelt.

IDENTIFIKATION KRITISCHER ASSETS

Wir helfen bei der Identifizierung geschäftskritischer IT-Assets und erstellen Wiederanlauf- und Wiederherstellungspläne.

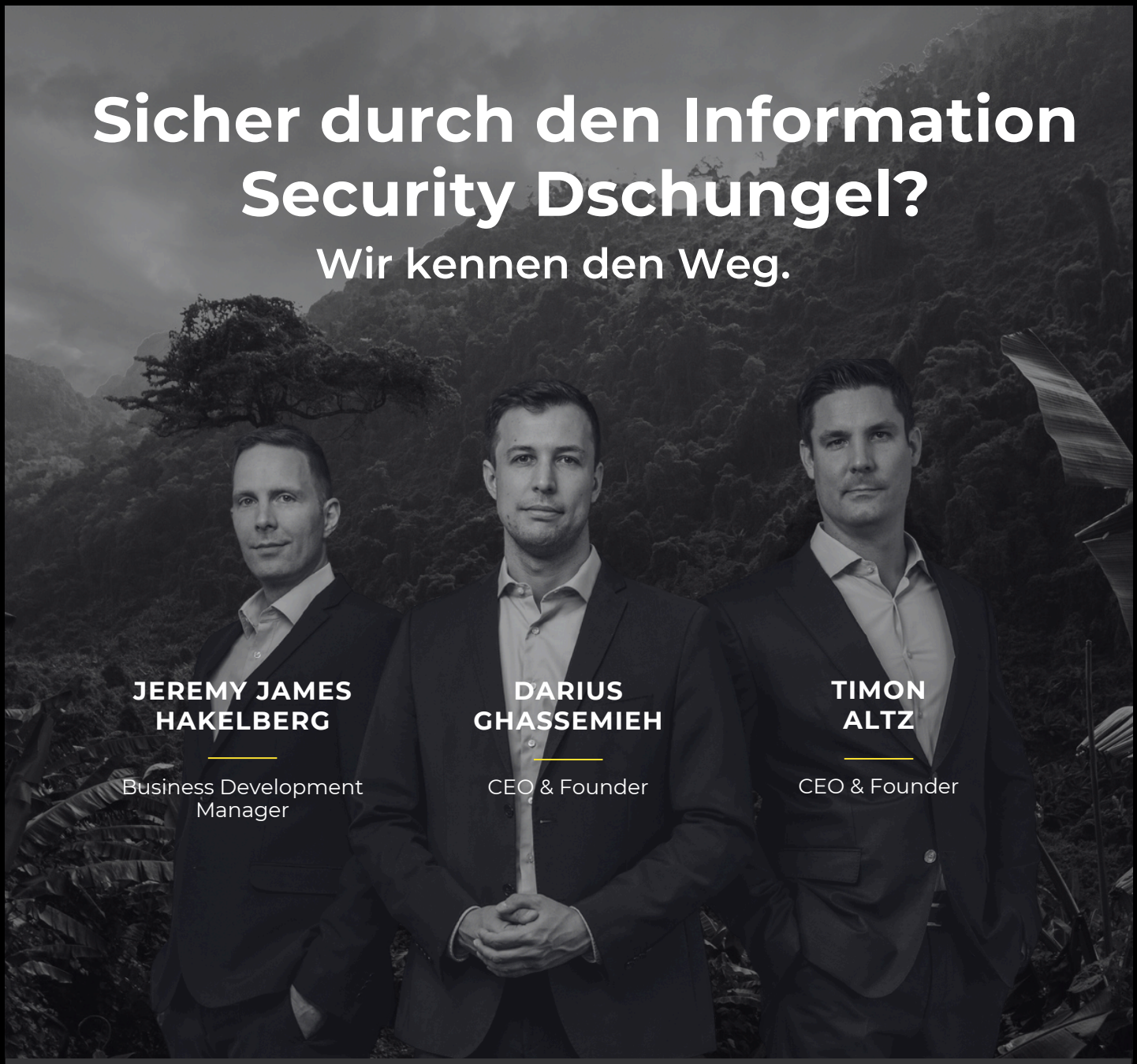
REALISTISCHE NOTFALLSIMULATIONEN

Durch regelmäßige Simulationen überprüfen wir die Wirksamkeit des Notfallmanagements und identifizieren Verbesserungspotenziale.

PROTFORCE
INFORMATION SECURITY

Sicher durch den Information Security Dschungel?

Wir kennen den Weg.



JEREMY JAMES HAKELBERG

Business Development Manager

DARIUS GHASSEMIEH

CEO & Founder

TIMON ALTZ

CEO & Founder

FORDERN SIE UNS HERAUS!

Fordern Sie uns mit Ihren aktuellen Themen zur Informationssicherheit heraus. Ob technische Spezialisten oder Security Manager, wir haben den passenden Experten für Sie!

+49 611 724 98 130

www.protforce.de

sales@protforce.de

Alte Schmelze 20, 65201 Wiesbaden