

BDO CYBER SECURITY

# BDO CYBER SECURITY

## GANZHEITLICHER ANSATZ



Es ist Ziel und Anspruch der BDO Cyber Security GmbH, zu allen wichtigen Aspekten der IT-Security ein passendes Beratungsangebot zur Verfügung zu stellen. Um diese umfangreiche Thematik angemessen darzustellen, ist es notwendig, sich dem Thema aus verschiedenen Blickwinkeln zu nähern:

### BUSINESS-PROZESSE / GESCHÄFTSMODELL

BEDROHUNGEN	REGULATORISCHER RAHMEN	KOMPONENTEN	BENUTZER
Klassifizierung	Gesetze	Basis	Identität
Signatur	Richtlinien	Plattform	Gruppe
Szenarien	Organisatorische Anforderungen	Netzwerk	Rollen
Maßnahmen	Allgemeine Anforderungen	Applikation	Account

### BEDROHUNGEN

Die erste Betrachtungsebene geht über die verschiedenen Bedrohungen. Es ist selbstverständlich eine originäre Aufgabe einer IT-Security-Architektur, Bedrohungsszenarien zu erkennen und abzuwehren bzw. ihnen vorzubeugen. Daraus resultieren Vorgaben für die Organisation und Implementierung.

### REGULATORISCHER RAHMEN

Die zweite Betrachtungsebene geht über die regulatorischen Grundlagen. Diese Ebene hat in letzter Zeit an Bedeutung immer weiter zugenommen, und dieser Trend wird sich fortsetzen. Wir bieten Analysen aller technischen und fachlichen Infrastrukturen und unterstützen beim Aufbau von regulatorisch konformen Zielarchitekturen.

### ÜBER BDO CYBER SECURITY

Wir bieten unseren Kunden im Rahmen einer ganzheitlichen Beratung zum Themenkomplex IT-Security das gesamte IT-Security Portfolio in Form von definierten Leistungsbausteinen innerhalb verschiedener Wertschöpfungsketten an. Wir stehen Ihnen zu Seite bei der strategischen Entwicklung, Implementierung und Inbetriebnahme von IT-Security-Maßnahmen.

[www.bdosecurity.de](http://www.bdosecurity.de)

### KONTAKT

**BDO Cyber Security**  
Fuhrentwiete 12  
20355 Hamburg



**Andreas Stemick**  
Vorsitzender der  
Geschäftsführung  
BDO Cyber Security GmbH  
Telefon: +49 211 1371-0  
[andreas.stemick@bdosecurity.de](mailto:andreas.stemick@bdosecurity.de)



**Klaus Stumm**  
Leiter Vertrieb  
BDO Cyber Security GmbH  
Telefon: +49 611 9904-264  
[klaus.stumm@bdosecurity.de](mailto:klaus.stumm@bdosecurity.de)

## KOMPONENTEN

Die dritte Betrachtungsebene geht über die beteiligten Komponenten. Die IT-Infrastruktur besteht aus einer ganzen Reihe von standardisierten oder gewachsenen Komponenten, welche ihre eigenen Sicherheitsstandards bzw. Konventionen haben. Diese Sichtweise ist wesentlich für jede Implementierung. Steht man vor der Aufgabe, Vorgaben für neu zu implementierende oder zu ändernde Komponenten zu entwickeln, möchte aber bestehende Lösungen aus ergonomischen Gründen so gut wie möglich weiter nutzen, empfiehlt sich eine Untergliederung in Plattform-, Netzwerk- und Application Security. Jede dieser Ebenen hat ihre eigenen Konventionen und Sicherheitsbestimmungen. Es wäre allerdings verfehlt, die Ebenen als vollkommen disjunkt zu betrachten, denn selbstverständlich lässt sich die gewünschte Security nur im Zusammenspiel erzielen.

## BENUTZER

Die vierte Betrachtungsebene hat als Ausgangspunkt den Benutzer. Es beginnt bei der Zuordnung der Identität, und hier ist die Kernanforderung nach der eindeutigen Identität angesiedelt, also die Forderung nach Eindeutigkeit des Identitätsschlüssels über die gesamte Systemlandschaft hinweg. Diese Forderung erstreckt sich auf alle Typen von Benutzern, also nicht nur auf named-User („warm bodies“), sondern auch auf alle technischen bzw. Maschinen-User („cold bodies“). Nächster Schritt ist die Einordnung der Identitäten in Benutzergruppen, welche wiederum der Ausgangspunkt sind für die Ableitung von Rollen- und Berechtigungskonzepten. Darüber hinaus gibt es noch eine ganze Reihe von Themenkomplexen, welche für sich alleine stehen, aber ebenfalls zur IT-Security gehören und erhebliche Relevanz haben. Beispielhaft zu nennen wären PAM (Privileged Account Management), SOC (Security Operation Center), SIEM (Security Information and Event Management), PKI (Private Key Infrastructure) und viele weitere. Auch dafür bieten wir Ihnen passende Leistungsangebote an.