



Security Research Sicherheitsforschung GmbH

Leistungsportfolio

Mit Sicherheit ein guter Partner.

www.securityresearch.at

## Hintergrund und Vorstellung

Security Research ist als forschungsnaher Technologieführer in Österreich Ihr Partner in den Bereichen technische und organisatorische IT-Sicherheitsberatung, Schulung und Umsetzung, Security Governance Engineering und kontrollorientiertes Prozessdesign.

Dabei werden wissenschaftliche Erkenntnisse aus der IT-Sicherheitsforschung mit Prozessmanagementmethodologien und Wissen um regulative Anforderungen kombiniert, um unter Berücksichtigung technischer und organisatorischer Sicherheitsaspekte Geschäftsprozesse zu optimieren.

Die zunehmende Abhängigkeit der Unternehmen von Verfügbarkeit, Vertraulichkeit und Integrität der Informationssysteme macht IT-Sicherheit zu einem zentralen Erfolgsfaktor für die langfristige Wettbewerbsfähigkeit.

Unser Ansatz einer ganzheitlichen Betrachtung von organisatorischen und technischen Aufgabenstellungen – orientiert an den produktiven/gewinnbringenden Kernprozessen – kann dabei einen wesentlichen Beitrag leisten.

Security Research bietet Ihnen eine breitgefächerte Dienstleistungspalette in Fragen Informationssicherheit an, um eine solche Gesamtbetrachtung zu ermöglichen.

Das Leistungsangebot gliedert sich grob in vier Bereiche, wobei die ersten zwei Bereiche vorwiegend organisatorische und die letzten beiden technologiefokussierte Aufgabenstellungen adressieren.

Im Technologiesegment sind wir auf sichere Softwareentwicklung und auf Microsoft Infrastruktur- und Architekturlösungen spezialisiert. Der organisatorische Bereich umfasst Audit-based Services und Informationssicherheitsdienstleistungen.

Regulative Anforderungen wie z.B. die 8. EU-Richtlinie und das Datenschutzgesetz fordern verstärkt den Einsatz eines internen Kontrollsystems (IKS), das die Sicherheit in Ihrem Unternehmen kontrollierbar und nachvollziehbar macht.

Unsere sicherheitsorientierten Analysen sowie unsere praktischen Umsetzungen können helfen, sowohl Schwachstellen als auch Optimierungspotential in Ihren IT-Prozessen oder Ihrer IT-Infrastruktur zu lokalisieren.

Unsere Mitarbeiter verwenden unterschiedliche, praxiserprobte Methoden und Ansätze, um solche Schwachstellen zu finden und zu beseitigen sowie praxisrelevante Verbesserungen umzusetzen. Dabei stehen sicherheitsrelevante Anforderungen wie etwa Vertraulichkeit, Integrität, Verfügbarkeit, Vollständigkeit, Verbindlichkeit und Nachvollziehbarkeit Ihrer Unternehmensinformationen im Fokus.

Ziel ist, verbesserte, effizientere und komfortablere Gesamtlösungen zu entwickeln, die den Informationssicherheitsanforderungen Rechnung tragen.

Im Folgenden möchten wir einen kleinen Auszug einschlägiger Referenzen mit Themen und Branche präsentieren. Wir gewährleisten unseren Kunden maximale Vertraulichkeit, deshalb wird hier die Anonymität der Unternehmen gewahrt:

- Implementierung eines IT-Kontrollsystems bei einem international agierenden und börsennotierten Fortune 500 Industrieunternehmen
- Implementierung eines Information Security Management Systems bei einem internationalen Energieversorger
- Begleitung des Rechenzentrums eines international agierenden und börsennotierten Fortune 500 Industrieunternehmens zur ISO 27001 Zertifizierung
- Mehrwöchige externer und interne Netzwerk-Penetrationstests bei international tätigen Versicherungen
- Mehrwöchige Sicherheitsuntersuchung von Web-Applikation bei international tätigen Banken
- Mehrwöchiger externer und interner Netzwerk-Penetrationstest des IT-Ressorts eines deutschen Automobilkonzerns
- Entwicklung einer komplexen und datenschutzrechtlich hochsensiblen Internetlösung auf Sharepoint-Basis für einen großen österreichischen Gesundheitsdienstleister

## Dienstleistungen

<b>Audit-based Services</b> Installation und Ausrichtung interner Kontrollsysteme IT-Revision IT-Auditing	<b>Security Services</b> IT-Governance, Risk & Compliance Beratung Informationssicherheitsanalyse Security Awareness BCM/ DRP Web-Application & Penetration Testing	<b>Entwicklung</b> Software Security Beratung Secure Coding Training Enterprise Solution Development	<b>Microsoft Gold Partner</b> Beratung Infrastruktur Architektur <b>Produktportfolio</b> Fortify 360 Data Loss Prevention
--	--	---	---

Ergänzend zu unseren Dienstleistungen sind wir als Exklusivvertretung in Österreich Ihr Ansprechpartner für die Produkte Fortify 360 und Data Loss Prevention von Symantec.

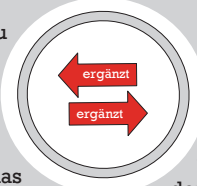


## Audit-based Services

### IKS Engineering

Security Research bietet Projektbegleitung bei Aufbau und Ausrichtung interner Kontrollsysteme an und schneidet diese individuell auf Ihr Unternehmen und dessen Rahmenbedingungen zu. Mögliche Arbeitsschritte im Rahmen von IKS Engineering sind:

- Auswahl und Beurteilung eines Regelwerks für das interne Kontrollsystem, deren **praktische Implementierung** und die Zuordnung von Verantwortlichkeiten
- Hilfestellung bei der Auswahl des Regelwerks für das interne Kontrollsystem und Vorbereitung auf mögliche Zertifizierungen wie z.B. ISO 27001
- Durchführung einer **Abweichungsanalyse** von dem bestehenden zu dem ausgewählten Regelwerk
- Ableitung von Handlungsempfehlungen und Unterstützung bei der **Umsetzung von Maßnahmen** zur Beseitigung der aufgedeckten Kontrolllücken
- Teilweise oder vollständige **Implementierung** eines IT-gestützten internen Kontrollsystems
- Unterstützung bei der Erstellung der notwendigen Dokumentation interner Kontrollen
- **Regelmäßige Prüfung** der Vollständigkeit und Funktionsfähigkeit der internen Kontrollen

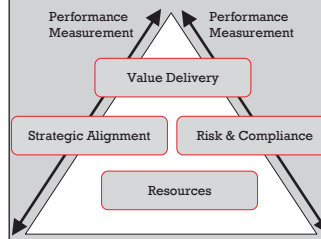


## Security Services

### Penetration Testing

Der Penetrationstest stellt eine Möglichkeit der Bewertung Ihrer IT-Sicherheit dar. Beim Penetrationstest werden Computersysteme und Netzwerke analysiert, um Schwachstellen in der IT Infrastruktur zu lokalisieren und zu beseitigen. Eine weitere Form des Penetrationstests ist der Web Applikation Penetrationstest, bei dem die Sicherheit Ihrer von außen zugänglichen Web Applikationen evaluiert wird.

### IT-Governance, Risk und Compliance Guidance



Die Ausrichtung der IT-Investitionen an den Geschäftszielen und Unternehmensstrategien ist heutzutage Kernaufgabe des IT-Managements. Um diese Aufgaben bewältigen zu können, werden den Entscheidungsträgern mit Hilfe eines IT-Governance Frameworks exakte und präzise Informationen zur Verfügung gestellt.

### Informationssicherheitsanalyse

Hierbei handelt es sich um eine Analyse der aktuellen Sicherheitslage in Ihrem Unternehmen und der Identifikation von Schwachstellen in Bezug auf **Vertraulichkeit, Integrität, Verfügbarkeit, Vollständigkeit, Verbindlichkeit und Nachvollziehbarkeit** von Unternehmensinformationen. Unsere Sicherheitsanalysen werden an die individuellen Bedürfnisse angepasst und reichen von kurzen Checklistenprüfungen bis hin zu detaillierten Untersuchungen der IT-Infrastruktur auf Netzwerk-, Betriebssystem-, Datenbank- sowie organisatorischer Ebene. Bei Sicherheitsanalysen setzen wir auf Best Practice Ansätze und Methoden wie z.B. **CRISAM**.

### Computer Forensics und Incident Response

Forensische Analysen ermöglichen **exakte Rekonstruktion und Beweisführung** eines Sicherheitsvorfalls, weiters die Datenrekonstruktion und Feststellung des Sachverhalts.

### Security Awareness

Die IT Sicherheit behandelt den Menschen als Risikofaktor. Dementsprechend muss jeder Mitarbeiter in das Sicherheitskonzept eines Unternehmens eingebunden werden. Security Awareness steht für das Verhalten bzw. das entwickelte Bewusstsein gegenüber sicherheitsrelevanten Themen und betrifft alle Mitarbeiter in einem Unternehmen. Ein gut geschulter Mitarbeiterstab kann frühzeitig Angriffsversuche erkennen und so essentiell zur Informationssicherheit im Unternehmen beitragen. Unter **Social Engineering** werden Angriffe auf menschliche Schwächen verstanden, die wir auf Wunsch planen und ausführen.

### Business Continuity Management

BCM gilt als wesentlicher Bestandteil eines IT Governance bzw. Security Governance Programms. Primäres BCM Ziel ist es, das Unternehmen auf katastrophale Ereignisse vorzubereiten, sodass das Unternehmen nicht nachhaltig geschädigt wird. BCM besteht vorrangig aus Business Impact Analyse, Risk Assessment, Lösungskonzeptionierung und Umsetzung. Lösungskonzepte sind z.B. Incident Response Plan & Struktur, Business Continuity Plan und Disaster Recovery Plan.

Prozesse



#### Planung

- Analyse
- Risiken identifizieren
- Festlegung der Audit-Strategie
- Bildung des Analyseteams
- Kommunikationskanäle festlegen
- Ressourcen- und Terminbestimmung

#### Evaluierung

- Prozessanalyse
- Kontrolldesign bewerten
- Kontrolleffizienz und -effektivität untersuchen
- Kontrolllücken und Schwachstellen identifizieren

#### Ausführliche Prüfung

- Durchführung technischer Prüfungen
- Aufzeigen von Sicherheitslücken
- Abgleich mit IT-Compliance Anforderungen

#### Abschluss

- Management Summary
- Detaillierter Analysebericht
- Katalog mit priorisierten Maßnahmen
- Workshops

Unser Expertenteam bietet Ihnen kompetente Unterstützung und übernimmt gerne teilweise oder vollständig die **IT-Revisionsfunktion** für Ihr Unternehmen, selbstverständlich unter Beachtung von geltenden nationalen und internationalen Fachgutachten und Gesetzgebungen.

### IT-Auditing

Ihre IT-Systemlandschaft wird demnächst von einem Wirtschaftsprüfer kontrolliert, Sie wissen aber nicht, was Ihr Unternehmen bei dieser Prüfung erwartet?

Sie sind sich nicht sicher, welche regulatorischen Anforderungen auf Ihr Unternehmen zutreffen oder welche Gutachten ein Wirtschaftsprüfer bei der IT-Prüfung heranzieht?

Die letzte IT-Prüfung ergab zahlreiche Schwachstellen - sie wissen aber nicht im Detail, ob diese Probleme schon beseitigt worden sind?

Wenn Sie sich als IT-Manager oder Rechnungswesenleiter mit ähnlichen Fragestellungen auseinandersetzen müssen, unterstützen wir Sie gerne bei der Vorbereitung für entsprechende Audits.

## Entwicklung

### Software Security Beratung

Die Sicherheit von Programmen hängt größtenteils von der Qualität des Quellcodes ab. Durch die Anwendung von modernen Programmier- und -prozessen sowie den profunden Security-Background unserer Entwickler können wir auf viele erfolgreiche Projekte im Bereich der sicheren Softwareentwicklung verweisen.

**Code Audits** sind eine wichtige Technik, um die Qualität und Sicherheit von Programmen zu erhöhen. Unser Leistungsportfolio umfasst sowohl automatisiertes Testen als auch manuelle Prüfungen. Durch die Kombination dieser beiden Ansätze können viele der gängigsten Fehler bereinigt, aber auch spezifische Probleme in den jeweiligen Architekturen beseitigt werden.

### Secure Coding Training

Eine Kette ist nur so stark wie ihr schwächstes Glied – so wäre auch die beste Absicherung Ihrer IT-Infrastruktur wirkungslos, wenn Ihre Software ausnutzbare Schwachstellen aufweist.

Unser Expertenteam verfügt über eine jahrelange Expertise im Bezug auf sichere Softwareentwicklung, dokumentiert anhand einschlägiger und umfassender Zertifizierungen.

Secure Coding Trainings unterliegen keiner Einschränkung durch die eingesetzten Programmiersprachen, da unser Ansatz produkt- bzw. sprachenunabhängig ist.

### Enterprise Solution Development

Unser Schwerpunkt liegt auf der Entwicklung maßgeschneiderter und individueller Softwarelösungen für Mittelstands- und Großkunden jeder Branche. Aufbauend auf bestehenden Geschäftsprozessen unterstützen wir Sie sowohl in der Ausschreibungs-, Planungs- und Entwicklungsphase einer Gesamtlösung für Ihr Unternehmen als auch bei der Implementierung und Integration von individuellen Applikationen oder Teilkomponenten. Wir **entwickeln integrierte, angepasste Unternehmenslösungen** und unterstützen Sie bei der Identifizierung und Optimierung Ihrer Geschäftsprozesse, angefangen bei der Analyse, Beratung und Konzeption bis hin zur Umsetzung. Des Weiteren verfügen wir im Rahmen unserer Partnerschaft mit Fortify über zusätzliche Möglichkeiten und Ansätze zur Verbesserung der Softwaresicherheit in ihrem Unternehmen.

Die Implementierung technischer Lösungen basierend auf **Microsoft Sharepoint Server** stellt eine Kernkompetenz im Rahmen von Enterprise Solution Development dar.

### Fortify 360

Fortify 360, die weltweit führende Lösung im Bereich der **automatisierten Schwachstellenanalyse**, unterstützt Sie bei der Identifizierung, Priorisierung und Beseitigung von Sicherheitslücken in Ihrer Software.

Die vier Kernkomponenten sind Schwachstellenerkennung, kooperative Korrektur, Berichterstellung und Regulierung sowie intelligentes Bedrohungsmanagement.

Mit Fortify 360 wird die erste Lösung bereitgestellt, die dynamische und statische Analyse integriert. Sowohl ein Static Code Analyser (SCA) als auch zwei dynamische Analysetools stehen zur Verfügung: ein Testphasen-fokussierter Program Trace Analyser (PTA) und ein Produktionsphasen-orientierter Real Time Analyser (RTA).



## Microsoft

### Beratung

Die IT-Infrastruktur ist heutzutage Grundlage für jedes innovative Unternehmen. Daher gilt es, die IT zu schützen, ohne die Funktionalität für und den Gebrauch durch die Mitarbeiter einzuschränken. **Schützen Sie Ihre IT, schützen sie Ihr Unternehmen!**

Als fünffacher **Microsoft Gold Partner** evaluieren wir den aktuellen Sicherheitsstatus Ihrer Microsoft-Infrastruktur, insbesondere in Hinblick auf Domain Controller, Exchange Server, Anti Virus/Spam und Firewalling. Dabei greifen wir auch auf unsere Unix-/Linux-Experten zurück, um heterogene Lösungen anbieten zu können.

Wir evaluieren und entwerfen State-of-the-Art Netzwerk- und IT-Umgebungen. Typische Szenarien sind: Software- und Clientvirtualisierung, Client Management, Rollout Management, Softwareverteilung und sicherheitskritische Architekturen.

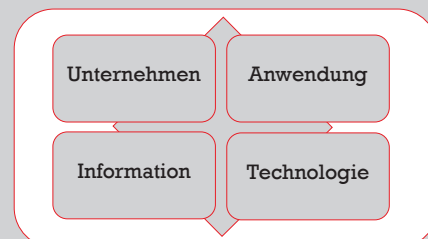
Bei unseren Mitarbeitern legen wir größten Wert auf begleitende Zertifizierungen, um die Qualität ihrer Leistungen auch formal zu dokumentieren. Im Microsoftumfeld haben wir daher eine hohe Dichte an entsprechenden Ausbildungen (MCITP, MCSA, MCSE etc.), die laufend aktualisiert und erweitert werden.

### Enterprise Infrastructure Solutions

Viele Komponenten im Enterprise-Umfeld erfordern Detailwissen und spezialisiertes Produkt Know How für den Einsatz erprobter Lösungen. Aufgrund unserer vielseitigen und langjährigen Tätigkeit in diesem Bereich legen unsere Kunden immer größeren Wert darauf, bei sensiblen Fragestellungen auf unsere Fachexperten zurückgreifen zu können. Dabei steht neben der effizienten Umsetzung vor Allem auch der **Wissens-transfer** zu Ihren eigenen Fachleuten im Vordergrund. Wir unterstützen Sie bei der Implementierung und Wartung von Microsoft Infrastrukturkomponenten wie z.B.:

- Windows Server 2008
- Hyper-V
- SCCM, SCOM, SCVMM
- Exchange Server 2007
- Office Communication Server
- Forefront Produktreihe

### Enterprise Architecture Design



Wir planen, adaptieren und entwickeln gemeinsam mit Ihnen unternehmensweite IT-Architekturen, die auf Ihre Bedürfnisse sowie gesetzliche und sicherheitstechnische Anforderungen abgestimmt sind und prüfen darüber hinaus bestehende Lösungsansätze. Die häufigsten Architekturfragen betreffen die Bereichen Netzwerkinfrastruktur, Softwarearchitektur und Prozessarchitektur (z.B.: ITIL, Microsoft Operating Framework).

### Data Loss Prevention (DLP)

Informationsaustausch im Unternehmen muss gesteuert und überwacht werden, um vertrauliche & wertvolle Informationen zu schützen.

Symantec Data Loss Prevention bietet eine umfassende Lösung, Informationen aufzuspüren, zu überwachen und zu schützen, unabhängig vom Ort der Speicherung, der Transportkanäle oder der Art der Nutzung.

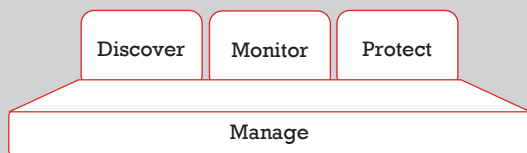
DLP beantwortet Ihnen drei grundlegende Fragen:

- Wo sind Ihre vertraulichen Daten?
- Wie werden Ihre Daten verwendet?
- Wie können Sie Ihre Daten schützen?

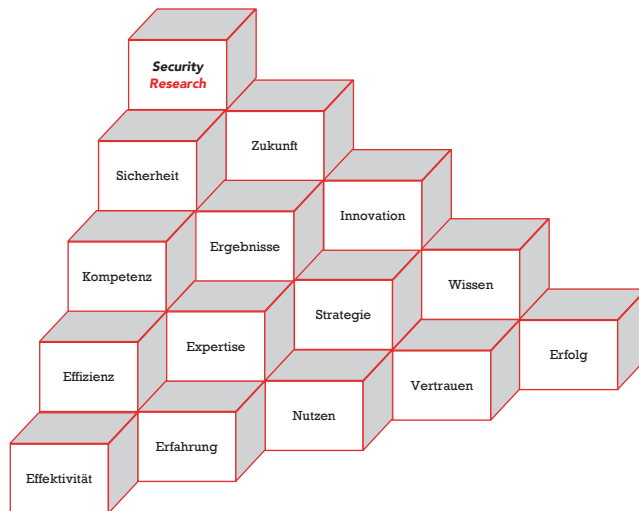
DLP dient zum Aufspüren, Überwachen, Verwalten und Schützen vertraulicher Daten und setzt sich aus vier Modulen zusammen:

Die Module **Discover**, **Monitor** und **Protect** bestehen sowohl aus einer clientseitigen Komponente (endpoint) als auch einer Netzwerkkomponente.

Mit dem **Management**-Modul wird die DLP-Infrastruktur zentral konfiguriert, gesteuert und gewartet.



Mit **Sicherheit** ein guter Partner.



- Prozesssicherheit**
- Softwaresicherheit**
- Organisatorische Sicherheit**
- Technologische Sicherheit**

Menschen

## Kontakt



Office: Sommerpalais Harrach  
Favoritenstraße 16  
A-1040 Wien

Telefon: +43 (1) 503 12 80  
Fax: +43 (1) 503 12 88

Identifizierung gemäß § 14 UGB:  
Firmenname: Security Research  
Sicherheitsforschung GmbH

Firmenbuchnummer: FN271386 y  
Firmenbuchgericht: Handelsgericht Wien

**Audit-based Services**

**IT-Security Services & Microsoft Consulting**

**Software Entwicklung**

Dipl.-Ing.(FH)

**Gerd Brunner**

CISA, Ziviltechniker für IT r.B.

Partner

Mobile: +43 (699) 1 4444 930

gbrunner@securityresearch.at

DI. Mag.

**Andreas Tomek**

CISA, CISSP, CTPS, MCSE, MCITP

Partner

Mobile: +43 (699) 1 1518 148

atomek@securityresearch.at

Mag.

**Markus Klemen**

CISA, CISSP

Partner

Mobile: +43 (644) 41 11 588

mkleme@securityresearch.at

[anfragen@securityresearch.at](mailto:anfragen@securityresearch.at)

