

## > Gefahr für Ihre IT-Sicherheit

Aktuellen Studien und Umfragen zufolge nennen deutsche Unternehmen als Hauptgefahren für ihre IT-Sicherheit:

- Irrtum und Nachlässigkeit der eigenen Mitarbeiter (unbeabsichtigte Fehler),
- Gefährdung durch Malware (Viren, Würmer, etc.),
- Softwaremängel,
- gezielte Angriffe.

Als besonders problematisch neben der unbefriedigenden Sicherheitslage bei mobilen Geräten, Heimarbeitsplätzen und Funknetztechnologien (WLAN, Bluetooth) wird die Angreifbarkeit von Serverdiensten und Extranets empfunden.

## > Folgen von Sicherheitslücken

Die Folgen von Sicherheitslücken können in vielfacher Hinsicht sehr schwerwiegend sein:

- Möglichkeit des unberechtigten Zugriffs auf vertrauliche Daten
- Möglichkeit der Datenmanipulation
- Möglichkeit des Datenverlusts
- gravierender Vertrauens- und Imageverlust
- Kommunikationsausfälle
- damit einhergehend Produktionsausfälle und Lieferengpässe
- rechtliche und finanzielle Konsequenzen (KonTraG, Basel-II)

## > Ihr verlässlicher Partner mtG

Generell macht es für Unternehmen sehr viel Sinn, Sicherheitsdienstleistungen einer neutralen externen Instanz wie der media transfer AG (mtG) zu übertragen.

Ein externer Partner unterliegt nicht der Gefahr der „Betriebsblindheit“, und erreicht zweifellos eine wesentlich höhere Effizienz durch das vorhandene spezifische Fachwissen und die langjährige Erfahrung.

mtG arbeitet bereits seit vielen Jahren als Sicherheitsdienstleister für eine Reihe namhafter Kunden. Neben unserer Fachkompetenz sind Diskretion und eine enge, vertrauensvolle Zusammenarbeit mit IT- oder Fachabteilung unserer Kunden selbstverständlich für uns.

## > Schwachstellenanalysen

Wir spüren Sicherheitslücken in Extranet und Intranet unserer Kunden auf, und geben wertvolle Unterstützung bei der Beseitigung der Schwachstellen.

Es ist notwendig, solche Untersuchungen in regelmäßigen Abständen durchzuführen. Ein IT-System ist keine feste unveränderliche Größe, sondern unterliegt laufender Veränderung durch Einsatz neuer Technologien, Systempatches oder –Upgrades vorhandener Software, Erweiterungen der Funktionalität, Reaktionen auf Sicherheitsvorfälle, usw.. Jede Veränderung kann Auswirkungen auf die Sicherheit des Systems haben.

Besonders wichtig für Sie: Bei unseren Tests bleibt die Integrität Ihres Systems gewährleistet (kein Datenverlust o.ä.).

Unsere Leistungen umfassen:

### >> Black-Box-Tests

Das sind Tests von „außen“, ohne detaillierte Kenntnis über die zu untersuchende Infrastruktur. Es wird versucht, die Sicherheit des untersuchten Systems zu kompromittieren, und insbesondere Sicherheitslücken bei den Serverdiensten/Extranets aufzudecken.

Diese Tests sind ohne Aufwand seitens des Auftraggebers durchführbar. Wir unterscheiden zwei Klassen von Tests:

#### >>> Penetration Tests

- Prüfung von Netzwerkabschottung und Firewall Konfiguration,
- Sammeln von Informationen, die für Angriffe ausgenutzt werden können,
- Angriff von Schwachstellen,
- Dokumentation der Testergebnisse.

#### >>> Sicherheitsprüfung vorhandener Webanwendungen

- Prüfung der Absicherung des Webservers und der Konfiguration,
- Buffer Overflow Attacken,
- Injection Attacken,
- Cross Site Scripting (XSS) Attacken,
- Dokumentation der Prüfungsergebnisse

## >> White-Box-Analysen und -Tests

Hierunter verstehen wir Analysen und Tests, die umfangreiche Kenntnisse über die Netzwerkinfrastruktur und die Applikationen des zu prüfenden Unternehmens voraussetzen.

Diese Art von Untersuchungen erfordern die intensive Mitwirkung des Auftraggebers, da die notwendigen Informationen u.U. nicht vollständig dokumentiert sind bzw. der direkte Zugang zu Systemen von der IT-Abteilung begleitet werden sollte. Nur durch White-Box-Untersuchungen kann beispielsweise die Einhaltung einer Sicherheitspolitik in allen Aspekten, auch den organisatorischen, überprüft werden.

Hiermit sind also höhere Kosten und auch Aufwand seitens des Auftraggebers verbunden. Eine stufenweises Herangehen ist daher sinnvoll. Wir bieten als Standard die beiden Stufen:

### >>> Stufe 1: Kurz-Check

- (grobe) Bestandsaufnahme der Netzwerk- und Applikationsinfrastruktur mit vorhandenen Sicherheitsmechanismen
- Dokumentation der Ergebnisse; Formulierung von Empfehlungen

### >>> Stufe 2: Ausführliche Untersuchung

Aufbauend auf detaillierten Kenntnissen der Netzwerk- und Applikationsinfrastruktur können die Server- und Systemkonfigurationen überprüft werden, um

- unerwünschte oder unerkannte Kommunikationsbeziehungen aufzudecken,
- unerwünschte Zugriffsmöglichkeiten festzustellen,
- Schwachstellen aufzudecken.
- Ggf. kann ein vorhandenes Sicherheitskonzept überprüft, bzw. dessen Überarbeitungsbedarf festgestellt werden.
- Dokumentation der Ergebnisse; Formulierung von Empfehlungen

## > Kontakt

media transfer AG  
Dolivostraße 11  
D-64293 Darmstadt  
Tel: +49 (0) 6151 8193-0  
Fax: +49 (0) 6151 8193-43  
e-mail: [contact@mtg.de](mailto:contact@mtg.de)  
[www.mtg.de](http://www.mtg.de)