IT-Schwachstellen identifizieren und abwehren

IT-Sicherheit im Unternehmen erhöhen

IT-Systeme gewinnen mehr und mehr an Komplexität. Installations- und/oder Konfigurationsfehler solcher IT-Systeme sowie deren komplexe Kommunikationsbeziehungen untereinander unter Nutzung von öffentlichen Netzwerken eröffnen für potentielle Angreifer oftmals sicherheitsrelevante Angriffsmöglichkeiten. Schwachstellenanalysen zielen darauf ab, solche meist unternehmenskritische Angriffsmöglichkeiten zu identifizieren und aus den Ergebnissen Handlungsempfehlungen zu deren Abwehr abzuleiten.

Warum Schwachstellenanalysen?

Der Betrieb einer Firewall und die Installation von Virenscannern zum Schutz des Unternehmensnetzwerks sind grundlegende Maßnahmen, die mittlerweile fast jedes Unternehmen ergriffen hat. Trotzdem kann eine wachsende Anzahl von Sicherheitsvorfällen beobachtet werden. 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 und
- "Datenklau" / Wirtschaftsspionage.

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

Dem gegenüber stehen eine Vielzahl von Gesetzen, Verordnungen und Richtlinien, die die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität sensibler personenbezogener Daten verlangen. Ebenso relevant ist die Sicherung steuer- bzw. handelsrechtlich bedeutsamer Daten sowie die Errichtung einer firmeninternen Risikovorsorge bzw. eines Risikomanagements. Zum Beispiel

- verlangt das Handelsgesetzbuch Sicherung und Schutz vorhandener Informationen im Rahmen eines internen Kontrollsystems;
- verpflichtet das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) den Vorstand von Aktiengesellschaften sowie die Geschäftsführung von GmbHs zur Errichtung eines Risikomanagementsystems;
- betreffen die Verordnungen und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Banken und andere Finanzdienstleister;
- verlangen das Bundesdatenschutzgesetz und EU-Datenschutzrichtlinien die Sicherstellung der Vertraulichkeit bei Erhebung und Verarbeitung personenbezogener Daten;
- fordert das Telekommunikationsgesetz den Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe;
- verpflichtet Basel II Unternehmen zur Messung und Steuerung der operationellen Risiken.

Die Folgen von Sicherheitslücken können in rechtlicher

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

und finanzieller Hinsicht sehr schwerwiegend sein wie

- Möglichkeit des unberechtigten Zugriffs auf vertrauliche Daten,
- Möglichkeit der Datenmanipulation,
- Möglichkeit des Datenverlusts,
- gravierender Vertrauens- und Imageverlust,
- Kommunikationsausfälle,
- damit einhergehend Produktionsausfälle und Lieferengpässe und
- persönliche Haftung des Managements.

Ziel bei der Durchführung von Schwachstellenanalysen ist es, hier Vorsorge zu treffen und die Sicherheit der technischen Systeme sowie ggf. auch der organisatorischen Infrastruktur zu bewerten und bei Bedarf zu erhöhen, bevor ein Schadensfall eintritt.

Und noch eine altbekannte Tatsache: Sicherheit im Unternehmensnetzwerk lässt sich durch eine einmalige Überprüfung nicht dauerhaft herstellen, sondern ist im Gegenteil ein kontinuierlicher Prozess, dem permanent die nötige Aufmerksamkeit geschenkt werden muss. 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. Im Rahmen eines kontinuierlichen Sicherheitsmanagements ist es daher notwendig, Schwachstellenanalysen in regelmäßigen Abständen zu wiederholen - Sicherheitsprozesse & Regeln müssen gelebt werden.

Die Qualifikation von media transfer AG

Generell macht es für Unternehmen sehr viel Sinn, Sicherheitsdienstleistungen einer neutralen externen Instanz wie der media transfer AG (kurz: mtG) zu übertragen. Ein externer Partner ist unvoreingenommen, unterliegt nicht der Gefahr der „Betriebsblindheit“ und erreicht zweifellos eine wesentlich höhere Effizienz durch das vorhandene spezifische Fachwissen und die langjährige Erfahrung.

media transfer AG 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. Die folgenden Referenzen belegen unsere Qualifikation:

media transfer AG ist akkreditierte Prüfstelle für IT-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI): Bundesweit gibt es lediglich 12 dieser Prüfstellen. Damit testiert das BSI die langjährige Sicherheits-Kompetenz unseres Unternehmens. Das anspruchsvolle Zulassungsverfahren dauerte über ein halbes Jahr. In dieser Zeit bewies media transfer AG die fachliche Kompetenz seiner Mitarbeiter und die Wirksamkeit des firmeneigenen Qualitätsmanagements. Damit unterstreicht media transfer AG nachhaltig ihre langjährige Kompetenz als Profi für IT-Sicherheit.

media transfer AG arbeitet bereits seit 1997 als Dienstleister für das Trust Center der Deutschen Telekom (jetzt T-Systems T-TeleSec): In dieser Zeit haben wir im Auftrag der TeleSec zahlreiche CA Dienste realisiert, die die Basis für die Realisierung sicherer Anwendungen wie gesichertes Extranet, sicherer Email-Verkehr, Dateiverschlüsselung usw. bilden.

media transfer AG betreibt seit 2001 im Auftrag von Netz-Betreibern und Geräteherstellern ein VPN Testlabor: In dem VPN Testlabor werden IPSec Geräte namhafter Hersteller auf Sicherheit (z.B. die korrekte Verwendung von Zertifikaten zur Authentifizierung der Geräte beim IPSec Verbindungsaufbau) und Interoperabilität geprüft werden.

media transfer AG sichert als Dienstleister für "Managed Security Services" durch Fernüberwachung und Fernwartung die Verfügbarkeit der Netze ihrer Kunden: Unser Know-How und unsere Erfahrung ermöglichen die Erkennung etwaiger Sicherheitsvorfälle und die sofortige Einleitung geeigneter Maßnahmen. Dabei beachten wir bei der technischen und organisatorischen Umsetzung des Remote Zugangs die gesetzlichen Anforderungen des Bundesdatenschutzgesetzes. Unsere Kunden können währenddessen ihre Arbeitskapazitäten voll und ganz auf ihr Kerngeschäft konzentrieren.

Die Testmethodik

Unsere Testmethodik definieren wir über Testmodule. Die Testmodule umfassen sowohl klassische IP basierte Pene-

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

trationstests als auch weitergehende Tests von Anwendungen (z.B. Filterapplikationen bei Web und Mail, kundenspezifische Internetapplikationen) sowie Sicherheitsanalysen und Audits mit Detailkenntnis des zu prüfenden Netzes. Unsere Testmethodik leiten wir dabei aus den Dokumenten

- BSI2003A Studie: Durchführungskonzept für Penetrationstests; BSI(Hrsg); 2003,
- OWASP Open Web Application Security Project (OWASP) Testing Guide v3.0; OWASP; 2008 und
- OWASP Top 10; The Ten Most Critical Web Application Security Risks; 2010

ab. In der praxisnah gestalteten Studie des BSI werden die folgenden Kriterien für Penetrationstests entwickelt, die sich aber auch auf die übrigen Testmodule anwenden lassen.

Kriterium: Informationsbasis

- Blackbox
- Whitebox

Kriterium: Agressivität

- passiv gescanned
- vorsichtig
- abwägend
- aggressiv

Kriterium: Umfang

- vollständig
- begrenzt
- fokussiert

Kriterium: Vorgehensweise

- verdeckt
- offensichtlich

Kriterium: Technik

- Netzwerkzugang
- sonstige Kommunikation
- physischer Zugang
- Social Engineering

Kriterium: Ausgangspunkt

- von außen
- von innen

Quelle: BSI2003A

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Ein Blackbox-Test simuliert einen realistischen Angriff von außen. Die notwendigen Informationen werden aus Internet Datenquellen oder durch zuvor durchgeführte Scans eruiert. Hierbei ist keinerlei Mitwirkung des Auftraggebers notwendig.

Als Whitebox-Test wird ein Test verstanden, welcher von bestimmten Detailkenntnissen des zu prüfenden Netzwerks ausgeht. So kann z.B. die Struktur der DMZ als bekannt vorausgesetzt werden oder es sind Benutzernamen und deren Rechte bekannt. Alle in einem solchen Test verwendeten Daten werden vom Auftraggeber zur Verfügung gestellt.

Wir kennzeichnen bei jedem unserer Testmodule, ob es als Blackbox- oder Whitebox-Test durchgeführt werden kann. Aggressivität und Testumfang werden mit dem Kunden vor Beginn der Tests abgesprochen. Generell arbeiten wir bei der Vorgehensweise nicht verdeckt; wir raten unseren Kunden dazu, ihre IT-Abteilung von vornherein in die Testpläne einzubeziehen, um eine konstruktive Arbeitsatmosphäre herzustellen.

Techniken des Social Engineering und physische Zutrittsversuche gehören nicht zum Spektrum unserer Dienstleistungen. Unsere Ausrichtung zielt auf die technische Prüfung und Bewertung von IT-Systemen über Netzwerk- und sonstige Kommunikationszugänge. Wir kennzeichnen bei jedem unserer Testmodule, ob es von außerhalb oder von innerhalb des Kundennetzes durchgeführt werden kann.

Die Testmodule

Wir haben unser Leistungsangebot zur Schwachstellenanalyse in Testmodule gegliedert. Erfahren Sie auf den nachfolgenden Seiten mehr über unsere Testmodule.

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Information Gathering"

Abhängigkeit von anderen Modulen:	keine
Info-Basis:	Blackbox (keinerlei Mitarbeit des Auftraggebers verlangt)
Ausgangspunkt:	extern
Beschreibung:	Information Gathering, das Sammeln verfügbarer Informationen über eine bestimmte Firma, stellt den Einstieg in den Arbeitsbereich Netzwerksicherheit dar. Es wird hierbei versucht, so viel als mögliche Informationen jeglicher Art über den Auftraggeber zu erhalten. Dies betrifft z.B. seine Internet Präsenz, die nach außen sichtbare Netzwerkstruktur und die verwendeten Applikationen. Methoden sind z.B. • Abfrage von DNS, Whois, RIPE • Abfrage von Suchmaschinen • Recherche in Newsgroups, Mailinglisten, IRC Foren • Ermittlung von Routing Informationen • Auswertung öffentlich zugänglicher Dokumente und Daten von und über den Kunden • Dokumentation der Ergebnisse
Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Network Transport & Services"

Abhängigkeit von anderen Modulen:	aufbauend auf dem Modul ”Information Gathering” im Fall von Blackbox Test
Info-Basis:	Blackbox oder Whitebox (entsprechende Informationen werden dann vom Kunden geliefert)
Ausgangspunkt:	extern
Beschreibung:	Dieses Testmodul analysiert die Absicherung der mit dem Internet verbundenen Netzwerke (DMZ) und Infrastrukturkomponenten (Router/Switches/Firewall) sowie die Serverdienste. Es deckt den Funktionsumfang der klassischen sog. Penetrationstests ab. Ziel ist es, eine möglichst vollständige Darstellung der Netzwerktopologie, der verwendeten Ports und der dazugehörenden Services zu erhalten. Darauf aufbauend werden vorhandene Schwachstellen und ihre möglichen Implikationen identifiziert und verifiziert. • Suche nach zugänglichen Serverdiensten wie SMTP, DNS, HTTP, FTP, LDAP, News- und Proxyserver, etc. • Prüfung auf Erreichbarkeit und Absicherung kritischer Dienste wie SSH, SNMP, Telnet, VNC, etc. • Analyse von Servern und Infrastrukturkomponenten wie Firewall, Webserver, Router hinsichtlich Software(versionen), Betriebssystemen und Absicherung • Identifikation und Verifikation von Schwachstellen bei den gefundenen Infrastrukturkomponenten und Serverdiensten • Basisprüfung der Mail- und Webfilterfunktionalität (Verfügbarkeit und Absicherung gegen Malware) • Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen Vor Durchführung dieser Tests wird eine komplette Datensicherung empfohlen.
Anmerkung:	Die Verfügbarkeit von Mail und Webdiensten sind von existentieller Bedeutung für die meisten Unternehmen. Das Modul „Networt Transport & Services“ beinhaltet eine Basisprüfung dieser kritischen Anwendungen, die im Rahmen eines externen Tests durchführbar ist. Wir empfehlen für diese kritischen Anwendungen dringend die Durchführung weitergehender Analysen, die wir im Rahmen des Moduls Network Applications in Form von Whitebox Tests anbieten.

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Network Applications"

Abhängigkeit von anderen Modulen:	aufbauend auf dem Modul "Network Transport & Services"
Info-Basis:	Whitebox
Ausgangspunkt:	extern
Beschreibung:	Dieses Testmodul betrachtet im Detail die Sicherheit und Verfügbarkeit von Serverapplikationen, die existentiell für die Kommunikation eines Unternehmens mit der Außenwelt sind. Betrachtet werden neben der Firewall der Web- und Mailzugang sowie VPN Lösungen. Weiterhin kann ein ggf. vorhandenes IDS detailliert untersucht werden. Der Umfang der Untersuchungen wird gemeinsam mit dem Kunden festgelegt. Diese detaillierten Untersuchungen werden vor Ort und „von innen" in Zusammenarbeit mit der IT-Abteilung des Kunden durchgeführt. • Analyse und Test der Konfiguration und Effizienz von Filterapplikationen (Malware/Spam) bei Mail • Analyse und Test der Konfiguration und Effizienz von Filterapplikationen (Malware/Zugriffsrechte) bei Web • DoS Angriffe auf Mailserver • Evaluierung von Firewall Regelsätzen • Sicherheitsanalyse von VPN Lösungen (z.B. Verschlüsselungsstärke, Authentifizierung, Robustheit, saubere Trennung verschiedener Netzwerkinterfaces) • Analyse und Test von Performanz und Sensibilität des IDS • Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen
Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "User Applications"

Abhängigkeit von anderen Modulen:	aufbauend auf dem Modul "Network Transport & Services"
Info-Basis:	Blackbox
Ausgangspunkt:	extern
Beschreibung:	Dieses Testmodul führt eine Untersuchung kundenspezifischer Internetapplikationen hinsichtlich ihrer Verwundbarkeit durch. Wir setzen [OWASP] Methodik und Technologien ein wie zum Beispiel: • Untersuchung der Verzeichnisstruktur bei Webanwendungen • Untersuchung von Formulareingaben, Cookies und Session Keys • Tests hinsichtlich SQL Injection • Tests hinsichtlich Cross Site Scripting (XSS) • Tests hinsichtlich Session Hijacking • Tests hinsichtlich DoS Attacken • Tests hinsichtlich unerlaubter Authentifizierung • Tests hinsichtlich Speicherlöchern • Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen
Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Access Methods/WLAN und Bluetooth"

Abhängigkeit von anderen Modulen:	aufbauend auf dem Modul "Network Transport & Services"
Info-Basis:	überwiegend Whitebox
Ausgangspunkt:	intern und extern
Beschreibung:	Dieses Testmodul analysiert die Absicherung von Funknetzwerkkomponenten (Wireless LAN und Bluetooth). Die Konfiguration und Sicherheit der Clients wird in einem weiteren Schritt überprüft.

- Suche und Dokumentation erreichbarer Funkzellen ("Wardriving", SSID-Scanning)
- passive Analyse der eingesetzten Verschlüsselungs- und Authentifizierungsverfahren (WEP, WPA, MAC) auf Verwundbarkeit
- Analyse der Konfiguration von Funknetzwerkkomponenten ("Open Authentication", SSID-Broadcast, WPA, MAC-Filterung, "any"-SSID, SNMP)
- Analyse der infrastrukturellen Einbindung von Funknetzwerkkomponenten (Router, Switch/Hub, VPN)
- weitere Angriffe: Session Hijacking, Client-Catching, ARP-Spoofing, MAC-Spoofing, Jamming (DoS)
- Analyse der Konfiguration mobiler Rechner (Laptops, PDAs) hinsichtlich Absicherung von WLAN-Keys, etc.
- Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen

Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Kurz-Check"

Abhängigkeit von anderen Modulen:	keine
Info-Basis:	Whitebox
Ausgangspunkt:	intern
Beschreibung:	Dieses Modul beinhaltet eine grobe Bestandsaufnahme der Netzwerk- und Applikationsinfrastruktur des Kunden einschließlich der vorhandenen Sicherheitsmechanismen. Diese Arbeit wird vor Ort und „von innen“ in Zusammenarbeit mit der IT-Abteilung des Kunden durchgeführt. • Sichtung vorhandener Netzpläne und Dokumentationen der Netzwerk- und Applikationsinfrastruktur • Durchführung von Interviews mit Mitarbeitern der IT-Abteilung zur Bestandsaufnahme des Ist-Zustands. • Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen
Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Testmodul "Ausführliche Interne Sicherheitsanalyse"

Abhängigkeit von anderen Modulen:	keine
Info-Basis:	Whitebox
Ausgangspunkt:	intern
Beschreibung:	Dieses Testmodul analysiert, welche Auswirkungen eine etwaige Überwindung der Schutzvorrichtungen von außen hätte bzw. welche Kommunikationsbeziehungen innerhalb des Intranets bestehen. Diese Arbeit wird vor Ort und „von innen“ in Zusammenarbeit mit der IT-Abteilung des Kunden durchgeführt. Der genaue Umfang und Fokus der Untersuchungen wird gemeinsam mit dem Kunden festgelegt. Möglich sind: • Durchführung von Penetrationstests „von innen“ • Aufdeckung unerwünschter oder unerkannter Kommunikationsbeziehungen (z.B. Zugriffsmöglichkeiten auf vertrauliche Informationen) • Untersuchung der Passwortgüte • Überprüfung des Datensicherungskonzepts • Überprüfung der Ausfallsicherheitskonzepte • Review und Verifikation vorhandener Sicherheitsrichtlinien • Review und Verifikation vorhandener Notfallpläne • Dokumentation der Ergebnisse und Formulierung von Empfehlungen zur Elimination evtl. vorhandener Schwachstellen
Anmerkungen:	keine

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde

Die Testwerkzeuge

Bei unseren Tests kommen je nach Testmodul eine Vielzahl von Werkzeugen meist auf Open Source Basis zum Einsatz. Wir setzen hierbei bewußt Open Source Werkzeuge mit offengelegtem und nachprüfbarem Source Code ein, um jederzeit die volle Kontrolle über die Tests zu haben. Hierbei ist es neben detaillierter Kenntnis der Werkzeuge und ihrer vielfältigen Konfigurationsoptionen erforderlich, jeweils die neuesten Versionen und aktuellsten Updates vorzuhalten. Mit dem Einsatz von im Internet verfügbaren Tools alleine lässt sich jedoch die komplexe Welt der Netzwerke und Applikationen nicht durchdringen. Erfahrung, Phantasie und tiefgehendes technisches Know-How sind gefragt, um sich Schritt für Schritt voran zu tasten und vorhandene Schwachstellen tatsächlich aufzudecken. Bei Bedarf werden eigene Testprogramme und Skripte zur Testautomation maßgeschneidert von uns entwickelt.

Die Testdokumentation

Wir liefern bei Bedarf eine vollständige Protokollierung der durchgeführten Tests mit Datum/Uhrzeit und der Art der Aktionen, damit alle Tests dem Kunden nachvollziehbar sind. Weiterhin erstellen wir eine Zusammenfassung der wesentlichen Ergebnisse und sprechen Empfehlungen zur Elimination evtl. vorhandener Schwachstellen aus.

Der Ablauf

In der Regel läuft eine Testkampagne folgendermaßen ab:

Zunächst erfolgt ein Gespräch mit dem Kunden mit folgenden Inhalten:

- Vorstellung der Testmodule im Überblick
- Ermittlung der Ziele des Auftraggebers
- Selektion der relevanten Module und Besprechung des Vorgehens und der möglichen Risiken
- Benennung eines fachlichen Ansprechpartners beim Kunden
- grobe Abstimmung des Testzeitraums

Bei Bedarf kann dies auch im Rahmen einer Telefonkonferenz geschehen.

Nächster Schritt ist die Vorlage des Angebots durch media transfer AG zusammen mit den allgemeinen Geschäftsbedingungen für die Durchführung von Schwachstellenanalysen. Nach Eingang von Auftrag und durch den Kunden unterzeichneter Einverständniserklärung für die Tests erfolgt die Abstimmung von genauen Terminen/Zeiten mit dem Ansprechpartner. Je nach Art der ausgewählten Module ist vom Kunden vorab eine Datensicherung durchzuführen. Die vereinbarten Tests werden durchgeführt und die Dokumentation erstellt. Es erfolgt die Übersendung der Dokumentation und auf Kundenanforderung eine Abschlusspräsentation der Ergebnisse und Empfehlungen.

Die Randbedingungen

Wir arbeiten nur mit schriftlichem Einverständnis unserer Kunden, unter klar definierten Allgemeinen Geschäftsbedingungen und unter Beachtung des "Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB (sog. Hackerparagraph)"des BITKOM aus dem Jahr 2008. Alle unsere Mitarbeiter, die an der Durchführung von Schwachstellenanalysen beteiligt sind, sind bei media transfer AG fest angestellt. Sie sind auf absolute Vertraulichkeit im Umgang mit den Daten und Testergebnissen unserer Kunden verpflichtet. Wir gehen davon aus, dass auf unsere Tests nicht mit einer Blockierung unserer IP-Adresse reagiert wird. Wir ergreifen im Normalfall keine Vorkehrungen, um unsere Angriffe zu tarnen. Gegebenenfalls ist es empfehlenswert, den ISP des Kunden vorab zu informieren (je nach geplanter Testinfrastruktur). Bei Untersuchungen im Intranet des Kunden (z.B. Traffic-Analysen, Protokollierung von Nutzdaten oder Passworten in diesem Zusammenhang) gehen wir davon aus, dass der Kunde die ggf. erforderliche Unterrichtung der Mitarbeiter bzw. des Betriebsrats vornimmt.

Kontakt
media transfer AG

Tel: +49 6151 8193-12
contact@mtg.de

media transfer AG
Dolivostrasse 11
64293 Darmstadt

Telefon: +49 6151 8193-0
Telefax: +49 6151 8193-43
Web: http://www.mtg.de

Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.),Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde