> 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.

> Schutz vor Malware und Spam

Im ersten Halbjahr 2004 wurden mehr als 5.000 neue Windows Viren- und Würmer registriert, ca. viereinhalb mal soviel wie im Vorjahreszeitraum. Bedenkt man gleichzeitig den angerichteten wirtschaftlichen Schaden in Form von System- und damit verbundenen Produktionsausfällen, ist wirkungsvoller Schutz vor Malware ein absolutes Muss.

Das Thema Spam gestaltet sich ebenso unerfreulich: ein durch die IETF oder andere Gremien standardisiertes Verfahren zur Überprüfung von Mailabsendern ist bislang nicht in Sicht.

Maßnahmen zur wirkungsvollen Abwehr von Malware und Spam tun also dringend not. Sie sind stark von der eingesetzten Server Software abhängig. mtG ist auf LINUX/UNIX Umgebungen mit frei verfügbaren Open Source Komponenten spezialisiert. Hier sind sehr kostengünstige Lösungen möglich, die aber auch spezifisches Know-How erfordern.

Auch wenn Sie mit Ihrer Serverinfrastruktur einen Umstieg zu Open Source Lösungen beabsichtigen, sind wir der richtige Partner und beraten Sie kompetent und zuverlässig bei Lösungen und Migrationswegen.

Selbstverständlich leisten wir aber auch wertvolle Hilfestellung im Fall von Windows basierten Umgebungen.

Unsere Konzepte und Maßnahmen umfassen:

>> Abwehr von E-Mail Spam/Viren- und Würmerschutz bei E-Mail

Eine mehrstufige Vorgehensweise bietet zuverlässigen Schutz vor unerwünschten oder gefährlichen Mails:

- Spezifische Mail Server Konfiguration zur Spam Abwehr
- Serverseitiges Online Content Filtering empfangener Mails nach verschiedenen definierbaren Kriterien (dient der Abwehr von Spam und Schutz vor Malware)
- Serverseitige automatische Speicherung und Scan der Mail Attachments (Schutz vor Malware)

Diese Maßnahmen werden nicht nur einmalig angewendet, sondern ihre Auswirkungen z.B. auf die Systemperformanz müssen beobachtet, und ggf. justiert werden. Auch sind die Filterkriterien in regelmäßigen Abständen zu überprüfen und ggf. zu erweitern.

>> Viren- und Würmerschutz allgemein

Generell ist der konsequente Einsatz von Virenscannern auf zentralen Serverkomponenten und auf Arbeitsplatzrechnern und mobilen Endgeräten unerlässlich. Zeitnahe Updates sind zwingend erforderlich.

Wir helfen bei der notwendigen Etablierung von Verfahren zum automatisierten Update der Arbeitsplatzrechner. Nur so ist die Integrität Ihrer Büroarbeitsplätze sicherzustellen.

Weiterhin beraten wir hinsichtlich der sicheren Konfiguration mobiler Devices (Laptops, Pocket PCs, usw.), die ein Haupteinfallstor für Malware in Firmennetze darstellen.

>> Kontrollierte Internet Nutzung/Content Security

Um ein wirkungsvolles Content Filtering zum Schutz vor Malware und gleichzeitig eine kontrollierte Internetnutzung zu erreichen, empfehlen wir den Einsatz eines Proxy Servers, der als Application Level Firewall fungiert.

Durch die klassische Firewall wird eine Paketfilterung auf IP Ebene durchgeführt. Gefährliche Inhalte lassen sich dadurch leider nicht erkennen. Eine Application-Level Firewall löst dieses Problem, und ist in der Lage,

- Verbindungen zu unerwünschten Webseiten zu unterbinden,
- Web Inhalte nach definierbaren Regeln zu filtern (z.B. Prüfung Datentypen und Dateigrößen von herunter geladenen Dateien oder Inhalte von Webseiten),
- sämtliche Internetzugriffe zu protokollieren.

> 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
www.mtg.de