

Security Policy

PowerWeb Hosting (Stand 1.2.2008)

PHADE Software

Inh. Dipl.-Inform. Frank Gadegast
Schinkelstraße 17
14558 Nuthetal OT Rehbrücke
Germany

Kommunikation

Fon + 49 33200 52920
Fax + 49 33200 52921

Internet

eMail : vertrieb@powerweb.de
eMail : info@powerweb.de
Surf : <http://www.powerweb.de>

Bankverbindung

Berliner Bank AG
BLZ 100 708 48
Konto 466001500

Sicherheit ist ein sehr wichtiger Aspekt bei sog. Hosting von Webinhalten, eMail und anderen Applikationen (Application Service Providing). Erfahrungsgemäß ist der Sicherheitsstandard bei professionellen Providern deutlich höher als bei kleineren Firmen und beim Endkunden, wenn dieser z.B. eigene Server betreibt.

PHADE Software hat sich mit seinem schon seit vielen Jahren erfolgreichem Produkt "PowerWeb" im Markt profiliert, insbesondere weil wir uns mit dem Problem der Datensicherheit genau befaßt haben.

Ausfallsicherheit Hardware:

Bei allen PowerWeb-Hosting-Produkten werden Hochleistungsserver von Sun Microsystems mit redundanten CPUs, redundanter Ethernetanbindung und redundanten Netzteilen eingesetzt. Bei PC-basierten Systemen (werden nur auf Wunsch des Kunden eingesetzt) sind mindestens die Netzteile redundant ausgelegt. Ein Ausfall der einzelnen Komponenten bedarf keinen Neustart der Server. Ersatzserver sind jeweils vor Ort vorhanden.

Ausfallsicherheit Speichersystem:

Alle Server sind mit einem eigenen, physikalisch getrennten RAID-Speichersystem (RAID Level 5 bzw. 6) ausgerüstet, ein Ausfall von einzelnen Festplatten bedeutet weder Datenverlust noch eine Betriebsunterbrechung. Da insbesondere alle Daten auf den RAID-Systemen liegen, kann im Notfall der komplette Server getauscht und das System vom RAID-System neu gestartet werden, so sind selbst komplett ausgefallene Server leicht zu ersetzen.

Raumschutz:

Alle Server stehen in entsprechend ausgestatteten Serverräumen unserer Backboneprovider in Frankfurt und Berlin. Notstrom, Unterbrechungsfreie Stromversorgungen, Notlöschanlagen und Klimaschutz sind dort vorhanden. Der Zugang zu den Räumen ist nur einem kleinen Personenkreis vorbehalten.

Router:

Verbunden sind alle Server mit Routern des Branchenführers Cisco. Diese Router fungieren auch als vorgeschaltete Firewall, so können Datenströme vor den Servern kanalisiert, überwacht und blockiert werden. Insbesondere ist hier der Schutz vor Attacken per ICMP, ECHO, DoS und DDoS implementiert. PHADE Software wurde bereits mehrfach attackiert, bei diesen Attacken konnte schnell reagiert werden, die Auswirkungen für den Betrieb der Server waren ausnahmslos gering.

Betriebssysteme:

Eingesetzt werden ausschließlich UNIX-Betriebssysteme, die dank Ihres Multi-User und Multi-Processsystems nur schwer von aussen angreifbar sind. Der entsprechende Root-Zugriff ist über die Firewall nur wenigen Personen möglich und ausschließlich über verschlüsselte Datenkanäle möglich. Das Betriebssystem Solaris von SUN Microsystems wird regelmäßig (im laufenden Betrieb) mit Updates versorgt, die allerdings zumeist nur die Fähigkeiten erweitern. Sicherheitslücken sind in den letzten Monaten nicht bekannt geworden. Das Betriebssystem Linux wird nicht mehr auf aktuellere Version geändert (was neue Sicherheitslücken ergeben könnte), die jetzt bei PHADE Software eingesetzte Version gilt als absolut sicher und stabil.

Services:

PHADE Software hat mehrere Mechanismen installiert, die die Server vor unberechtigter Nutzung schützen. eMail kann nur von berechtigten Usern bzw. deren Domains aus genutzt werden. Methoden zur Verschlüsselung können kostenfrei genutzt werden (SSL). Scripte werden in getrennten Bereichen abgelegt und können dank des Multi-User-Konzepts der UNIX-Betriebssysteme nur auf festgelegte Bereiche und Applikationen zugreifen. Eine Verschlüsselung des Zugriffs der berechtigten User per FTP ist auf Wunsch möglich. Datenbankzugriff ist nur berechtigten Usern von berechtigten IP-Adressen aus erlaubt. Alle Service werden von unabhängigen Servern und Routern überwacht und analysiert, die dauernde Verfügbarkeit einzelner Dienste bzw. deren eventueller Ausfall wird angezeigt und teilweise automatisch behoben (Watchdog/Heartbeat-Funktionen).

Eine Anti-Viren-Lösung ist im eMail-Bereich ist installiert, um die Weiterverteilung über bei PowerWeb eingerichtete Mailboxen zu verhindern, die eingesetzten Systeme selber sind nicht anfällig für Viren.

Java bzw. Scriptkomponenten, die vom Kunden installiert werden laufen teilweise in getrennten Umgebungen (Sandbox), die dem System an sich nicht gefährlich werden können.

Backup:

Datenbankinhalte und Logdateien werden täglich auf Massenspeicher bzw. Band gesichert, um z.B. versehentlich gelöschte Kundendaten wieder herstellen und Straftaten oder unberechtigte Nutzung nachweisen zu können. Täglich werden auf allen Servern die während des letzten Tages geänderten Daten archiviert und auf die Server übertragen, die mit Backupsystemen (z.B. DAT-Laufwerken) ausgerüstet sind. Diese täglichen "Unterschiede" werden 14 Tage aufbewahrt. Alle Server werden komplett alle 7 Tage gesichert.

Beratung:

Da PHADE Software Logfiles auswertet und die Server dauernd überwacht, kann der Endkunden auf eventuelle Sicherheitsprobleme seiner eigenen Software hingewiesen und beraten werden.