

## E-Business-Sicherheit – Ein Thema, das immer mehr an Bedeutung gewinnt



cirosec GmbH  
Jörg-Ratgeb-Platz 3  
74081 Heilbronn  
Tel.: 07131 / 59455-60  
Fax: 07131 / 59455-99  
www.cirosec.de

Firewalls, Content-Security, Intrusion Detection und andere Sicherheitsmechanismen gelten als etabliert und beinahe schon klassisch. Selbst wenn noch bei weitem nicht alle Organisationen vernünftige Firewalls implementiert haben, ist das Verständnis, dass Firewalls ein nötiger Grundschutz sind, allgemein akzeptiert.

Dennoch sind erfolgreiche Hackerangriffe an der Tagesordnung und nicht selten werden Webserver von Firmen gehackt, die durchaus Firewalls einsetzen. In Hacker-Kreisen spricht man davon, dass mindestens jeder zweite Webserver manipuliert werden kann. Bei Untersuchungen von Sicherheitsfirmen werden sogar noch größere Prozentzahlen ermittelt. Die Frage liegt also nahe, ob Firewalls und andere klassische Komponenten der Netzwerksicherheit überhaupt einen wirksamen Schutz von Webservern und damit für E-Business-Systeme herstellen können.

Es ist eindeutig, dass heute vor allem Webserver das primäre Angriffsziel im Internet sind. Einerseits weil Webserver für jedermann erreichbar sind, und andererseits weil Webserver häufig Schwachstellen enthalten und so „dankbare“ Opfer sind. Webserver sind die Eingangsportale in die Firmen - Nicht nur aus Anwendungs- und Marketingsicht, sondern auch aus Sicht der Hacker. Gleichzeitig steigt die Bedeutung dieser Server für die Firmen. Während es noch vor ein paar Jahren als netter Luxus galt, einen Internet-Auftritt zu haben, so ist dies heute für viele Firmen unverzichtbar geworden. Einzelne Reiseveranstalter berichten, dass sie bereits über 50% ihrer Anfragen über das Internet bekommen. Versandhäuser wickeln bereits einen nicht unerheblichen Teil ihrer Geschäfte über das Internet ab, von reinen E-Business Anbietern wie Amazon ganz zu schweigen. Die eigentliche Gefahr, die von einem echten E-Business System ausgeht wird häufig nicht wahrgenommen. Bei oberflächlicher Betrachtung ist das Risiko nur der Verlust des Web-Auftritts und eventueller öffentlicher Daten auf dem Webserver selbst. Was dabei vergessen wird sind die Kommunikationsbeziehungen des Webserver zu internen Systemen. Gerade E-Business Systeme müssen mit internen Servern, Datenbanken oder Hosts kommunizieren und diese Verbindung kann ein Hacker angreifen.

Aus der Frage nach der Sicherheit eines Webserver wird damit sofort die Frage nach der Sicherheit des internen Netzes, aller darin operierenden Server und ihrer Daten. All diese Sachverhalte und Argumente sprechen dafür, dem Sicherheitsaspekt bei E-Business besondere Aufmerksamkeit zu schenken. Viele Annahmen aus den vergangenen Jahren treffen in der Zeit von E-Business nicht mehr zu und die bisherigen Schutzmechanismen sind kein wirksamer Schutz für moderne E-Business Systeme. Es ist daher nötig, die Angriffsmöglichkeiten und potentielle Technologien zu deren Abwehr gegenüber zu stellen und neue Konzepte für den wirksamen Schutz zu entwickeln.

Dies bedeutet nicht, dass Firewalls oder Intrusion Detection Systeme immer wirkungslos oder unsinnig sind. Sie adressieren nur ein anderes Problem und schützen vor anderen Gefahren.

Für eine durchgängige Sicherheit sind beide Seiten nötig. Firewalls, Content Security, Verschlüsselung und Authentisierung sind wichtige Mechanismen, die vor etablierten und immer noch aktuellen direkten Angriffen auf interne Netze schützen. E-Business Systeme bringen neue Angriffsmöglichkeiten und Risiken mit sich, die zusätzliche Mechanismen nötig machen, damit die klassischen Sicherheits-Installationen nicht untergraben werden.

*Stefan Strobel, Geschäftsführer der cirosec GmbH*