Sichere
eBusiness Lösungen

Informationssicherheit

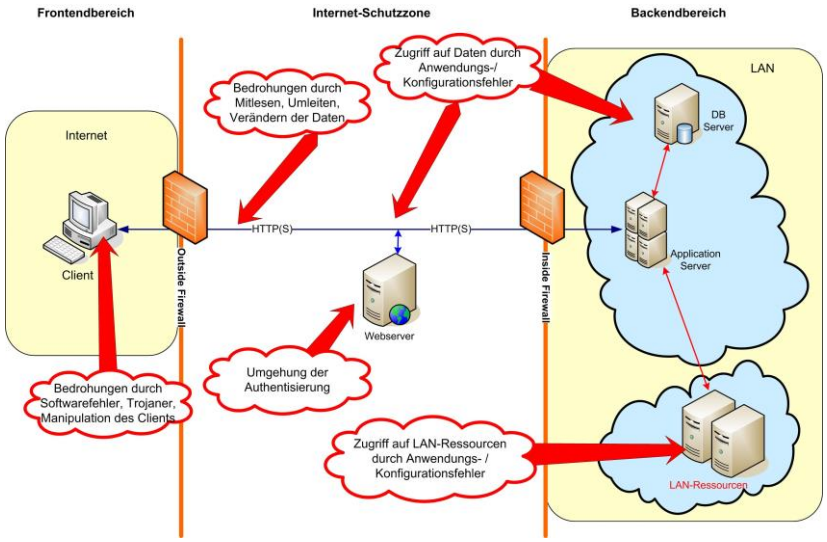
Überprüfung von Webanwendungen

Bedrohungen von Webanwendungen

Mit der zunehmenden Bereitstellung von Webanwendungen, die über das Internet Kunden oder auch Mitarbeitern einen einfachen Zugriff auf bereit gestellte Geschäftsvorgänge und Daten ermöglichen, sind auch beachtenswerte Sicherheitsrisiken verbunden.

Herkömmliche Sicherheitskomponenten wie Firewalls haben ihre Stärken in der Kontrolle auf Netzebene, können aber auf Anwendungsebene bestenfalls offensichtliche und wohlbekannte Angriffe erkennen. Angriffe neuerer Art zielen über Buffer-Overflows, SQL-Injection oder Cross-Site-Scripting aber eher auf auszunutzende Schwächen innerhalb einer Anwendung und sind damit nur schwer zu verhindern.

Häufigste Schwachstellen sind die unzureichende Prüfung von Nutzereingaben und die ungefilterte Anzeige von Fehlermeldungen, die oft wichtige Informationen für einen Angreifer enthalten. Da Entwickler in aller Regel deutlich mehr Aufwand auf Funktionalität als auf Sicherheit legen, bieten sich einem Angreifer oft sehr gute Möglichkeiten über die Anwendung auf Firmen- und Nutzerdaten oder gar das Basissystem selber zuzugreifen.



Lässt sich manipulierter Code auf einem Web- oder Web-Application-Server einschleusen, kann hierüber sogar der externe Nutzer angegriffen werden. Zumindest der Imageschaden für das hierfür verantwortliche Unternehmen wäre gewaltig. Der Betreiber solcher Webanwendungen wird die Details der Programmierung selber kaum kennen und wiegt sich oft in trügerischer Sicherheit.
Nur durch einen kombinierten Einsatz von Security-Scannern und manueller Inspektion lassen sich vorhandene Schwachstellen ermitteln und Gegenmaßnahmen einleiten.

Vorgehen bei einer Sicherheitsüberprüfung

Bei der Sicherheitsüberprüfung von Webanwendungen wird mit zwei Testszenarien gearbeitet:
Basis-Test: Es wird ein externer Blackbox-Test durchgeführt. Hierbei verhalten sich die Prüfer wie Angreifer, die neben der URL der Webanwendung über keine weiteren Informationen verfügen. Sie versuchen über identifizierte Schwachstellen auf Nutzer- oder Firmendaten zuzugreifen oder unberechtigten Zugang auf Systemebene zu erlangen. Bieten sich Möglichkeiten zum Eindringen in geschützte Netzbereiche (DMZ, LAN) werden diese erst nach Abstimmung mit dem Auftraggeber wahrgenommen.

Nutzer-Test: Es wird eine vorher zur Verfügung gestellte Zugangsberechtigung verwendet, um Prüfungen direkt auf Anwendungsebene vornehmen zu können. Ziel ist es, andere Sitzungs- und Nutzerdaten einzusehen, zu manipulieren oder aus der Anwendungsumgebung auszubrechen und auf Systemebene zu gelangen. Bieten sich Möglichkeiten zum Eindringen in geschützte Netzbereiche (DMZ, LAN) werden diese erst nach Abstimmung mit dem Auftraggeber wahrgenommen.

Die Überprüfungen umfassen im Wesentlichen:

- Tests mit manipulierten Eingabedaten
- Tests mit manipulierten Eingabeparametern
- Code-Analyse von Webseiten
- Angriffe gegen Nutzerverbindungen
- Analyse der Zugriffssicherung
- Analyse der eingesetzten Verschlüsselung
- Prüfung der zugänglichen Web Directory-Struktur

GAI NetConsult GmbH, Am Borsigturm 58, 13507 Berlin, Tel: 030-417 898-0, Fax: 030-417 898-300
E-Mail: vertrieb@gai-netconsult.de Internet: http://www.gai-netconsult.de