Wie funktionieren Internet-Firewalls?

Das Internet ist zunehmend der Dreh- und Angelpunkt für viele Unternehmen geworden. Internet-Firewalls sollen zum Schutz vor Angreifern (Hacker) in das private Unternehmens-Netzwerk dienen. Unser Autor Thomas Burgard gibt eine detaillierte Einführung in das komplexe Thema Internet-Firewalls.

Einführung

Das öffentliche Netzwerk „Internet" dient immer mehr als Kommunikations-, Handels- und Marketing-Plattform für Unternehmen aller Branchen. Das bedeutet aber auch, dass die Computersysteme im privaten Unternehmensnetzwerk (auch als Local Area Network, kurz LAN, bezeichnet) mit dem Internet verbunden sind. Genau das ist die Schwachstelle, die von Hackern zum Eindringen in das lokale Netz ausgenutzt wird, wenn keine Vorsichtsmaßnahmen dagegen getroffen wurden.

Die IT-Sicherheit ist in der letzten Zeit immer mehr zu einem sehr wichtigen und zentralen Thema für Unternehmen geworden, die das öffentliche Internet für Kommunikations-, Handels- und Marketingzwecke benötigen. Immer mehr Hackerangriffe werden gemeldet und immer mehr Unternehmen sind technisch hochkomplexen Hackerangriffen ausgesetzt.

Man muss dazu sagen, dass die meisten Angriffe aus verschiedenen Gründen (z. B. Imageverlust) gar nicht gemeldet werden. Es kommt noch viel schlimmer: Viele Unternehmen, vornehmlich kleine Unternehmen, Selbstständige und Freiberufler investieren wenig bis gar nichts für die Sicherheit der eigenen IT-Infrastruktur. Immer wieder werden die gleichen Argumente wie: „Wir sind zu klein", „Was soll denn schon passieren", „Uns passiert schon nichts", „Keine Zeit", „Kein Budget", „Kein Know-how" vorgeschoben.

Ist aber ein erfolgreicher Angriff von außen auf das lokale Unternehmens-Netzwerk durchgeführt worden, kann der Schaden und die dadurch entstandenen Kosten sehr groß bis katastrophal sein und kann sogar die Insolvenz für ein Unternehmen bedeuten.

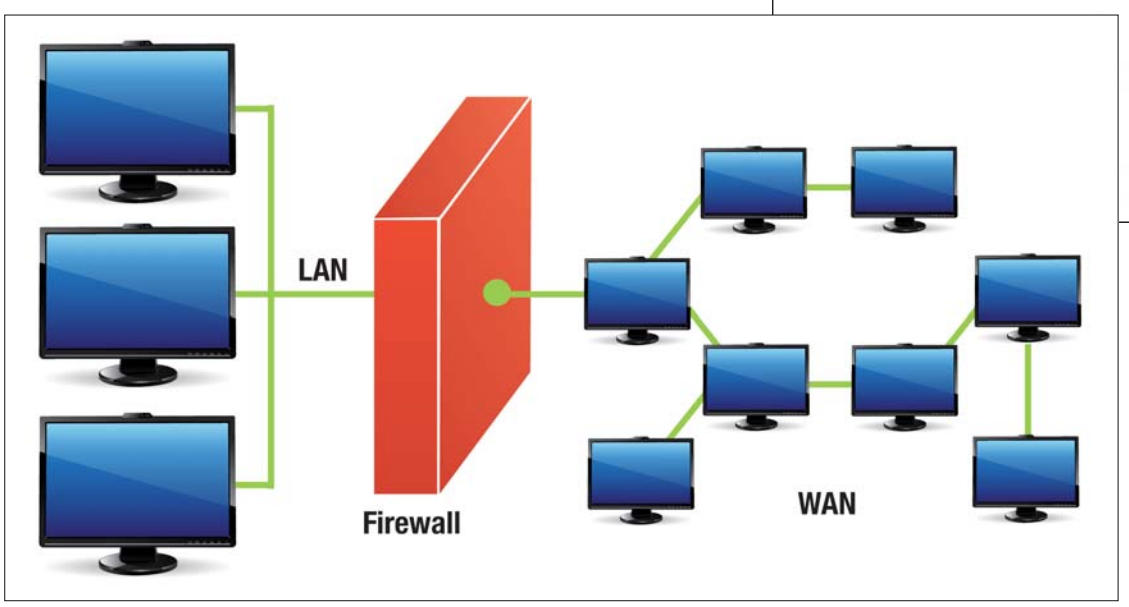

Abb. 1: Einfaches externes Firewall-Konzept.

Faustregel: Die IT-Sicherheit steht an oberster Stelle, sobald das private Unternehmens-Netzwerk mit dem öffentlichen Internet verbunden ist.

Sogenannte Firewall- bzw. Internet-Firewall-Systeme schützen private Netzwerke vor unerwünschten Zugriffen von außen. Firewall ist ein englisches Wort und bedeutet ins Deutsche übersetzt „Feuerwand". In der Tat bildet eine Firewall eine Schutzmauer, die schützend zwischen zwei Netzwerken fungiert, so wie eine Gebäude-Brandschutzmauer zwei Gebäude vor Feuerübertritt schützt.

Die Internet-Firewall gibt es in zwei Ausprägungen:

- Firewall-Software für den Arbeitsplatz-Computer, auch als „Personal Firewall" bezeichnet. Kennzeichen: Die Firewall-Software läuft direkt auf dem zu schützenden System.
- Spezielle Firewall-Systeme als Hard- und Softwarelösung, die wiederum unterschiedliche Teilbereiche abdecken (wird später noch genauer erklärt). Kennzeichen: Die Firewall-Software läuft nicht auf dem zu schützenden System, sondern auf einem externen Firewall-Rechnersystem (Abb. 1).

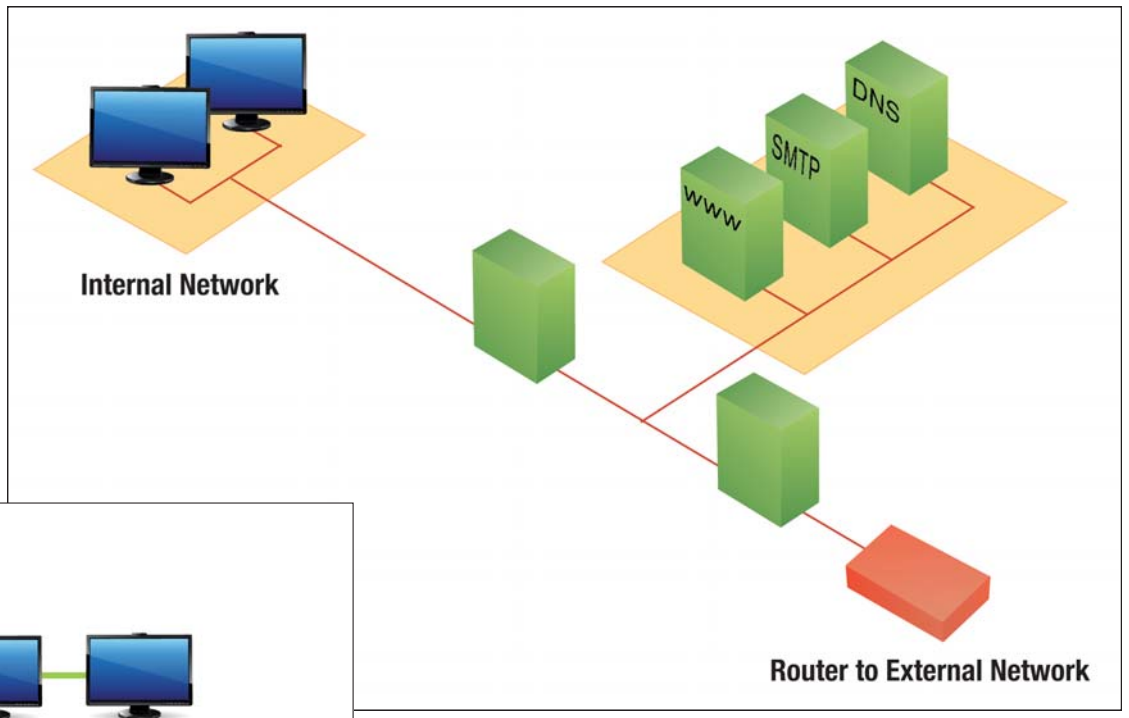

Abb. 2: DMZ als zweistufiges Firewall-Konzept.

Was ist eine Internet-Firewall genau?

Die Daten im privaten Netzwerk und im Internet werden in Pakete aufgeteilt und dann versendet. Der Empfänger bekommt die Datenpakete und muss diese dann wieder in einen kontinuierlichen Datenstrom (mit der korrekten Reihenfolge) zusammenbauen. Damit die Anfrage nicht im Internet verloren geht, werden in diesen Paketen (im Header) die Absender- und Empfänger-Daten gespeichert (z. B. TCP/IP-Adresse, die vom Provider vergeben wurde). Dadurch ist es aber auch möglich, dass Hacker die gespeicherten Adressdaten lesen und für böswillige Angriffe verwenden. Zum Beispiel könnte ein Angreifer manipulierte Datenpakete mit der gelesenen IP-Adresse auf einem nicht verwendeten und offenen Port (Hausnummer eines Dienstes, z. B. hat der HTTP-Dienst des WWW die Portnummer 80) des Zielrechners senden und somit Zugang zum Zielrechner bekommen. Hat der Angreifer erst einmal den Zugang bekommen, können die in den manipulierten Datenpaketen enthaltenen Angreifer-Daten (z. B. wird ein Trojaner mit eingeschleust) dann meist unbemerkt bösen Schaden anrichten.

Wie schon weiter oben beschrieben, soll eine Firewall ein privates Computer-Netzwerk vor unerwünschten Zugriffen von außen schützen. Anders ausgedrückt: Eine Firewall verbindet (Gateway-Funktion) ein

privates Computer-Netzwerk mit dem öffentlichen und prinzipiell „unsicheren“ Internet und ermöglicht zusätzlich eine konfigurierbare Zugangskontrolle (Torwächter) über sogenannte

Filter bzw. **Packet-Filter**. Die Datenpakete, die von außen zur Firewall gelangen, werden mit konfigurierbaren Regeln verglichen. Erfüllt ein Datenpaket nicht die vorgegebenen Bedingungen, wird es verworfen und kann den Zielrechner im privaten Netzwerk dann nicht erreichen. Außer den Filtern gibt es noch als weiteren Bestandteil der Firewall die sogenannten **Application-Gateway**, mit denen man die Nutzdaten der Dienste (z.B. die Nutzdaten in einer E-Mail-Nachricht) analysieren kann. Es sei an dieser Stelle deutlich gesagt, dass eine Firewall nur eine Maßnahme von vielen für ein Unternehmen darstellen sollte. Eine Firewall als einziger Baustein in einem Sicherheitskonzept ist wenig sinnvoll.

Welche Anforderungen muss eine Internet-Firewall als Sicherheitsbaustein erfüllen und welche Funktionen sollten somit enthalten sein?

- **Gateway** zwischen dem zu schützenden Netzwerk (privates Netzwerk) und dem Internet (öffentliches Netzwerk) und stellt somit eine Netztrennung dar.
- **Konfigurierbare Filter** erlauben das Prüfen auf bestimmte Bedingungen in den Datenpaketen.
- **UTM (**Unified **T**hreat **M**anagement) vereint eine Vielzahl von unterschiedlichen Sicherheitsfunktionen auf einer gemeinsamen Plattform:
  - **IDS** (**I**ntrusion **D**etection **S**ystem) & **IPS** (**I**ntrusion **P**revention **S**ystem) Ein **IDS** ist eine Art Alarmanlage für Netzwerke. Es dient zur Filterung und Erkennung von böswilligen und potenziell gefährlichen Zugriffen. Ein IPS überwacht die eingehenden und ausgehenden Datenpakete.
  - **VPN** (**V**irtual **P**rivate **N**etwork) Zum Datenaustausch über öffentliche Netze werden die Pakete mittels Packet-Filter verschlüsselt. Man spricht hier auch von einem „Tunnel“ bzw. „die Verbindung ist getunnelt“.
  - **Antivirus/Antispam** Diese Firewall-Komponente prüft die Daten auf Viren und Spams.
  - **Proxy-Funktion** Eine Proxy-Firewall arbeitet als „Stellvertreter“ zwischen dem Quell- und Zielsystem. Neben der Firewall-Funktion kann der Proxy gleichzeitig auch Cache-Funktionen übernehmen. Da hierbei die Firewall selbst als Kommunikationspartner fungiert, können die Datenpakete analysiert werden.
  - **Web-Filter** Die Web-Filter-Komponente überprüft eingehende Web-Datenpakte aus dem http-Protokoll. Zum Beispiel können die URL's überprüft werden.
  - **Layer7-Filter** Diese Filterfunktionen laufen auf der obersten Schicht und somit auf der „Anwendungsschicht“. Diese Funktion wird auch als **Application-Gateway** bezeichnet. Es werden z.B. Authentisierungsinformationen überprüft.
- **Reporting & Statistik** ermöglicht eine gezielte Auswertung der gespeicherten „Log-Daten“ der Firewall. Durch diese Funktion kann eine Optimierung der Firewall erreicht werden, die prinzipiell immer durchgeführt werden sollte, da sich ja die Angriffsarten und Angriffsmethoden ständig ändern.
- Mit **Firewall-Auditing** kann eine Firewall überprüft werden, was durchaus sehr komplex und zeitraubend sein kann. Man kann sagen, dass Firewall-Auditing mittlerweile zu einem zentralen und entscheidenden Thema geworden ist, da dadurch eine optimale Funktionsweise der Firewall gewährleistet werden kann.
- **Accounting** bzw. IP-Accounting zählt die Daten, die eine Firewall empfängt bzw. sendet. Dadurch ist es möglich, Optimierungen der Filterregeln und anderer Firewall-Konfigurationen vorzunehmen.
- **Bandbreitenregelung**, auch als **Quality of Service** (QoS) bezeichnet, kann den einzelnen Diensten, die eine Firewall behandelt, ein bestimmtes Datenvolumen zuweisen. Die Zuweisung erfolgt dynamisch und wird von auftretenden Situationen abhängig gemacht.

Ganz wichtig: Eine Firewall sollte nur die Software installiert haben, die für die Funktionsfähigkeit der Firewall notwendig ist.

Was ist eine DMZ?

DMZ steht für **demilitarisierte Zone** und stellt ein besonderes Rechnernetz dar, in dem die installierten Server und Dienste (z.B. WWW, SMTP, DNS) vor Angriffen von außen geschützt sind. Eine DMZ kann als einstufiges oder zweistufiges Firewall-Konzept realisiert werden, wobei das zweistufige Konzept die bessere Sicherheit bietet. Beim zweistufigen Konzept trennt eine Firewall das öffentliche Netz (Internet) von der DMZ und eine zweite installierte Firewall die DMZ vom privaten Netz (Unternehmens-Netz). Dadurch kann eine einzelne Schwachstelle nicht sofort das private Netz in Schwierigkeiten bringen.
Das Besondere an einer DMZ ist die Möglichkeit, auf die in der DMZ installierten und öffentlich erreichbaren Dienste bzw. Server (diese Server werden auch als **Bastion Hosts** bezeichnet) Zugriff zu gewähren und gleichzeitig aber das private Netz vor Angriffen von außen zu schützen. Mit einer DMZ hat ein Unternehmen mit Sicherheit den besten Schutz, da die in der DMZ installierten Rechnersysteme von den anderen Netzen isoliert sind. Für Unternehmen kostet eine DMZ aber viel Know-how, Zeit und nicht zuletzt hohe Investitions- und Unterhaltungskosten (Abb. 2). ZT

ZT Autor

Thomas Burgard entwickelt Applikationssoftware und professionelle Internetauftritte für Unternehmen.

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastr. 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft