Erstellung eines Lehrkonzeptes zur IT-Sicherheit mit praktischer Umsetzung in der Umgebung des Logistik-Labors

Projektleiter
Prof. Dr.
Heinz-Michael Winkels

Zeitraum
2004

Förderung
Fachhochschule
Dortmund,
Forschungssemester

Kontakt
Prof. Dr.
Heinz-Michael Winkels,
Fachbereich Wirtschaft,
Fachhochschule
Dortmund,
Emil-Figge-Str. 42/44,
44227 Dortmund
Telefon:
(0231) 755- 4966
E-Mail:
heinz-michael.winkels@
fh-dortmund.de

Abstract
Aufbauend auf eigenen schmerzhaften Erfahrungen des Einbruchs in das Netzwerk des Logistik-Labors wurde ein Sicherheitskonzept für LANs entwickelt, theoretisch dargestellt und praktisch umgesetzt.

Das entwickelte Konzept steht als Leitfaden zur Verfügung und kann von kleinen und mittelständischen Unternehmen direkt für die Nutzung eines abgesicherten Intranets umgesetzt werden. Darüber hinaus wurde eine neue Vorlesung zum Thema „IT-Sicherheit“ entwickelt, die entsprechenden Unterlagen ausgearbeitet und ins Internet zur allgemeinen Verfügung gestellt.

Als besonderer Schwerpunkt wurde dabei das Thema „Information Warfare: Militärische Nutzung von und in Informationsnetzwerken behandelt“. Ein zugehöriger Vortrag wurde vor Bundestagsmitgliedern der „Mars und Minerva“ in Berlin gehalten.

1. Forschungsgegenstand

IT-Sicherheit wird immer mehr zur Nagelprobe für den Erfolg von E-Business und M-Business. Vor dem Hintergrund zunehmender Angriffe auf Web-Server und Netzwerke ist es hier unerläßlich, über die neuesten Trends hinsichtlich Hackermethoden und zugehöriger Verteidigungsmöglichkeiten informiert zu sein.

Durch die Nutzung des Betriebssystems Linux in Verbindung mit Firewalls war im Logistik-Labor schon ein recht hoher Sicherheitsaspekt umgesetzt worden. Das führte zu einem problemlosen Betrieb des Servers über einen Zeitraum von mehr als zwei Jahren.

Die Vielfalt der Angriffe mit zerstörerischer Intention nahm aber leider extrem zu, so dass quasi pünktlich zu Beginn des Forschungssemesters auch das Netzwerk des Logistik-Labors kompromitiert wurde.

Alle angebotenen Webseiten wurden deaktiviert und mit anti-amerikanischen und anti-jüdischen, also pro-palästinensischen Parolen überschrieben. Darüber hinaus wurde auf den Rechner ein Trojaner installiert, der vermutlich als Sprungbrett für weitere Hacks oder SPAM-Verbreitung herhalten sollte. Hintergrund dieser Attacke waren nicht Fehler bzw. fehlende Schutzmaßnahmen im zentralen FH-Netz. Vielmehr erfordert die Notwendigkeit, Dienste lokaler Labornetze auch öffentlich verfügbar zu machen, ein darauf zugeschnittenes Sicherheitskonzept für den Betrieb der Server.

Es zeigte sich übrigens, dass der Angriff nicht wie zunächst befürchtet direkt aus Dortmund kam. Die Spur des Hackers führte zunächst nach Südamerika und von dort aus dann weiter auf einen brasilianischen Server. Solche Rechner werden oft als Plattformen für illegale Web-Inhalte benutzt.
Da etwa zum gleichen Zeitpunkt ein Sicherheitsleck der zugrunde liegenden Linux-Distribution Debian bekannt wurde, blieb keine andere Wahl, als den Rechner aus dem Netz zu nehmen und ein völlig neues Netzwerk im Logistik-Labor aufzubauen, das verschärften Sicherheitsansprüchen genügt.

Der Schaden durch diesen Einbruch belief sich auf eine eklatante Behinderung der Informationsweitergabe an unsere Studierenden, auf die Verzögerung und Behinderung von Projekt- und Diplomarbeiten sowie einen immensen Zeitaufwand des Dozenten zur Beseitigung der Schäden und der Entwicklung eines neuen Konzeptes.

In der Laborumgebung wurden neueste Softwaretools wie Intrusion Detection Systeme sowie Tools zum Angriff auf Netzwerke getestet.

Ziel des Forschungssemesters war es damit,
- ein abgesichertes neues Netzwerk zu konzipieren und aufzubauendas Konzept als Leitfaden zu dokumentieren und zu publizieren
- eine Vorlesung über IT-Sicherheit nach den neuesten Erkenntnissen zu konzipieren und in Präsentationsform aufzubereiten,
- die Ergebnisse im Rahmen einer Multimedia CD-ROM zusammenzufassen
- und in die Lehrinhalte des Schwerpunktfaches Logistik/ E-Business zu integrieren.

2. Aktueller Stand der wissenschaftlichen Diskussion

Nach gegenwärtigem Stand der Sichertstechnologien reichen Firewalls zum Schutz von IT-Infrastrukturen allein nicht mehr aus, sondern verlangen nach Intrusion-Detection-Systemen, die Eindringlinge gezielt abwehren und aufspüren: Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe,

Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen.

Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.
Intrusion-Detection ist als Prozess zu verstehen und bedarf einer geeigneten organisatorischen Einbindung sowie der technischen Unterstützung durch geeignete Werkzeuge.

Als Intrusion-Detection-System (IDS) wird eine Zusammenstellung von Werkzeugen bezeichnet, die den gesamten Intrusion-Detection-Prozess von der Ereigniserkennung über die Auswertung bis hin zur Eskalation und Dokumentation von Ereignissen unterstützt.

Firewall-Systeme dienen zur Kontrolle des Netzverkehrs an Netzübergängen. Durch die Filterung des Datenflusses gemäß vorgegebener Regeln bieten Firewall-Systeme eine aktive Sicherheit, da nur der gemäß der eingestellten Regeln zulässige Verkehr das Firewall-System passieren darf. IDS bietet keine aktive Sicherheit, sondern reagiert nur auf erkannte Angriffe.

Durch die unterschiedliche Art der Kontrolle und die unterschiedlichen Einsatzpunkte ergänzen sich Firewall-Systeme und IDS in ihrer Funktionalität. Kein System kann das andere ersetzten, sondern lediglich die Funktionalität des anderen Systems erweitern. Die im Folgenden aufgeführten Beispiele verdeutlichen einige Einsatzbereiche von IDS, die von Firewall-Systemen nicht geleistet werden können.

Erkennung von Angriffen aus dem internen Netz.
Eine Firewall kann nur Angriffe abwehren, die über sie laufen. Die Firewall bietet keinen Schutz gegen Angriffe auf interne Systeme, die im internen Netz ausgelöst werden. IDS können sowohl den Datenfluss als auch Server im internen Netz überwachen.

Überwachung der Firewall Konfiguration
Als IT-Komponente ist die Firewall selbst Angriffen ausgesetzt. Daneben sind Fehlkonfigurationen der Firewall gerade in komplexen Einsatzszenarien nicht auszuschließen. Mit einem IDS kann kontrolliert werden, ob die Firewall gemäß ihrer Vorgaben arbeitet.

Zusätzliche Überwachung von Diensten, die aktiv nicht ausreichend kontrollierbar sind
Für Protokolle, für die keine Applikations-Gateways verfügbar sind, kann durch netzbasierte Sensoren die Datenflusskontrolle verbessert werden. Auch können Firewalls getunnelte und verschlüsselte Kommunikation nicht analysieren. An dieser Stelle helfen hostbasierte IDS, die die Kommunikation nach der Entschlüsselung prüfen.

Erkennung externer Zugänge, die nicht über die Firewall führen.

Die Firewall bietet nur Schutz gegen über sie geleitete Kommunikation. Mit einem IDS können dagegen auch zusätzliche Zugänge (z. B. über Modems) erkannt und überwacht werden. Sofern IDS-Komponenten über mehrere Teilnetze hinweg verteilt sind, ist darauf zu achten, dass auch die IDS-Kommunikation an den Netzübergängen entsprechend gefiltert wird.

Im Rahmen der Neukonzeption des Logistik-Netzes wurde als nach einem IDS mit integrierter Firewall gesucht, welches auf Basis von Linux funktioniert und als Open Source Anwendung frei zur Verfügung steht. Ein solches System wurde mit IPCop unter Linux/Debian gefunden und umgesetzt.

3. Angewandte Forschungsmethoden
Die Forschungsergebnisse bauen zunächst auf einer Studie des Verfassers über IT-Sicherheit, insbesondere in Verwendung mit dem Betriebssystem Linux auf.

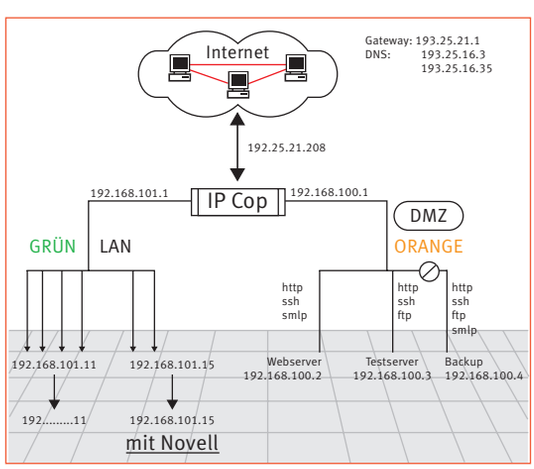
Im Anschluss daran sind eine Reihe von Seminaren und Diplomarbeiten unter der Anleitung des Verfassers abgehalten worden, mit der die unterschiedlichen Aspekte des Angriffes und des Schutzes, also der Verteidigung gegen solche Angriffe untersucht wurde. Wesentliche Quellen waren dabei das Internet selbst und die einschlägigen Seiten über Hacker-Angriffe und deren Verteidigung (CERTs).

Behandelte Diplomarbeiten:
- Virtuelle Private Netzwerke für kleine und mittelständische Unternehmen (Frank Nölken, SS2003)
- Zugangsschutz für Internetseiten mittels USB-Technik (Sven Teske; WS 2003/04)
- Datenschutz im E-Commerce (Semir Alagic, WS 2003/04)
- Realisierung von Filesharing-Servern unter Linux (Hoang Ly Phuoc, WS 2003/04)
- Umsetzung eines IT-Sicherheitskonzeptes auf Debian GNU/Linux (Nguyen Bui, WS 2003/04)

- Biometrische Verfahren und Anwendungsbeispiele aus der Praxis (Johanna STRONZIK, SS 2004)
- Viren, Würmer und Trojaner: Entwicklung und Warnmechanismus über das Internet (Oliver Bauch, SS 2004)
- Aufbau Virtueller Privater Netze mit Linux unter besonderer Berücksichtigung der Sicherheitsaspekte (Carsten Crell, WS 2000/2001)
- Sichere Geschäftstransaktionen über das Internet, ausgerichtet auf kleine und mittelständische Unternehmen (Oleg Kolesnikov, SS 2002)
- Zahlungsverkehr im Internet unter besonderer Berücksichtigung der Sicherheitsaspekte (Manuela Kneffel, SS 1998)
- Digitale Signaturen für den Elektronischen Handel (Schulz, WS 1998/99)
  Sicherheitsmechanismen im Internet ausgerichtet auf elektronische Geschäftsbeziehungen und virtuelles Geld (Kimmel, SS 1997)

4. Forschungsergebnisse

Zunächst wurde ein abgesichertes Logistik-Intranet umgesetzt, das durch das Intrusion-Detection-System IPCop geschützt wird.



Das IDS zeigte dabei enorme Angriffsversuche aus dem lokalen FH-Netz, also aus den Rechner-Pools der Fachhochschule selbst!

Die Forschungsergebnisse sind auf einer CD-ROM zusammengefasst und werden im Internet über die Web-Seite www1.logistik.fh-dortmund.de unter der Vorlesung „IT-Sicherheit“ angeboten.

Die in diesem Forschungssemester gewonnen Erkenntnisse sind in einem Leitfaden zum Aufbau eines LAMP-Systems zusammengefasst und lassen sich direkt auf die Absicherung von Intranets kleiner und mittelständischer Unternehmen anwenden.

Weitere Leitfäden zum Aufbau eines IPCop-Rechners und eines VPN (Virtuellen Privaten Netzwerkes) sind in Arbeit.

5. Weiterführende Fragestellungen

Einer der wichtigsten Punkte für die deutsche Standortfrage ist die Absicherung von eigenem Know-how, und damit auch die Absicherung getätigter Investitionen in Forschung und Entwicklung. Die Zunahme von Wirtschaftsspionage und Angriffen auf die Netzwerkstruktur von Unternehmen zeigt die Bedeutung der IT-Sicherheit.

Hier gilt es Methoden zu entwickeln,

- um bei vorherrschender Informationsflut über den neuesten Entwicklungsstand permanent informiert zu bleiben
- Automatismen zu erfinden, die in Gefahrensituationen frühzeitig warnen und Hilfen bereitstellen
- Datenbestände zu organisieren und zu sichern, so dass im worst case Schadensbegrenzung betrieben werden kann.
- unsere Studierenden zu sensibilisieren und mit den nötigen Schutzkenntnissen auszustatten.

6. Einfluss der Forschungsergebnisse auf die Lehre

Dies Lehrinhalte zur „IT-Sicherheit“ sollen ab dem WS 2005 in die Grundvorlesungen des Fachbereichs Wirtschaft über „Informationsmanagement“ aufgenommen werden und innerhalb der speziellen Wahlpflichtfächer „E-Business“, „E-Commerce“ und „Informationslogistik“ im Hauptstudium erweitert und vertieft werden.
Zur Beantwortung der Fragen über die neuesten Möglichkeiten des „Information Warfare“ und die notwendigen Absicherungen aktueller IT-Systeme sind Seminarreihen und eine Vielfalt von Diplomarbeitsprojekten geplant, die mit dem WS 2004 /05 gestartet werden.