

***„We are not cynical. Our assessment is that security is very difficult,
both to understand and to implement.”***

Carl Ellison und Bruce Schneier

Inhaltsverzeichnis

Abbildungsverzeichnis.....	IV
Tabellenverzeichnis	V
Abkürzungsverzeichnis.....	VI
Glossar	VII
1 Einführung	1
1.1 Ziele und Abgrenzung dieser Arbeit.....	2
1.2 Aufbau der Arbeit	3
2 Grundlagen.....	7
2.1 Der Begriff Webanwendung	7
2.2 Der Begriff IT-Sicherheit	7
2.2.1 Vertraulichkeit.....	8
2.2.2 Verfügbarkeit.....	8
2.2.3 Integrität	8
2.2.4 Authentizität	8
2.2.5 Nachvollziehbarkeit	8
2.3 Funktionsweise des Internets	9
2.3.1 Das HTTP-Protokoll.....	9
3 Angriffe.....	14
3.1 Angriffsarten	15
3.1.1 Kriminelle Angriffe	15
3.1.2 Publicity-Angriffe.....	15
3.1.3 Juristische Angriffe.....	16
3.2 Motivation und Täter	17
3.3 Angriffsprozess	21
4 Reconnaissance und Gegenmaßnahmen	22
4.1 Öffentliche Quellen.....	23

4.1.1	Internet-Suchmaschinen.....	23
4.1.2	Whois- und DNS-Datenbankeinträge.....	29
4.1.3	Passive virtual host-Ermittlung.....	31
4.1.4	robots.txt.....	32
4.2	Enumeration.....	34
4.2.1	Aktive virtual host-Ermittlung.....	34
4.2.2	Fingerprinting.....	36
4.2.3	Banner Grabbing.....	38
4.2.4	Server-Statistik.....	41
4.2.5	Portscan.....	42
4.2.6	Web Spidering.....	43
4.2.7	Web-Anwendungs-Scanner.....	45
4.2.8	Proxy-Analyse.....	46
4.3	Zusammenfassung.....	48
5	Schwachstellen und Gegenmaßnahmen.....	49
5.1	Buffer Overflows.....	49
5.1.1	Speicher- und Prozessorganisation.....	52
5.1.2	Funktionsprinzip des Stacks.....	54
5.1.3	Der klassische Stack-basierte Buffer Overflow.....	58
5.1.4	Off-by-Ones / Frame Pointer Overwrites.....	62
5.1.5	BSS Overflows.....	63
5.1.6	Heap Overflows.....	63
5.1.7	Weitere Overflows.....	64
5.1.8	Gegenmaßnahmen zu Buffer Overflows.....	64
5.2	SQL Injection.....	71
5.2.1	SQL Injection erkennen/überprüfen.....	74
5.2.2	SQL Injection ausnutzen.....	75
5.2.3	Gegenmaßnahmen zu SQL Injections.....	84
5.3	Cross-Site Scripting.....	90

5.3.1	Cross-Site Scripting erkennen/überprüfen	93
5.3.2	Cross-Site Scripting ausnutzen.....	94
5.3.3	Gegenmaßnahmen	100
6	Zusammenfassung und Ausblick.....	106
6.1	Resümee	106
6.2	Ausblick	107
	Literaturverzeichnis	109
	Anhang	126
	Index	144

1 Einführung

„Erst zweifeln, dann untersuchen, dann entdecken!“

Henry Thomas Buckle

Im Jahr 2004 fanden 75 Prozent aller Angriffe über Webanwendungen statt.¹ Von 250 getesteten komplexen Webanwendungen weisen 92 Prozent Sicherheitslücken auf, die von einem Angreifer ausgenutzt werden können.² Bei 130 getesteten Webanwendungen, die Finanzdienstleistungen anbieten, waren 71 Prozent anfällig gegen Angriffe, die zu einem Identitätsdiebstahl (engl. *phishing*) führen können.³ Aus der letzten Bedrohungsanalyse von Symantec geht hervor, dass im ersten Halbjahr 2006 insgesamt 69 Prozent der veröffentlichten Schwachstellen Webanwendungen zuzuordnen waren.⁴ Davon müssen 78 Prozent als leicht ausnutzbare Schwachstellen bezeichnet werden.

Seit dem 15. Februar 2005 werden unter der Adresse <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (Stand: 21.09.2006) alle Vorfälle aufgezeichnet, bei denen unbefugte Dritte personenbezogene Daten einsehen oder stehlen konnten. Bis zum 21.09.2006 wurden 301 Vorfälle veröffentlicht. Dadurch konnten unbefugte Dritte über 93.706.229 Millionen personenbezogene Datensätze einsehen oder stehlen.

Da die Zahl privater Haushalte mit Internet-Zugang in den letzten Jahren aufgrund preiswerter Angebote stark zugenommen hat, ist das Medieninteresse für solche Sicherheitsvorfälle entsprechend groß. Doch werden nicht unbedingt alle Vorfälle veröffentlicht und die Dunkelziffer schätzen Experten noch viel höher ein.⁵ Die Folgen und die Reichweite eines erfolgreichen und bekannt gewordenen Angriffs sind schwer einzuordnen. Immerhin kann ein Imageschaden so nachhaltig sein, dass ca. 20 bis 45 Prozent der Kunden zur Konkurrenz wechseln.⁶ Als die Citibank 1999 öffentlich bekannt gab, dass ein russischer Hacker 12 Millionen US-Dollar unrechtsam auf sein Konto überwie-

¹ S. [HULME]

² S. [SURF&SHULMAN]

³ S. [ORRIN&TOWLE]

⁴ S. [SYMANTEC]

⁵ Vgl. [SANS], Autorenkommentar von Kreitner zu dem Vorfall: *Ohio University Alumns, Donors Weigh in on Data Breaches (12 June 2006)*

⁶ S. [GREEN]

sen habe, hoben viele Kunden ihr Geld ab, obwohl die Citibank gleichzeitig verkündete, dass sie neue und stärkere Sicherheitsmaßnahmen implementiert habe.⁷

Findet ein Zugriff von unbefugten Dritten auf personenbezogene Daten statt, verstößt das Unternehmen gegen die hiesigen Datenschutzgesetze. Das wird, je nachdem, in welchem Land das Unternehmen operiert, von Gerichten mit einer hohen Geldstrafe belegt.⁸

Wie werden Webanwendungen geschützt, die über das Internet erreichbar sind?

Unternehmen schützen sich vor computerbasierten Angriffen durch Sicherheitsendgeräte. Firewallsysteme regulieren, welche Serverdienste angesprochen werden dürfen, netzwerkbasierete Intrusion-Detection-Systeme überprüfen den Datenverkehr auf bekannte Daten-Anomalien. Unternehmen setzen eine Sicherheitsstrategie um, das als *Defence-in-Depth* bekannt ist, bei dem besonders gefährdete Ziele durch eine oder mehrere Bastionen geschützt werden. Unternehmen tun alles, damit sie nicht über das unsichere globale Netzwerk namens Internet angegriffen werden.

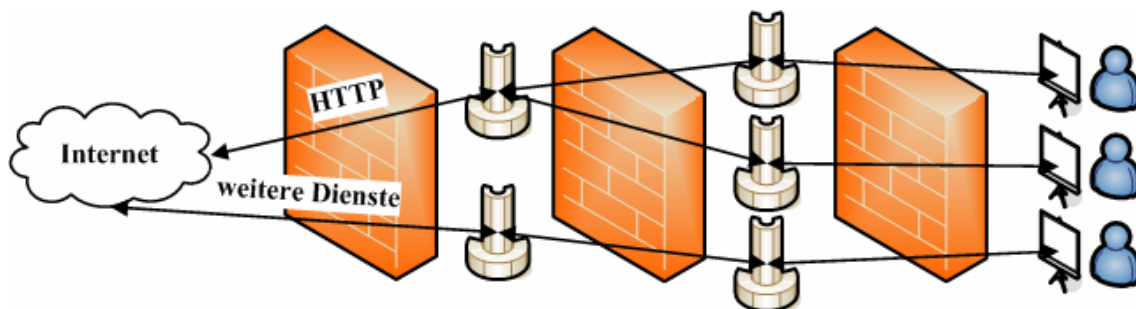


Abb. 1: Beispiel der Umsetzung der Sicherheitsstrategie *Defence-in-Depth*

Das Problem bei dieser Sicherheitsstrategie stellen die offenen Dienste dar. Typische offene Dienste, wie die Webanwendung, die in der Abbildung 1 als HTTP gekennzeichnet ist, kommunizieren mit Benutzern aus dem geschützten Netz (blaue Figuren). Das bedeutet, dass ein Angreifer die Schwachstelle eines offenen Dienstes so ausnutzen kann, dass er in das geschützte Netzwerk gelangt.

1.1 Ziele und Abgrenzung dieser Arbeit

Das vorrangige Ziel dieser Arbeit ist, Schwachstellen und Gegenmaßnahmen aufzuzeigen, die Software-Architekten und/oder Software-Entwickler bei Ihrer täglichen Arbeit

⁷ Vgl. [SCHNEIER], S. 381

⁸ S. [VANCE]

bei der Planung und Umsetzung einer Webanwendung zu berücksichtigen haben, damit das Eindringen in einen geschützten Bereich, beispielsweise ein Netzwerk, vermieden werden kann.

Diese Intention verbindet sich mit einer Reihe von abgeleiteten und konkreten Fragestellungen, deren Beantwortung dazu beiträgt, das gesteckte Ziel zu erreichen. Die folgenden Fragestellungen bilden den Kern der Arbeit und werden sukzessive erörtert:

1. Wieso finden computerbasierte Angriffe statt, d.h. aus welcher Motivation heraus? Lassen sich die Angriffe bestimmten Interessengruppen zuordnen und wie wirkt sich dies gegebenenfalls auf ein Unternehmen oder ein Projekt aus?
2. Wie ist das methodische Vorgehen eines solchen Angriffs? Kann der Angriff schon während der „Vorbereitungsphase“ unterbunden werden?
3. Welches sind die weitestverbreiteten Schwachstellen bei Webanwendungen und wie lassen sie sich von den Angreifern ausnutzen?
4. Wie können solche Schwachstellen während der Entwicklungsphase vermieden werden? Existieren dazu Ansätze? Wie können diese konkret aussehen?

Diese Arbeit eruiert nicht die einzelnen Tätergruppen. Sie stützt sich ausschließlich auf Erkenntnisse der Literatur und unterstreicht diese, wenn notwendig, durch aktuelle Ereignisse. Die Arbeit konzentriert sich auf drei wesentliche Schwachstellen, die statistisch zu belegen sind. Wie die Schwachstellen ausgenutzt werden können, um in ein fremdes System einzudringen, ist nicht Gegenstand dieser Arbeit.

Aufgrund der Schnellebigkeit von IT-Sicherheit bei Webanwendungen gibt es nur wenige Fachbücher mit dieser Thematik. Deswegen werden in dieser Arbeit viele Internetquellen herangezogen. Da diese Quellen primär in englischer Sprache sind, werden nicht eingedeutschte Fachbegriffe erklärt. Sofern ein eingedeutschter Fachbegriff existiert, wird in Klammern die englische Fachbezeichnung erwähnt.

1.2 Aufbau der Arbeit

Die Abbildung 2 zeigt den schematischen Aufbau der Arbeit. Dargestellt sind die einzelnen Kapitel mitsamt ihren Kapitelnummern und Kurzfassungen der Überschriften. Beigefügt wurden die wesentlichen Inhalte der einzelnen Kapitel. Die Pfeile dienen als Symbole für die gegenseitige Abhängigkeit und Beeinflussung der Kapitel. Obwohl dem Leser dadurch ein der Pfeilrichtung folgender Lesefluss suggeriert und auch empfohlen wird, können die einzelnen Kapitel auch in anderer Reihenfolge gelesen werden.

Für ein Verständnis der Ergebnisse des letzten Kapitels ist aber ein durchgehendes Lesen der Arbeit erforderlich.

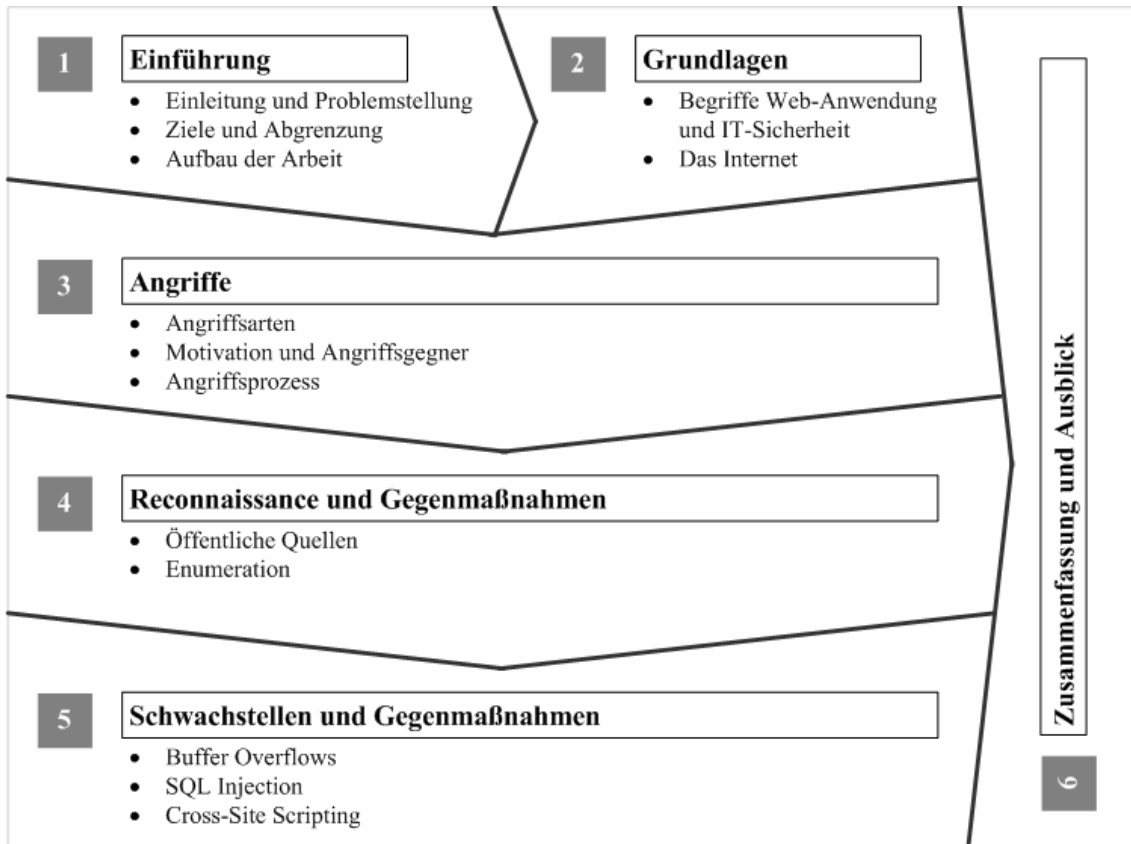


Abb. 2: Schematischer Aufbau der Arbeit

Für eine schnelle Orientierung beim Durchblättern der Arbeit wurden jedem Kapitel einleitende Worte über die Absichten des jeweiligen Kapitels vorangestellt. Im Folgenden werden die einzelnen Kapitel kurz nach ihrem Inhalt vorgestellt. Die Ausführungen sind als textuelle Ergänzung zur oben gezeigten Abbildung zu verstehen.

Kapitel 1 – Einleitung

Die Einleitung möchte den Leser auf die Brisanz des Themas mit aktuellen Fakten hinweisen. Zugleich soll der Leser mit den Zielen der Arbeit und den damit verbundenen Fragestellungen vertraut gemacht werden.

Kapitel 2 – Grundlagen

Das Kapitel beschreibt den Begriff Webanwendung, woraus sich die in Kapitel 5 beschriebenen Schwachstellen ableiten. Ferner werden die Sicherheitsbedürfnisse vorgestellt sowie das grundlegende Kommunikationsprotokoll von Webanwendungen.

Kapitel 3 – Angriffe

In diesem Kapitel werden die einzelnen Angreifertypen und deren Motivation besprochen. Anschließend wird ein Angriffsprozess dargestellt, der das Vorgehen bei einem geplanten Angriff beschreibt.

Kapitel 4 – Reconnaissance

Der Erfolg eines Angriffs beruht auf einer genügenden Anzahl von Informationen über das Zielobjekt. In Kapitel 4 werden mehrere mögliche Informationsquellen und Methoden vorgestellt. Sofern eine Gegenmaßnahme existiert, wird diese am Ende des jeweiligen Abschnitts vorgestellt. Für den eiligen Leser findet am Ende des Kapitels eine Zusammenfassung in tabellarischer Form statt, die den einzelnen Methoden das gewünschte Zielergebnis gegenüberstellt.

Kapitel 5 – Schwachstellen

Den größten Umfang dieser Arbeit nimmt das Kapitel über die Schwachstellen ein. Es beschreibt die drei häufigsten Schwachstellen bei Webanwendungen. Zunächst findet eine kurze Einleitung zur jeweiligen Schwachstelle statt. Historie, Verbreitungsgrad, Auswirkung der Schwachstelle und deren Unterarten werden in diesem Kontext ebenfalls kurz vorgestellt. Anschließend wird die Schwachstelle mit Ihren Ausprägungen erläutert. Zu den jeweiligen Schwachstellen werden auch die Gegenmaßnahmen diskutiert. Dabei wird unterschieden zwischen Maßnahmen, die die eigentliche Ursache einzudämmen versuchen, und Maßnahmen, die die Auswirkungen eingrenzen können oder sollen.

Einer der drei Schwachstellen kommt in dieser Arbeit besondere Aufmerksamkeit zu. Denn diese Schwachstelle, der *Buffer Overflow*, ist so umfangreich, dass der Leser zunächst nähere Informationen benötigt, um die nachfolgenden Erläuterungen zu verstehen.

Kapitel 6 – Fazit

Das letzte Kapitel reflektiert die wichtigsten Ergebnisse in Bezug auf die Leitfragen aus der Einleitung. Der Ausblick beschreibt kurz einen praktikablen Ansatz, wie Webanwendungen zukünftig entwickelt werden können, um die in dieser Arbeit beschriebenen Schwachstellen einzudämmen und womöglich grundsätzlich „sichere“ Webanwendungen herzustellen.

Hinweise zum Anhang

Alle im Anhang hinterlegten Quelltexte werden auch auf der Webseite <http://www.sicherheit-von-webanwendungen.de> als Download zur Verfügung gestellt. Die Quelltexte beschreiben zwei Beispiel-Anwendungen einschließlich einiger Möglichkeiten zur Ausnutzung der vorhandenen Schwachstellen sowie möglicher Gegenmaßnahmen. Dem Leser soll damit die Möglichkeit gegeben werden, die angesprochenen Vorgänge im Detail für sich zu reproduzieren und nachzuvollziehen. Der Anhang ist alphabetisch in die Abschnitte A–N unterteilt, auf die in dieser Arbeit entsprechend verwiesen wird.