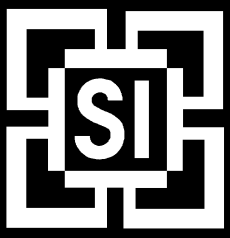


Schweizerische Informatikgesellschaft
Fachgruppe Security

Switzerland Chapter

Sicherheitsüberprüfung

von

IT-Systemen

mit Hilfe von

"Tiger-Teams"

Vertrag
Gefahrenanalyse
Durchführung
Reporting
Fallbeispiel
Rechtslage

Weitere Exemplare und Informationen zu den Fachvereinigungen erhalten Sie unter den nachfolgenden Adressen:

SI Fachgruppe Security **WWW.FGSEC.CH**
c/o Rolph Haefelfinger
PricewaterhouseCoopers
Nordstr. 15, 8035 Zürich
Tel: 01 / 630 27 60

ISACA Switzerland Chapter **WWW.ISACA.CH**
c/o Maher Kamal, CISA
Arthur Andersen AG
Binzmühlestr. 14, 8050 Zürich
Tel: 01 / 308 18 88

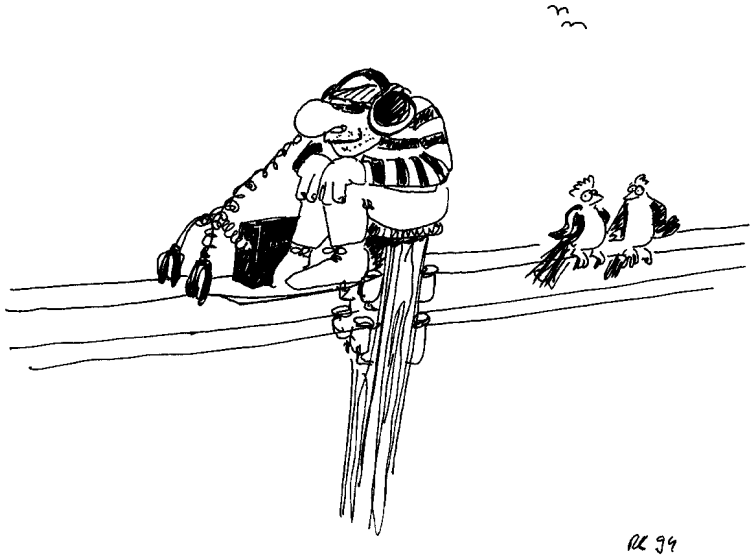
Achtung
Diese Broschüre enthält zahlreiche Hinweise für Hacking-Teams und ihre Auftraggeber. Weder die Autoren der Broschüre noch die Fachvereinigungen "SI Fachgruppe Security" oder "ISACA Switzerland Chapter" übernehmen irgendwelche Gewähr für die inhaltliche Richtigkeit oder Haftung für die Anwendung der enthaltenen Hinweise.

Impressum

Beiträge:	Mitglieder der Arbeitsgruppe "Tiger-Team"
Abbildungen:	Mitglieder der Interessengruppe "Tiger-Team"
Redaktion:	Peter R. Bitterli
Satz:	Evelyn Hug, Bitterli Consulting
Layout:	Francesca Lüscher Baglioni, Wissenstransfer
Zeichnung:	Rolf Kränzlin, Zürich

Die Erstellung dieser Broschüre wurde gesponsert von der SI Fachgruppe Security und dem ISACA Switzerland Chapter.

Inhaltsverzeichnis



Diese Seite bleibt aus technischen Gründen leer.

Arbeitsgruppe “Tiger-Team”

Die Arbeitsgruppe “Tiger-Team” der Fachgruppe Security der Schweizerischen Informatikergesellschaft (SI) beschäftigte sich mit dem Thema Sicherheitsüberprüfungen von IT-Systemen mit Hilfe von beauftragten Hackern, den sogenannten“Tiger-Teams”.

Das Ziel der Arbeitsgruppe war, sich mit den operationellen Risiken einer Hacking-Attacke auseinanderzusetzen. Dabei handelt es sich um einen Angriff, der im Auftrag eines Kunden durchgeführt werden soll. Diese Art von Hacking ist auch unter dem Begriff “Ethical Hacking” bekannt.

Die acht Mitglieder dieser Arbeitsgruppe, die sich beruflich vorwiegend in diesem Gebiet betätigen, trafen sich während eines Jahres zu regelmässigen Sitzungen. Dabei wurden nachfolgende Fragestellungen diskutiert:

- Wie weit darf und wie weit muss eine Attacke gehen, um den gewünschten Nutzen zu erreichen?
- Was sind die Vor- und Nachteile einer Attacke, d.h. was ist der direkte Nutzen, den ein Kunde hat?
- Kann eine solche Attacke einen Mehrwert generieren?
- Wie sehen bei obigen Punkten die rechtlichen Aspekte aus?

Die Arbeitsgruppe befasste sich mit dem Thema Hacking nicht nur auf der Meta-Ebene sondern deckte den gesamten Bereich von den technischen und organisatorischen bis zu den operationellen Aspekten ab. Zur systematischen Aufarbeitung wurde das Thema in vier Phasen unterteilt, welche gleichzeitig den Ablauf einer Hacking-Attacke darstellen:

- Akquisition, Offerte und Vertrag
- Risikoanalyse
- Durchführung
- Bericht und Präsentation

Entlang dieser vier Phasen haben sich Sub-Arbeitsgruppen zu ausserordentlichen Sitzungen getroffen, um sich im Detail mit den entsprechenden Inhalten auseinanderzusetzen und so ihren Beitrag zum Gesamtwerk zu liefern. Die wesentlichsten Resultate der interessanten Diskussionen wurden im vorliegenden Bericht zusammengefasst.

Dieser Bericht beinhaltet zu jeder erwähnten Stufe ein eigenes Kapitel, welches zum Teil als Vorlage für die Tätigkeit im Kundenauftrag dienen kann. Er richtet sich nicht nur an jene Unternehmungen oder Einzelpersonen, welche Hacking-Attacken im Auftrag ausführen, sondern auch an die zu überprüfenden Unternehmen (Auftraggeber).

Für die erste Gruppe stellt der Bericht einen Leitfaden dar – und für die zweite soll er dazu dienen, bei einer Sicherheitsüberprüfung von IT-Systemen mit der Hilfe von Tiger-Teams mehr Transparenz in die Vorgehensweise zu bringen.

Die Mitglieder dieser Arbeitsgruppe in alphabetischer Reihenfolge:

Roger Auinger (PricewaterhouseCoopers AG; Leiter der Arbeitsgruppe)
Peter R. Bitterli (Bitterli Consulting AG)
René Eberhard (r^3 security engineering ag)
Vladimir Kulhavy (Syscom Engineering AG)
Kurt Müller (UBS AG)
Alberto Parisi (Swiss Security Service Laboratory AG)
Paul Schöbi (cnlab AG)
Stefan Vogt (UBS AG)

Vertrag

Die Tätigkeit eines Hackers im Auftragsverhältnis bewegt sich in einem rechtlich heiklen Gebiet. Eindringen in ein geschütztes Computersystem, Zeitdiebstahl, Manipulation von Daten und andere der für derartige Aufträge benötigten Hacking-Techniken gelten als Straftatbestände. Es ist daher von grosser Bedeutung, dass Auftraggeber wie Auftragnehmer sich durch ein entsprechendes Vertragswerk rechtlich einwandfrei absichern. Dieses Kapitel enthält Hinweise und zentrale Textbausteine zur Integration in einen möglichen Vertrag.

1 Präambel

Dem Auftrag sollte unbedingt eine Präambel vorausgehen, aus welcher die Motivation des Auftraggebers für die Erteilung des Auftrags hervorgeht.

Insbesondere sollte festgehalten werden, dass der Auftraggeber eine dem heutigen Stand der Technik optimale Informationssicherheit anstrebt und deshalb ein Hacker-Team beauftragt, Lücken im bisherigen System ausfindig zu machen.

2 Auftraggeber

Auftraggeber ist die *Gesellschaft*, welche den Auftrag erteilt. Einzelne Mitarbeiter des Auftraggebers sind allenfalls als Ansprechpartner für den Auftragnehmer namentlich zu bezeichnen, sofern dies der Auftraggeber oder der Auftragnehmer als Schutzmassnahme wünschen. Diese Mitarbeiter sind berechtigt, Änderungen an den vereinbarten Dienstleistungen vorzunehmen.

Da das Hacken ohne Einverständnis des Auftraggebers verboten ist, muss ausserdem genau darauf geachtet werden, *wer* den Auftrag seitens des Auftraggebers unterzeichnet, damit die Erlaubnis rechtsgültig erfolgt. Die unterzeichnenden Personen müssen gemäss Handelsregistereintrag (eventuell kollektiv zu zweien) zeichnungsberechtigt sein. Es ist demnach zu empfehlen, einen aktuellen Handelsregister-Auszug des Auftraggebers einzuholen.

3 Auftragnehmer

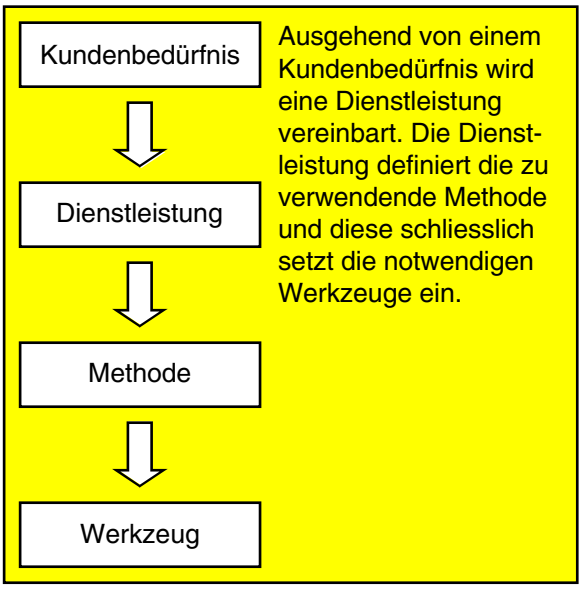
Der Auftragnehmer muss klar definiert sein. Nur für diesen Auftragnehmer besteht ein Einverständnis des Auftraggebers zum Hacken.

Bereits bekannte Unterlieferanten sind in den Vertrag aufzunehmen und namentlich zu bezeichnen. Später hinzukommende Unterlieferanten benötigen schon zu ihrer eigenen Sicherheit eine schriftliche “Hack-Erlaubnis”. Ausserdem ist es aus haftungsrechtlicher Sicht wichtig, dass der Beizug von Unterlieferanten (rechtlich: Substitution) vom Auftraggeber erlaubt ist.

Durch diese Erlaubnis haftet der Auftragnehmer nur für die gehörige Sorgfalt bei der Auswahl und Instruktion der beigezogenen Dritten. Bei unerlaubtem Beizug von Dritten haftet der Auftragnehmer für den beigezogenen Dritten wie für sich selbst. Empfohlen ist es, an dieser Stelle die gesamte Projektorganisation darzustellen.

4 Vertragsgegenstand

Die folgende Grafik soll die verwendeten Begriffe erläutern:



Der Auftrag ist möglichst klar zu formulieren. Die eingesetzten Methoden und Mittel sind soweit sinnvoll aufzuführen. Falls eine Wahl des Vorgehens noch nicht möglich ist, so sind geeignete Meilensteine vorzusehen, welche eine Abstimmung mit dem Auftraggeber ermöglichen.

Die Tätigkeiten des Auftragnehmers sind nicht ziel- oder erfolgsorientiert, sondern tätigkeitsorientiert, weshalb das Vertragsverhältnis rechtlich als Auftrag zu qualifizieren ist.

Vertragsgegenstand sind die durchzuführenden Arbeiten, z.B.

- Überprüfung der Einhaltung von Richtlinien (Compliance)
- Ermittlung eines allfälligen Handlungsbedarf
- Förderung des Sicherheitsbewusstseins
- Schwachstellenanalyse
- Risikoanalyse
- Schutz vor Hacking/Crime
- Audit von Prozessen
- Security Review
- Benchmarking (Soll/Ist-Vergleich)
- Zertifizierung Hardware, Software oder System
- Abnahme Hardware, Software oder System
- “Recovery” verlorener Daten
- Hacken/Eindringen
- Information Retrieval

Im Bereich der Methoden werden die folgenden Themen betrachtet (die Methoden in Klammern werden aus ethischen oder anderen Gründen nicht durchgeführt):

- Sniffing
- (Social Engineering)
- Scanning
- Information Gathering
- Phreaking

- Cracking
- Denial of Service
- Malicious Software
- Information Analysis
- (Physical Security)
- Trusted Relationship
- Session Hijacking
- (Wire Tapping)

Compliance, Zertifizierung und Audit stellen erhöhte Anforderungen an die Arbeitsmethodik, Arbeitspapiere, Projektmanagement usw. Strafrechtlich relevant sind Recovery, Hacken, Scanning, Social Engineering.

5 Auftragserteilung

Die Erteilung des Auftrags muss schriftlich erfolgen.

Dadurch, dass das Hacken in Datenverarbeitungssystemen strafbar ist, wenn es in unbefugter Weise erfolgt, sollten weitere Aufträge oder Modifikationen des Auftrags, die strafrechtlich relevant sein könnten, *nie* mündlich entgegengenommen werden.

Andere Aufträge die lediglich kostenrelevant sind, sollten nach mündlicher Erteilung immer schriftlich bestätigt werden. Andernfalls könnte es zu einem zivilrechtlichen Beweisproblem in Falle eines Streits über die Kosten kommen.

6 Obliegenheiten des Auftraggebers

Die Obliegenheiten des Auftraggebers sollten wie folgt festgelegt werden (nachfolgender Textbaustein ist zu empfehlen):

> *"Zu den Obliegenheiten des Auftraggebers gehören alle Leistungen, welche der Auftraggeber als Voraussetzung für die Erfüllung dieses Auftrags zu erbringen hat. Darunter fallen grundsätzlich:*
> - *Die Abgabe aller Unterlagen und Informationen, welche der Auftragnehmer zur Ausführung der Arbeiten benötigt;*
> - *Die Prüfung und Abnahme der vom Auftragnehmer vorgelegten Konzepte, Zwischenresultate, Auswertungen etc.;*
> - *Die Auswahl der zu verarbeitenden Daten;*
> - *Die Schaffung der technischen, organisatorischen und administrativen Voraussetzungen für die Durchführung der Prüfungen;*
> - *Die Massnahmen zur Überprüfung von Ergebnissen und Auswertungen sowie zur Sicherstellung von Daten und Programmen.*
>
> *Stellt der Auftragnehmer fest, dass die Obliegenheiten nicht vollständig oder nicht gehörig (unrichtig bzw. unzweckmässig) erfüllt worden sind, hat er dies umgehend nach Erkennung beim Auftraggeber anzumahnen."*

7 Kosten und Termine

Gemäss den im Unternehmen üblichen Konditionen. Neben den normalen Kosten sind insbesondere die Konditionen bei unerwartetem Verlauf des Projekts (erhöhter Aufwand, vorzeitiger Abbruch) zu behandeln. Neben den vereinbarten Vergütungen sollten die Zahlungskonditionen genau festgelegt werden.

8 Auftragsbeendigung

Start und Ende des Projekts müssen klar definiert sein.

Zwischen dem Auftraggeber und dem Auftragnehmer besteht aus rechtlicher Sicht gesehen ein Auftragsverhältnis gemäss Art. 394 ff. OR. Der Auftragnehmer schuldet dem Auftraggeber ein Tätigwerden, indem er ein Informationssystem auf dessen Sicherheit überprüft. Die Gesetzesbestimmungen über das Auftragsverhältnis gehen von einem Vertrauensverhältnis zwischen dem Auftraggeber und dem Auftragnehmer aus, das, falls es gestört wird, die Weiterführung des Auftrags nicht als sinnvoll erscheinen lässt.

8.1 Kündigung

Art. 404 Abs.1 OR besagt, dass dieses Auftragsverhältnis von jeder Partei jederzeit widerrufen oder gekündigt werden kann. Diese Norm ist gemäss ständiger Rechtsprechung des Bundesgerichts *zwingender* Natur, sie kann – sofern es sich um ein typisches Auftragsverhältnis handelt – vertraglich *nicht* abgeändert werden. Vereinbarte Kündigungsfristen wären aus diesem Grunde von vorneherein nicht beachtlich.

In rechtlicher Hinsicht ist das Widerrufsrecht im Auftragsverhältnis ein sehr komplexes und in der juristischen Lehre und Praxis umstrittenes Thema. Mit den obigen Ausführungen sollte lediglich dargetan werden, dass eine vereinbarte Kündigungsfrist *vor Gericht* möglicherweise nicht standhalten wird. Dennoch ist empfehlenswert, bei zeitlich unbegrenzten Aufträgen eine Kündigungsfrist zu vereinbaren. Im Einzelfall wäre nämlich zu prüfen, ob das Auftragsverhältnis ein “typisches” im Sinne des Gesetzes ist oder nicht. Letzterenfalls wären die vereinbarten Kündigungsfristen gültig.

8.2 Kündigung zur Unzeit

In wichtigen Fällen muss eine sofortige Beendigung des Auftrags möglich sein. Widerruf oder Kündigung einer Partei dürfen jedoch gemäss Art. 404 Abs. 2 OR nicht zur Unzeit erfolgen, sonst wird die widerrufende oder kündigende Partei schadenersatzpflichtig. “Zur Unzeit” bedeutet, dass die beendende Partei *ohne Grund*, d.h. in einem ungünstigen Moment ohne sachliche Rechtfertigung (z.B. ohne Vertragsverletzung der anderen Partei) der anderen Partei besondere Nachteile verschafft. Die Schadenersatzpflicht bei einer Kündigung zur Unzeit deckt jedoch nicht den entgangenen Gewinn der anderen Partei ab. Sie ist lediglich ein Ersatz für den entstandenen Schaden resp. der Aufwendungen, die im Hinblick auf die Vertragserfüllung getätigt wurden.

"Widerruft oder kündigt eine Partei das Auftragsverhältnis zur Unzeit, so schuldet sie der anderen Partei vollen Schadenersatz zuzüglich eine Konventionalstrafe im Betrag von CHF ..."

In folgenden Fällen sollte eine sofortige Beendigung der Arbeit ohne Kostenfolgen für den Auftragnehmer möglich sein, wobei der Auftraggeber dem Auftragnehmer den vollen Schadenersatz für die bis dahin erbrachten Arbeiten zu vergüten hat:

- Einsicht in ungesetzliche Aktivitäten des Auftraggebers
- Notwendigkeit der Verletzung des geltenden Rechts durch die zur Erfüllung des Auftrags durchzuführenden Arbeiten.

9 Vertraulichkeit

Der Auftragnehmer verpflichtet sich, die im Zusammenhang mit dem Mandat erhaltenen Informationen sowie die Resultate der Beratung zeitlich unbefristet streng vertraulich zu behandeln, sofern diese nicht bereits öffentlich bekannt waren oder später öffentlich bekannt werden.

Der Auftragnehmer ist ausserdem zu verpflichten, den Zugang zu diesen Informationen auf diejenigen Personen zu beschränken, welche diese zur Erledigung des Auftrags benötigen, und die von ihm eruierten Resultate ausschliesslich dem Auftraggeber zur Verfügung zu stellen. Die Informationen müssen unabhängig von ihrer Aufbewahrungsart vor unberechtigtem Zugriff geschützt werden.

Der Auftragnehmer geht bei den vom Auftraggeber zur Verfügung gestellten Informationen, Unterlagen und Datenträgern davon aus, dass dadurch keinerlei Vorschriften des Daten- oder Persönlichkeitsschutzes verletzt werden.

Aus der Sicht des Auftragnehmers empfiehlt sich, die Verantwortung für die Unterzeichnung der "Vertraulichkeitsklausel mit Drittfirmen" dem Auftraggeber zu übertragen. Der Auftragnehmer soll so wenig wie möglich für die Aktivitäten des Auftraggebers einstehen müssen.

Die Übertragung der Verantwortung für die Unterzeichnung der Vertraulichkeitsklausel rechtfertigt sich gegenüber dem Auftraggeber deshalb, weil die Einsetzung von Unterakkordanten der Zustimmung des Auftraggebers bedarf.

10 Ansprechpartner für kritische Fälle

Für kritische Fälle ist eine unabhängige Stelle beim Auftraggeber zu bezeichnen, welche über die Behandlung von unerwarteten, kritischen Daten und der daraus gewonnenen Erkenntnisse entscheiden kann. Diese Stelle darf nicht direkt in das eigentliche Projekt involviert sein. Sie auch das Kapitel "Ethik".

11 Haftungsausschluss

Es empfiehlt, sich die Haftungsbeschränkung wie folgt zu formulieren:

> *"Der Auftragnehmer erbringt seine Arbeit mit der gebotenen Sorgfalt. Er haftet für direkte Schäden, die er in grobfahrlässiger oder vorsätzlicher Weise verursacht. Die Haftung für leichte Fahrlässigkeit, für Folge- oder indirekte Schäden wird ausgeschlossen.*
>
> *Dem Auftraggeber ist bekannt, dass die Tätigkeiten des Auftragnehmers, insbesondere das "Hacken" ein hohes Risikopotential in sich tragen und eventuell zu Systemabstürzen oder Datenverlusten führen können. Für die daraus entstehenden Schäden haftet der Auftragnehmer nur in oben umschriebenem Umfang."*

Die Haftung für Drittpersonen (Unterakkordanten) muss nicht mehr speziell geregelt werden. Wie oben erwähnt, haftet der Auftragnehmer gegenüber dem Auftraggeber bei *erlaubter* Substitution lediglich für die gehörige Sorgfalt bei der Wahl und Instruktion des Dritten (Art. 399 Abs. 2 OR).

Für Hilfspersonen und bei unerlaubter Substitution (z.B. Angestellte des Auftragnehmers) haftet der Auftragnehmer wie für sich selbst, das heisst wie in oben formuliertem Haftungsausschluss. Die Haftung für Hilfspersonen kann auch ganz ausgeschlossen werden.

12 Urheberrecht/Lizenz

Zur Regelung der Lizenzproblematik kann der folgende Textbaustein empfohlen werden:

> *"Der Auftraggeber trägt die alleinige rechtliche und finanzielle Verantwortung, falls durch die Überlassung von Daten, Dokumenten und Unterlagen an den Auftragnehmer oder durch die Tätigkeiten des Auftragnehmers im Zusammenhang mit der Erfüllung dieses Auftrags-, Urheber- oder Lizenzrechte verletzt* werden.
>
> *Der Auftragnehmer trägt die Verantwortung dafür, dass die von ihm im Zusammenhang mit der Erfüllung dieses Auftrags erstellten Dokumentationen keine Urheberrechte verletzen."*

13 Arbeitsdokumentation

Um den Anforderungen des Datenschutzgesetzes gerecht zu werden, sollte zusätzlich zu den Bestimmungen betreffend Protokollierung aller Untersuchungshandlungen folgendes Recht des Auftraggebers in den Vertrag aufgenommen werden:

> *"Der Auftraggeber hat das Recht, den Auftragnehmer jederzeit bezüglich seiner Tätigkeiten im Zusammenhang mit der Vertragserfüllung zu kontrollieren."*

Der Auftragnehmer ist verpflichtet, die durchgeführten Arbeiten (Tätigkeiten) an wichtigen Systemen durchgängig schriftlich festzuhalten und dem Auftraggeber diese Aufzeichnungen auf Wunsch zur Verfügung zu stellen.

Die Überlassung von Zwischenergebnissen (welche, wann, aufgrund welcher Ereignisse, in welcher Form, etc.) ist zu definieren. Im Normalfall wird ein schriftlicher Bericht über die Arbeiten abgegeben. Die Form des Berichtes wird im Kapitel 3 des Teils “Reporting” vorgestellt.

Es wird empfohlen, die Aufbewahrungsproblematik mit der folgenden Klausel zu regeln:

> *Dem Auftragnehmer obliegt gegenüber dem Auftraggeber keine Verpflichtung, die dem Auftraggeber übergebenen Projektdokumente weiterhin aufzubewahren.*

Im Normalfall verpflichtet sich der Auftragnehmer, die nicht mehr benötigten Projektunterlagen nach Abschluss des Auftrags zu vernichten. Eine generelle Pflicht zur Vernichtung aller Unterlagen kann in vielen Fällen nicht eingehalten werden (da zu Dokumentationszwecken, z.B. für Disputfälle, gewisse Daten aufbewahrt werden müssen).

14 Weitere vertragliche Anforderungen

14.1 Vollständigkeitsklausel

Der Vertrag beinhaltet alle Abmachungen.

14.2 Gültigkeit

Falls Teile des Vertrags aus irgendwelchen Gründen (z.B. gesetzlichen) nicht gültig sind, so ist die Gültigkeit der andern Teile nicht betroffen. Im Zweifelsfalle gilt eine Regelung, welche der ursprünglich definierten möglichst nahe kommt.

14.3 Gerichtsstand

Neben dem Gerichtsstand muss das anzuwendende Recht definiert werden, z.B. Gerichtsstand ist **Zürich**, es wird Schweizer Recht angewendet.

Diese Seite bleibt aus technischen Gründen leer.

Gefahrenanalyse

1 Einleitung

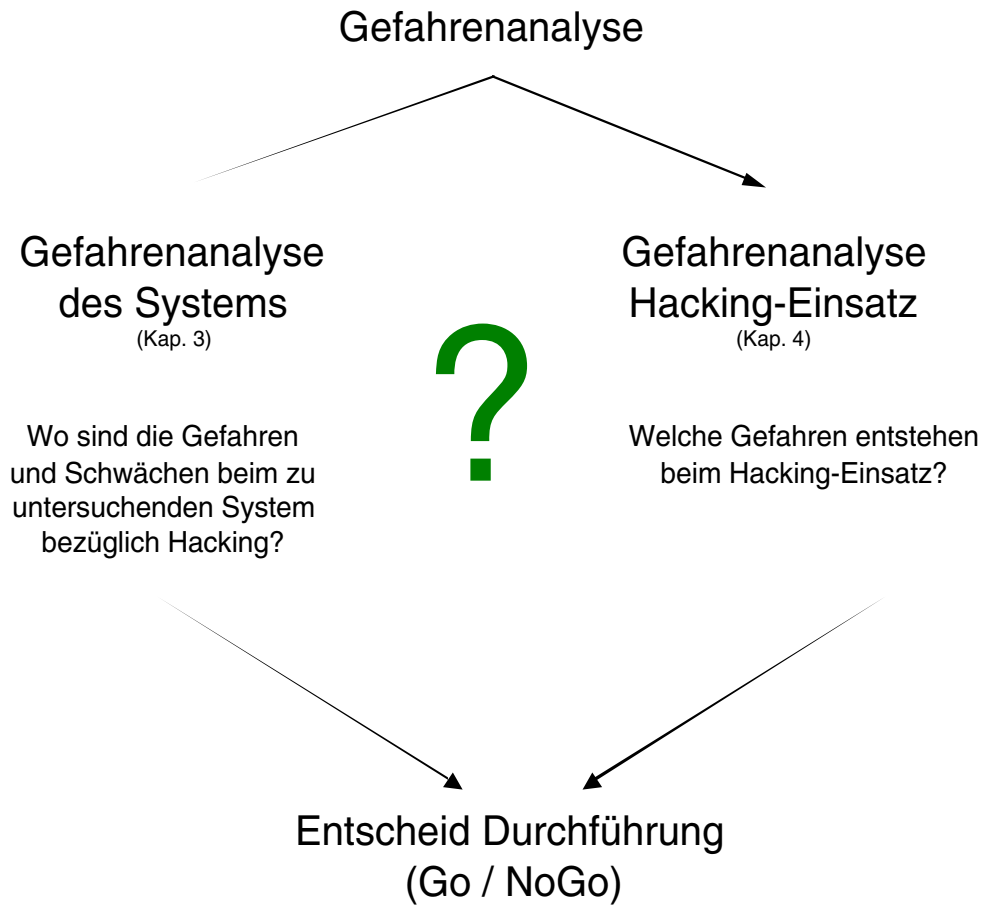
Das Kapitel beschreibt ein Vorgehen für das Erfassen und die Beurteilung von Gefahren des Einsatzes von Tiger-Teams für Sicherheitsüberprüfungen. Die Gesamtgefahr wird in zwei Teilschritten ermittelt:

- Gefahrenanalyse des Systems
- Gefahrenanalyse Hacking-Einsatz

Die *Gefahrenanalyse des Systems* untersucht die Verletzbarkeit des Systems auf Hacking-Angriffe Dritter. Die *Gefahrenanalyse Hacking-Einsatz* beschreibt die zusätzlichen Gefahren, welche durch den Einsatz von Tiger-Teams am System entstehen.

2 Gefahrenanalyse

2.1 Komponenten



Die *Gefahrenanalyse des Systems* im Kapitel 3 beschreibt die Schwachstellen und Gefahren des Systems in Bezug auf Hacking-Angriffe (Wie einfach kann ein Hacker das System überlisten?). Im Teil *Gefahrenanalyse Hacking-Einsatz* (Kapitel 4) soll aufgezeigt werden, welche Gefahren durch den Einsatz von Tiger-Teams entstehen.

Die Resultate dieser beiden Analysen werden in der Gesamtbeurteilung zusammengefasst und bilden die Entscheidungsgrundlage für die Durchführung der eigentlichen Hacking-Angriffe (Go / NoGo Entscheid).

Unter Umständen können aufgrund der Analysen entsprechende Massnahmen zur Verminderung der Risiken evaluiert werden.

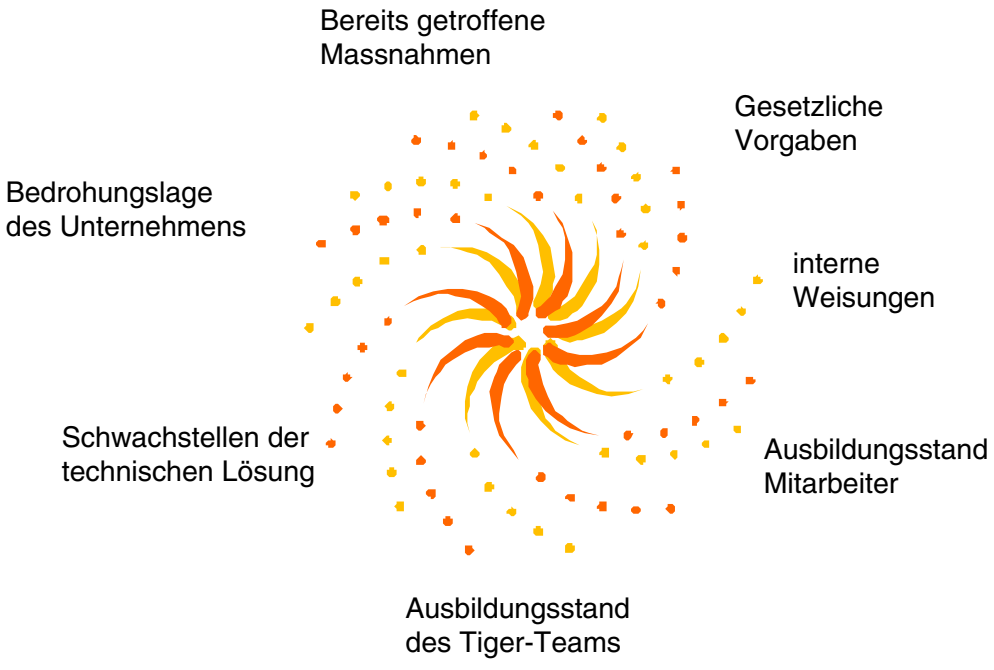
2.2 Einfluss der Gefahrenanalyse im Gesamtprozess

Phase	Art des Einflusses
Vorgehensplan	Der Vorgehensplan wird aufgrund der Gefahrenanalyse revidiert und gegebenenfalls angepasst.
Durchführung	Während der Durchführung wird die Gefahrenanalyse als Grundlage für kurzfristige Entscheide (Z.B. Sollen wir diesen Angriff wagen?) beigezogen.
Bericht	Im Bericht werden Methoden, welche aufgrund der Gefahrenanalyse nicht zur Durchführung gelangten, festgehalten.

2.3 Gefahren-Analyse kontra Risk-Assessment-Prozess

Im Gegensatz zum Risk-Assessment-Prozess für ein System oder eine Firma beschreibt die Gefahren-Analyse nur die in Bezug auf das Hacking relevanten Aspekte. So wird zum Beispiel die generelle Risikolage eines Unternehmens in der Gefahren-Analyse nicht berücksichtigt. Solche Überlegungen müssen Teil des Risk-Assessment-Prozesses sein.

2.4 Faktoren einer Gefahren-Analyse in Bezug auf Hacking



3 Gefahrenanalyse des Systems

3.1 Generelle Bemerkung

Wir gehen davon aus, dass die zu betrachtenden Systeme in einer kontrollierten und sicheren Umgebung betrieben werden. Unerlaubte physische Zugriffe auf die Systeme, Control-Panels und Konsolen betrachten wir nicht als Hacking. Diesen Gefahren kann durch entsprechende organisatorische und bauliche Massnahmen begegnet werden. Bedrohungen, herrührend von ungenügendem physischen Zugriffsschutz, werden daher zwar im Gefahrenkatalog aufgeführt, sind aber nicht Gegenstand unserer Gefahrenanalyse.

3.2 Umsetzung

Damit die entsprechenden Risiken des Systems systematisch erfasst und klassifiziert werden können, werden die Gefahr, Bedrohungsgrad, Hackervoraussetzung sowie Einstufung der Bedrohung (intern/extern) mit einbezogen. Im Kapitel 5.3 befindet sich eine Mustertabelle einer Gefahrenanalyse, in welcher diese Informationen in den Spalten 1 bis 7 festgehalten werden können.

4 Gefahrenanalyse Hacking-Einsatz

Aufgrund der bei der Gefahrenanalyse des Systems erfassten relevanten Gefährdungen werden nun in der Gefahrenanalyse Hacking-Einsatz die Angriffsmethoden, deren Erfolgschance und der Aufwand beurteilt. Zur Verminderung der Risiken werden mögliche Gegenmassnahmen erfasst. Diese Informationen können in der Tabelle Gefahrenanalyse (Kap. 5.3) in den Spalten 8 bis 12 eingefügt werden.

5. Hacking-Planung

5.1 Generelle Bemerkungen

Die Basis für die untenstehende Liste von Gefährdungen stammt vom BSI (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) IT-Grundschutzhandbuch 1998 (http://www.bsi.de). Zur leichteren Referenzierung von Zusatzinformationen wurde die Originalnummer beibehalten.

5.2 Bemerkung zu den Kolonnen

Nr.	Titel	Beschreibung	Massstab
1	Nr.	Eindeutige Referenzierung der Gefährdung	
2	BSI Nr.	Nummer der Gefährdung bei BSI gemäss IT-Grundschutzhandbuch	
3	Gefährdung	Beschreibung der Gefährdung, die betreffend Hacking relevant sein könnte	
4	Bedrohungsgrad	Einstufung der Gefährdungr für unser spezifisches System oder Netz	1: nicht relevant 2: unkritisch für das System 3: kritisch für das System 4: äusserst kritisch für das System
5	Hackervoraussetzung	Erfordernis für die Chance der Ausnützung dieser Gefährdung durch einen Hacker	1: Benutzer ohne Spezialkenntnisse 2: Spezialist 3: Spezialist mit aufwendigen Mitteln 4: Gruppe von Spezialisten mit aufwändigen Mitteln
6	intern/extern	Bedrohung von innen und/oder von aussen?	
7	Go / NoGo Planung	Soll für diese Gefährdung ein Hacking-Angriff untersucht werden? (J/N)	
8	Angriffsmethode	Beschreibung der geplanten Methode für den Zugriff	
9	Erfolgschance	Erfolgsaussichten für den geplanten Angriff	1: Erfolg unwahrscheinlich 2: Erfolg möglich 3: Erfolg wahrscheinlich 4: Erfolg garantiert
10	Aufwand	Aufwand (z.B. finanziell, personell) für die Durchführung	
11	Risikobeurteilung	Beurteilung der möglichen Risiken und Auswirkungen einer Durchführung der Attacke	1: geringes Risiko 2: mittleres Risiko 3: grosses Risiko 4: sehr grosses Risiko
12	Gegenmassnahme	Gegenmassnahmen, um Risiko zu minimieren	
13	Go/ NoGo Definitiv	Soll die Attacke aufgrund des Risikos durchgeführt werden?	

5.3 Muster einer Gefahrenanalyse-Tabelle

			Gefahrenanalyse des Systems				Gefahrenanalyse Hacking-Einsatz					
1	2	3	4	5	6	7	8	9	10	11	12	13
Nr.	**BSI Nr.**	**Gefährdung**	**Bedrohungsgrad (1–4)**	**Hackervoraussetzung (1–4)**	**int./ ext.**	**Go/ NoGo Planung**	**Angriffsmethode**	**Erfolgschance (1–4)**	**Aufwand**	**Risikobeurteilung (1–4)**	**Gegenmassnahme**	**Go/ NoGo Definitiv**
	G 2	**Gefährdungskatalog: Organisatorische Mängel**										
1	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen		1–3	i, e							
2	G 2.45	Konzeptionelle Schwächen des Netzes (Segmentierung)		2, 3	i, e							
3		Platzhalter für Gefährdungen										
4		"										
5		"										
	G 3	**Gefährdungskatalog:** Menschliche Fehlhandlungen										
6	G 3.10	Falsches Exportieren von Dateisystemen unter Unix		2								
7	G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten		2, 3	i, e							
8	G 3.29	Fehlende oder ungeeignete Segmentierung		2, 3	i, e							
9		Platzhalter für Gefährdungen										
10		"										
11		"										
	G 4	**Gefährdungskatalog: Technisches Versagen**										
12	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen		2, 3	i, e							
13	G 4.22	Schwachstellen oder Fehler in Standardsoftware		2, 3	i, e							
14		Platzhalter für Gefährdungen										
15		"										
16		"										
	G 5	**Gefährdungskatalog: Vorsätzliche Handlungen**										
17	G 5.7	Abhören von Leitungen		2	i							
18	G 5.9	Unberechtigte IT-Nutzung										
19	G 5.10	Missbrauch von Fernwartungszugängen		2, 3	i, e							
20	G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal		2	i							
21	G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal		2, 3	i, e							
22	G 5.18	Systematisches Ausprobieren von Passwörtern		2	i							
23	G 5.19	Missbrauch von Benutzerrechten		1, 2	i							
24	G 5.20	Missbrauch von Administratorrechten		2, 3	i, e							

Fortsetzung der Tabelle auf der nächsten Seite.

Fortsetzung Muster einer Gefahrenanalyse-Tabelle

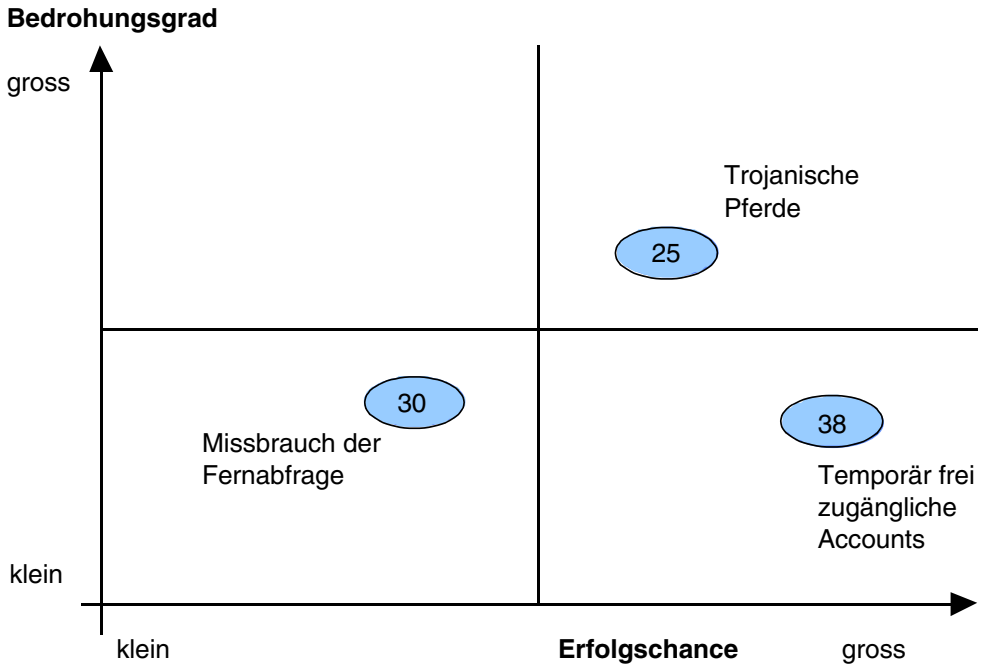
			Gefahrenanalyse des Systems				Gefahrenanalyse Hacking-Einsatz					
1	2	3	4	5	6	7	8	9	10	11	12	13
Nr.	**BSI Nr.**	**Gefährdung**	**Bedro-hungs-grad (1–4)**	**Hacker-voraus-setzung (1–4)**	**int./ ext.**	**Go/ NoGo Planung**	**Angriffs-methode**	**Erfolgs-chance (1–4)**	**Auf-wand**	**Risiko-beur-teilung (1–4)**	**Gegen-mass-nahme**	**Go/ NoGo Definitiv**
25	G 5.21	Trojanische Pferde		2, 3	i, e							
26	G 5.23	Computer-Viren		1, 2, 3	i, e							
27	G 5.24	Wiedereinspielen von Nachrichten (User-Id, PW, ...)		2, 3	i, e							
28	G 5.25	Maskerade		2, 3	i, e							
29	G 5.26	Analyse des Nachrichtenflusses		2, 3	i, e							
30	G 5.38	Missbrauch der Fernabfrage		2, 3	i, e							
31	G 5.39	Eindringen in Rechnersysteme über Modem		2, 3	i, e							
32	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon		2	i							
33	G 5.41	Missbräuchliche Nutzung eines Unix-Systems		2, 3	i, e							
34	G 5.42	Social Engineering		1, 2, 3	i, e							
35	G 5.43	Makro-Viren		1, 2, 3	i, e							
36	G 5.48 – G .51	Missbrauch von Netzwerk und Protokoll-Schwachstellen (IP-Spoofing, Source-Routing, etc.)		2, 3	i, e							
37	G 5.54	Vorsätzliches Herbeiführen eines Abnormal End (denial of service)		2, 3	i, e							
38	G 5.56	Temporär frei zugängliche Accounts		2, 3	i, e							
39	G 5.61	Missbrauch von Remote-Zugängen für Management-funktionen von Routern		2, 3	i, e							
40	G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme (Telearbeitsplätze)		2, 3	i, e							
41	G 5.66	Unberechtigter Anschluß von IT-Systemen an ein Netz		2	i							
42	G 5.67	Unberechtigte Ausführung von Netzmanagementfunktionen		2, 3	i, e							
43	G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten		2	i							
44	G 5.73	Vortäuschen eines falschen Absenders		2, 3	i, e							
45	G 5.78	DNS-Spoofing		2, 3	i, e							
46	G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT		2, 3	i, e							
47												
48												

6 Entscheide für die Durchführung

Als Entscheidungshilfsmittel für die Auswahl der durchzuführenden Testmethoden, werden die Informationen der Tabelle Gefahrenanalyse (Kap. 5.3) grafisch dargestellt.

6.1 Darstellung der Resultate

Die untenstehende Grafik zeigt anhand *eines Beispiels* den Zusammenhang zwischen der Erfolgschance eines Angriffs und der Bedrohung für das System. Die Grafik kann somit als erstes Selektionskriterium für die Durchführungsplanung verwendet werden. Wichtig dabei ist, dass nach dieser Vorselektion für jeden Angriff die Risikobeurteilung (Spalte Nr. 11 der vorhergehenden Tabelle) sowie die entsprechenden Gegenmassnahmen (Spalte Nr. 12) beurteilt werden.



Diese Seite bleibt aus technischen Gründen leer.

Durchführung

1 Einleitung

Dieser Teil beschreibt die Phase der Durchführung einer Hacking-Attacke. Deren Ausführung kann die unterschiedlichsten Ziele haben – darum ist es wichtig, diese auch identifizieren zu können. Eine der Grundvoraussetzungen für eine erfolgreiche Realisierung wird sein, die richtige Methode zum richtigen Zeitpunkt anzuwenden.

2 Dienstleistungsangebot

Mittels einer Hacking-Attacke kann ein breites Dienstleistungsangebot unterstützt oder abgedeckt werden:

Dienstleistungsangebot	Beschreibung
Konformität überprüfen (Compliance)	Überprüfen der Einhaltung gesetzlicher Vorgaben und interner/externer Richtlinien
Awareness schaffen	Demonstrieren der potentiellen Verwundbarkeit
Schwachstellen analysieren	Ermitteln und analysieren von Schwachstellen
Risiken analysieren	Ermitteln und analysieren der Geschäftsrisiken
Businessprozesse auditieren	Überprüfen der Abläufe und Vorgehensschritte
Sicherheitsmassnahmen reviewen	Begutachten der eingesetzten Sicherheits-massnahmen
Zertifizierung HW/SW/System	Formale Evaluation nach ITSEC/CCSEC
Abnahme HW/SW/System	Durchführen von Abnahmetests und Ausstellen interner Zertifikate
Design-Review	Begutachten der verwendeten Architektur-designs

Eine Hacking-Attacke kann die verschiedensten Zwecke erfüllen; z.B. die Überprüfung bestimmter Parameter oder die Identifikation von Schwachstellen im zu überprüfenden System mit ihrer anschliessenden Behebung.

3 Methoden

Die Auswahl der Methode, um die gewünschte Dienstleistung zu erbringen, ist in den meisten Fällen schwierig. Die folgenden Methoden und Arbeitspakete wurden von uns als wesentlich und erwähnenswert identifiziert.

Arbeitspaket 1: Carrier Scan

Ein Carrier Scan umfasst die automatisierte Suche nach Modems (Carrier), die Anrufe entgegen nehmen. Je nach Konfiguration kann ein Modem ein “entry point” in das

interne Netz sein. Es stellt damit potentiell eine hohe Gefährdung dar. Zusammen mit einem schwachen Zugangsschutz (kein Passwort oder Standardpasswort) stehen einem Angreifer Tür und Tor offen, um jeglichen nur denkbaren Schaden anzurichten (Corruption or Disclosure of Information, Theft of Service, Denial of Service).

Ziel dieses Arbeitspaketes ist, ein Verzeichnis der von aussen zugänglichen Modems zu erhalten. Für jedes Modem wird angegeben, ob eine Benutzerauthentisierung durch Eingabe von Name und Passwort möglich ist (logon prompt erscheint).

Abgrenzung: In diesem Arbeitspaket wird der Zugangsschutz nur rudimentär geprüft. Dictionary- oder Brute-force-Angriffe sind Gegenstand der zweiten Phase.

Lieferobjekt-1: Modemverzeichnis

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes gibt der Auftraggeber den zu untersuchenden Telefonnummernbereich bekannt.

Arbeitspaket 2: Internet Scan

Ein Internet-Scan umfasst die automatisierte Suche nach Computersystemen und Netzwerk-Infrastrukturkomponenten (z.B. Router) über das Internet. Es werden mit Hilfe eines Internet-Scanning-Tool alle von extern sichtbaren Komponenten identifiziert und auf derzeit bekannte Schwachstellen untersucht. Dies macht nur Sinn für geroutete Netze, also für Komponenten mit einer öffentlich registrierten IP Adresse (z.B. Firewall, Web Server, Mail Server etc.).

Schwachstellen können verschiedenster Herkunft sein (z.B. Design, Implementation oder Konfiguration); sie haben je nachdem geringere oder grössere Auswirkungen auf die Gefährdung der betroffenen Komponente und des betroffenen Netzwerkes. Entsprechend werden Schwachstellen auch als “high”, “medium” oder “low severity” klassifiziert. Zusammen mit weiteren Attributen, die durch die Schwachstelle bekannt gegeben werden, kann dadurch eine sehr hohe Gefährdung einer Komponente oder auch eines Netzwerkes resultieren.

Beim Port- und auch Service-Scanning muss zwischen zwei Arten unterschieden werden. Diejenige, welche offensichtlich ist und auch ohne Probleme erkannt werden kann, und diejenige, die in den meisten Fällen unentdeckt bleibt. Beide sind als Teil der Informationsbeschaffung zu sehen und doch haben sie ein ungleichartiges Nebenziel. Die unentdeckte kann dazu dienen, das Sicherheitsbewusstsein von Systemadministratoren zu steigern und diese auf die Problematik zu sensibilisieren, indem das Resultat im nachhinein diskutiert wird. Die offensichtliche Variante kann dazu dienen, die tägliche Arbeit von Systemadministratoren zu überprüfen und zu verifizieren.

Ziel dieses Arbeitspaketes ist, eine ausführliche Analyse der von aussen zugänglichen Schwachstellen zu erhalten. Die Schwachstellen werden nach Herkunft kategorisiert und für jede Kategorie (oder wo sinnvoll für jede einzelne Schwachstelle) wird eine klassifizierte Empfehlung zur Behebung der Gefährdung angegeben. Die Klassifikation der Empfehlung orientiert sich an den Dimensionen Wichtigkeit und Dringlichkeit.

Abgrenzung: Bedingt durch technische Einschränkungen kann es vorkommen, dass eine bestehende Schwachstelle von intern aber nicht von extern identifiziert werden kann. Ebenso kann es vorkommen, dass eine nicht vorhandene Schwachstelle gemeldet wird (false positiv). Ersterem wird bis zu einem gewissen Grad in der zweiten Phase begegnet, während letzteres keine eigentliche Gefährdung darstellt, im Sinne des Qualitätsmanagements aber im Rahmen der Umsetzung überprüft werden sollte.

Lieferobjekt-2: Schwachstellenanalyse extern

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes gibt der Auftraggeber den zu untersuchenden IP-Adressbereich bekannt.

Alternative: Auf Wunsch kann dies auch nur durch Bekanntgabe einer Email- oder www-Adresse durchgeführt werden. In diesem Falle muss mit zusätzlichem Aufwand für die Ermittlung des IP-Adressbereichs gerechnet werden. Zwar ist die Ermittlung der IP-Adresse des Netzes, in welchem der Mail- oder der Webserver untergebracht sind, normalerweise eine Sache von Minuten und wird daher nicht separat verrechnet. Im Ausnahmefall muss aber mit einem grösseren Aufwand gerechnet werden. Unseres Erachtens ist es nicht sinnvoll, den Ziel-IP-Adressbereich nicht bekannt zu geben; es ist viel effizienter diese Grösse als gegeben zu betrachten. Voraussetzung für einen Internet-Scan ist, dass die Email- und/oder Webserver in der Verwaltung des Auftraggebers sind und nicht bei einem Serviceprovider stehen (web hosting).

Arbeitspaket 3: Password Cracking

Password-Cracking eignet sich zur Überprüfung der Umsetzung von Passwort-Richtlinien. Es muss jedoch bei der Realisierung bedacht werden, dass beliebige Passwörter geknackt werden können. Aus diesem Grund kann es von Seiten des Kunden wünschenswert sein, eine Vorselektion zu tätigen, um die Enthüllung solcher Passwörter zu vermeiden. Es ist aber klar, dass solche Ausschlüsse eine Abschwächung der Überprüfung darstellen und gleichzeitig ein nicht quantifizierbares Restrisiko darstellen.

3a Dictionary Attack (Password Cracking)

Eine Dictionary-Attacke umfasst das systematische Ausprobieren von Passwörtern für bekannte Zugangskennungen mit Hilfe eines Wörterbuches, das zahlreiche gängige Passworte enthält. Ziel dieses Arbeitspaketes ist die Prüfung der Qualität der verwendeten Passwörter. Grundsätzlich steigt der Zugangsschutz mit der zunehmenden Komplexität der eingesetzten Passwörter (Verwendung von langen Passwörtern mit gemischtem Zeichensatz; Buchstaben, Zahlen, Sonderzeichen). Die Verwendung von schwachen Passworten hingegen stellt eine sehr grosse Gefährdung dar.

Abgrenzung: Aufgrund der begrenzten Ressourcen (Zeit und Geld) können für eine derartige Untersuchung nicht sämtliche existierenden Wörterbücher verwendet werden. Es ist deshalb möglich, dass trotz einer erfolglosen Dictionary-Attacke ein Angreifer mit einem anderen Wörterbuch ein gültiges Passwort findet. Im Weiteren wird in diesem Arbeitspaket nicht untersucht, wie weit in das System eingedrungen werden kann; dies ist Gegenstand des Paketes 4.

Lieferobjekt-3: Passwort-Verzeichnis

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes bestimmt der Auftraggeber, welche Komponenten einer Untersuchung unterzogen werden sollen.

Alternative: Die Dictionary-Attacke kann sehr ressourcenaufwendig sein (Zeit und Geld). Es ist daher sinnvoll, dass der Auftraggeber einige User-Accounts mit zugehörigen Passwörtern liefert, so dass direkt das Arbeitspaket 4 ausgeführt werden kann.

3b Brute Force Attack (Password Cracking)

Eine Brute-force-Attacke umfasst den Versuch, für eine Zugangskennung das gültige Passwort durch vollständige Permutation zu ermitteln. Dabei werden alle möglichen Buchstaben- und Zahlenkombinationen systematisch durchprobiert und jeweils geprüft, ob ein gültiges Passwort gefunden wurde.

Ziel dieses Arbeitspaketes ist die Prüfung der verwendeten Passwörter. Grundsätzlich steigt der Zugangsschutz mit der zunehmenden Komplexität der eingesetzten Passwörter (lange Passwörter mit gemischtem Zeichensatz: Buchstaben, Zahlen, Sonderzeichen). Schwache Passwörter lassen sich mit solchen Verfahren innert Minuten herausfinden; sie stellen damit eine sehr grosse Gefährdung dar.

Abgrenzung: Aufgrund der begrenzten Ressourcen (Zeit und Geld) können für eine derartige Untersuchtung nicht sämtliche möglichen Kombinationen durchprobiert werden. Es ist daher normal, dass nach einer erfolglos abgebrochenen Brute-force-Attacke ein Angreifer ohne zeitliche Beschränkung dennoch in das System eindringen kann. Im weiteren wird in diesem Arbeitspaket nicht untersucht, wie weit in das System eingedrungen werden kann; dies ist Gegenstand des Paketes 4.

Lieferobjekt-3: Passwortverzeichnis

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes bestimmt der Auftraggeber, welche Komponenten einer Untersuchung unterzogen werden sollen. Zur Vereinfachung gibt der Auftraggeber weiter bekannt, wie lange die verwendeten Passworte sind.

Alternative: Die Dictionary-Attacke kann sehr ressourcenaufwendig sein (Zeit und Geld). Es ist daher sinnvoll, dass der Auftraggeber einige User-Accounts mit zugehörigen Passwörtern liefert, so dass direkt das Arbeitspaket 4 ausgeführt werden kann.

Arbeitspaket 4: Manuelles Hacking

Das manuelle Hacking umfasst den Versuch, eine identifizierte Schwachstelle auszunützen und so weit wie möglich in das System einzudringen. Ziel dieses Arbeitspaketes ist also, aufzuzeigen, wie weit in das interne Firmennetzwerk eingedrungen und welcher Schaden angerichtet werden könnte. Als Grundlage dienen dazu die Ergebnisse der Arbeitspakete 1 bis 3.

Abgrenzung: Es werden nur solche Methoden verwendet, die keinen Schaden an Systemen oder Daten verursachen. Es werden explizit keinerlei Daten gelöscht oder verändert, sondern höchstens darauf hingewiesen, dass dies auf diese oder jene Art und Weise möglich ist!

Lieferobjekt-4: Verwundbarkeitsbericht

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes bestimmt der Auftraggeber, welche Komponenten einer Untersuchung unterzogen werden sollen.

Arbeitspaket 5: Intranet Scan

Ein Intranet-Scan ist im wesentlichen dasselbe wie der Internet-Scan (Arbeitspaket 2), diesmal aber innerhalb des Netzwerkes. Er umfasst die automatisierte Suche nach Computersystemen und Netzwerken die intern sichtbar und zugänglich sind. Es werden mit Hilfe eines Intranet-Scanning-Tools alle von innen sichtbaren Komponenten identifiziert und auf derzeit bekannte Schwachstellen untersucht.

Diese Methode beinhaltet auch das Paket-Sniffing, welches passiv ist und praktisch keiner Eingriffe in eine bestehende Netzwerkarchitektur bedarf. Dennoch gilt es einen wichtigen Punkt zu beachten: Beim Sammeln der Pakete können mit dem Sniffer neben Klartext-Passwörtern auch streng geheime Dokumente des Kunden (z.B. Strategiepapiere) protokolliert werden. Weiter sollte der Kunde darauf aufmerksam gemacht werden, dass auch die Passwörter der Geschäftsleitung vor einem Sniffer-Angriff nicht sicher sind. Sniffing kann sowohl intern als auch extern dazu dienen, um die Verwundbarkeit der Vertraulichkeit infolge fehlender Chiffrierung zu demonstrieren.

Im Gegensatz zum Arbeitspaket 2 ist die Durchführung dieses Arbeitspaketes auch sinnvoll für nicht geroutete Windows NT- oder UNIX-Netze. In diesem Fall ist die Optik auf die internen Gefahren gerichtet. Es ist notwendig, dass Systeme und Daten nicht nur gegen externe sondern auch gegen interne Angriffe geschützt sind. Eine out-of-the-box-Konfiguration eines Windows NT-Servers reicht zum Beispiel in den meisten Fällen nicht aus, um eine angemessene Sicherheit im eigenen LAN zu gewährleisten.

Ziel dieses Arbeitspaketes ist eine möglichst ausführliche Analyse der von innen zugänglichen Schwachstellen. Die Schwachstellen werden nach Herkunft kategorisiert und für jede Kategorie (oder wo sinnvoll für jede einzelne Schwachstelle) wird eine klassifizierte Empfehlung zur Behebung der Gefährdung angegeben. Die Klassifikation der Empfehlung orientiert sich an den beiden Dimensionen Wichtigkeit und Dringlichkeit.

Interne Informationsanalysen sind eine absolute Notwendigkeit, um ein reales Abbild der gesamten Sicherheit einer Architektur zu erhalten. Oft werden Systeme durch irgendwelche zusätzlichen, aussenliegenden Schutzmechanismen geschützt. Falls diese Schutzsysteme ihre Aufgabe adäquat erledigen, kann von aussen her die Sicherheit des eigentlichen Zielsystems nicht bewertet werden. Die Beurteilung der inneren

Sicherheit ist aber im Allgemeinen sehr wichtig, da eine unbeabsichtigt hinzukommende Schwachstelle im aussenliegenden Schutzsystem das Zielsystem exponieren würde, falls dieses selbst ungenügend geschützt ist.

Abgrenzung: Auch hier können technische Einschränkungen dazu führen, dass nicht alle Schwachstellen identifiziert werden können. Dem daraus entstehenden Restrisiko kann durch die Verwendung eines Intrusion-Detection-Systems begegnet werden, das regelbasierte Angriffsversuche erkennen und melden kann. Dies erweitert die statische Untersuchung um eine zusätzliche dynamische Dimension im Betrieb.

Manchmal werden bei der Untersuchung nicht vorhandene Schwachstellen gemeldet werden (false positiv). Dies stellt eigentliche keine Gefährdung dar, sollte aber im Sinne des Qualitätsmanagements weiter überprüft werden.

Lieferobjekt-5: Schwachstellenanalyse intern

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes gibt der Auftraggeber den zu untersuchenden IP-Adressbereich bekannt. Für die Analyse ist es erforderlich, dass das Werkzeug des Auftragnehmers (in der Regel ein Laptop mit installierter Scanning-Software) ans interne Netzwerk angeschlossen werden kann. Der Auftraggeber stellt dazu einen entsprechenden Anschluss zur Verfügung.

Arbeitspaket 6: System Scan

Kritische Computersysteme (Netzwerkserver, Webserver u.a.) sollten nach dem Minimumprinzip konfiguriert werden. Oftmals reicht eine out-of-the-box-Installation nicht aus, um einen Server “sicher” zu konfigurieren: Es sind Sicherheitspatches zu installieren, Dienste zu deaktivieren oder Systemparameter zu setzen. Mit Hilfe eines System-Scanning-Tool werden diese Computersysteme einer genauen Konfigurationsprüfung unterzogen.

Ziel dieses Arbeitspaketes ist, eine möglichst ausführliche Analyse der Schwachstellen zu erhalten. Die Optik ist auf die korrekte und sichere Konfiguration eines bestimmten Betriebssystemtyps (UNIX, Windows NT) gerichtet und es wird gefragt: “Wo sind meine Schwachstellen?”. Bis zu einem gewissen Grad überschneidet sich dies mit den Ergebnissen der Arbeitspakete 2 und 5, welche eine Systempenetration (“Ich bin ein Angreifer, wie kann ich eindringen?”) in den Vordergrund stellen.

Die Schwachstellen werden nach Herkunft kategorisiert und für jede Kategorie (oder wo sinnvoll für jede einzelne Schwachstelle) wird eine klassifizierte Empfehlung zur Behebung der Gefährdung angegeben. Die Klassifikation der Empfehlung orientiert sich an den beiden Dimensionen Wichtigkeit und Dringlichkeit.

Abgrenzung: Die Durchführung dieses Arbeitspaketes macht eigentlich nur Sinn, wenn beabsichtigt ist, die Zielsysteme einer regelmässigen Kontrolle zu unterziehen. Die Konfigurationsprüfungen können automatisiert und periodisch (zum Beispiel beim Systemstart) wiederholt werden. Im Arbeitspaket enthalten ist deshalb eine Instruktion des Systemadministrators.

Lieferobjekt-6: Konfigurationsprüfung

Lieferung des Auftraggebers: Für die Durchführung dieses Arbeitspaketes gibt der Auftraggeber die zu untersuchenden Computersysteme (IP-Adressen) bekannt. Der benötigte System-Scanner kann entweder auf dem Laptop des Auftragnehmers oder einem System des Auftraggebers installiert werden. Idealerweise stellt der Auftraggeber einen Ansprechspartner zur Verfügung, der bei der Konfiguration des System Scanners behilflich ist und zur weiteren Benützung des Programms geschult werden darf.

Arbeitspaket 7: Phreaking

Mittels Phreaking können Systeme überprüft werden, welche im Zusammenhang mit dem Telefonnetz stehen, also alle Systeme, die dieses Netz nutzen oder Netzkomponenten sind. Auch hier gilt es zu beachten, dass sich die Tests auf Elemente beschränken, für welche ein Auftrag besteht und bei denen der Kunde auch berechtigt ist, die Ermächtigung für solche Tests zu erteilen.

Arbeitspaket 8: Analyse von Vertrauensbeziehungen

Oft bestehen Beziehungen zu Geschäftspartnern, Kunden oder Lieferanten, bei denen davon ausgegangen wird, dass sie keinerlei Risiken für die eigene Sicherheit darstellen. Eine Analyse solcher Vertrauensbeziehungen soll aufzeigen, ob dieses blinde Vertrauen berechtigt ist oder ob mangelnde Sicherheit und die Möglichkeit eines einfachen Zuganges ein potentielles Risiko für eine Kompromitierung der gesamten Sicherheit darstellen.

4 Werkzeuge

Mit der Hilfe von sogenannten Werkzeugen ist es möglich, die Methode in die Tat umzusetzen. Die richtige Auswahl der Methode zur Abdeckung des gewünschten Dienstleistungsangebots ist essentiell. Auf der anderen Seite ist es jedoch genauso wichtig, die richtigen Werkzeuge zu identifizieren, konfigurieren und einzusetzen. Der Begriff Werkzeuge soll an dieser Stelle ausgedehnt werden. Werkzeuge sind nicht nur Programme, welche einen bestimmten Nutzen bringen, sondern generell Techniken, die es ermöglichen, eine Hacking-Attacke zu unterstützen oder zum Ziel zu bringen. Dabei wird davon ausgegangen, dass sowohl automatische als auch manuelle Techniken dazugehören.

Grundsätzlich kann bei Werkzeugen zwischen kommerziellen und nicht-kommerziellen unterschieden werden. Beide bieten Vor- und Nachteile, die anschliessend im Einzelnen erläutert werden. Ein wesentlicher Unterschied zwischen kommerziellen und nicht-kommerziellen Tools besteht darin, dass mit den Erstgenannten effektiv Attacken auf Systeme durchgeführt werden können. Hierbei gilt es anzumerken, dass diese individuell auf verschieden Betriebssystemplattformen angepasst werden können. Bei den nicht-kommerziellen beschränkt sich die Möglichkeit einer Attacke, wenn überhaupt, auf ein einziges Betriebssystem. Die Mächtigkeit der kommerziellen Tools ist eindeutig

grösser, was die Möglichkeiten einer erfolgreichen Attacke anbelangt. Aus diesem Grund wird sich der Benutzer registrieren lassen müssen. Es ist leicht vorstellbar, dass jedem Anfänger uneingeschränkte Möglichkeiten geboten werden, falls solche Tools plötzlich keiner Registrierung mehr bedürfen, weil ihr Gebrauchsschutz geknackt wurde.

Kommerzielle Werkzeuge

Der Einsatz kommerzieller Werkzeuge ist im Normalfall mit Kosten für deren Nutzung verbunden. Der finanzielle Aufwand bietet aber nebst der Nutzung in den meisten Fällen auch einige Extras. So kann zum Beispiel auf eine produktspezifische Beratung zurückgegriffen werden, die zum Teil sogar Schulung beinhaltet. Des Weiteren kann ein gewisses aber begrenztes Vertrauen gegenüber diesem Werkzeug entgegengebracht werden. Die Wahrscheinlichkeit, dass ein Tool Informationen an Dritte sendet, ist bei kommerziellen Tools um einiges geringer als bei nichtkommerziellen. Der Hersteller ist durch einen Kaufvertrag an das Gesetz gebunden. Seine Haftbarkeit ist in den meisten Fällen gewährleistet. Je grösser die Verbreitung des Einsatzes eines solchen Tools ist desto mehr kann von einer gewissen Seriosität ausgegangen werden. Es darf jedoch auch bei solchen Werkzeugen kein blindes Vertrauen in diese gesetzt werden.

Nicht-kommerzielle Werkzeuge

Der Einsatz nicht-kommerzieller Werkzeuge, sogenannter “freeware”, ist prinzipiell mit Risiken verbunden. Es gibt aber Möglichkeiten, diesen Risiken so zu entgegnen, dass sich diese auf einen akzeptablen Rest reduzieren lassen. Für solche Werkzeuge liegt der Quellencode meist nicht vor und es kann somit am Anfang nicht genau gesagt werden, wie es sich verhält. Es ist zum Beispiel möglich, dass ein Tool Informationen sammelt und diese an eine Adresse im Internet weitersendet. Dass es sich dabei nicht nur um selten eintreffende Möglichkeiten handelt, zeigen die zahlreichen Fälle aus der Praxis. Es ist deshalb absolut notwendig, solche Produkte vor ihrem ersten Einsatz ausgedehnt zu testen. Damit kann so manche böse Überraschung vermieden werden.

Ein weiteres Risiko ist, die Haftbarkeit beim Eintreten eines Schadenfalles. Die Haftung wird schlussendlich auf den zurückgreifen, der das Tool eingesetzt hat. Nicht-kommerzielle Werkzeuge bieten zwar den Vorteil, dass sie gratis sind, sie haben aber den Nachteil, dass sie zahlreiche Risiken in sich bergen, die nur teilweise identifiziert werden können.

Reporting

1 Einleitung

Als Mitglied eines Tiger-Teams in einem Hacking Auftrag bewegt man sich in einer Grauzone zwischen Recht und Unrecht. Damit das im Auftrag handelnde Tiger-Team sich und seine Handlungen jederzeit vor sich selbst, dem Auftraggeber und der Öffentlichkeit verantworten kann, ist eine genaue und offene Dokumentation notwendig.

Dieses Kapitel stellt eine Arbeitshilfe dar für die Dokumentation eines Hacking-Projektes, wie es von der Arbeitsgruppe Tiger-Team definiert worden ist. Dieser Teil ist kein Rezeptbuch sondern fasst konzentriert die Erfahrung der Mitglieder der Arbeitsgruppe im Erstellen von Projektdokumentationen bei ähnlich gelagerten Projekten zusammen.

Wir haben eine Projektdokumentation mit entsprechender Strukturierung so aufgestellt, dass wesentliche Informationen an den richtigen Orten untergebracht werden können. Wichtige Dokumente und ihre Kapitel wurden entsprechend bezeichnet. Grundsätzlich sollte ausreichend Spielraum eingeräumt worden sein, damit jedes Tiger-Team seinen eigenen Schreibstil pflegen kann.

Das vorgestellte Projekt-Informationssystem definiert den Informationsfluss zwischen Auftraggeber und Auftragnehmer. Die verwendeten Kommunikations- und Informationspapiere werden kurz aufgeführt.

Das wichtigste Ergebnis einer durchgeführten Hacking-Attacke ist der Abschlussbericht. Daher wird auf seine Gestaltung besonders eingegangen. Damit aus einem Hacking-Auftrag nicht unverhofft ein Nachspiel entsteht, werden Empfehlungen abgegeben, wie ein solches Projekt dokumentiert und diese Dokumentation aufbewahrt werden sollte.

2 Projekt-Informationssystem

Eine klare, offene und schnelle Kommunikation über Aktivitäten, Erfolge, Gefahren und Unregelmässigkeiten ist enorm wichtig. Die Handlungen müssen nachvollziehbar sein. Daher wird an dieser Stelle ein mögliches Projektinformationssystem vorgeschlagen:

- Offerte
- Protokolle
- Aktennotiz
- Bericht

2.1 Offerte

Ziel: Definition des Auftrages und seiner Abgrenzung

Die Offerte wird zu Rate gezogen, wenn Unstimmigkeiten bezüglich der folgenden Punkte bestehen:
1. Verantwortlichkeiten
2. Ansprechpartner
3. zu erbringende Leistungen
4. finanzielle Auswirkungen
5. rechtliche Auswirkungen

Die Offerte ist tätigkeitsorientiert abzufassen. Entsprechende Empfehlungen sind im Abschnitt Vertrag formuliert.

2.2 Protokoll

Ziel: Wertfreie und objektive Darstellung der Sachverhalte

Mit einem Protokoll sollen Projektbeteiligte, Firmenverantwortliche und Revisionsstellen in einer prägnanten Art über den aktuellen Projektstand informiert werden. Protokolle widerspiegeln den chronologischen Verlauf eines Projektes und bilden somit ein wichtiges Instrument für die Rückverfolgbarkeit des Projektablaufs. Mindestens die folgenden Informationen sollten mindestens in einem Protokoll enthalten sein:
1. durchgeführte Aktivitäten
2. gesammelte Daten und Informationen (nur Bezeichnung, keine Details)
3. Beschlüsse in Sitzungen
4. Teilnehmer bei Beschlüssen

Die Protokolle sollten den Projektablauf und allfällige Abweichungen zu offerierten oder abgesprochenen Tätigkeiten auch im nachhinein klar ersichtlich darstellen. Das Mitführen einer Projekt-Pendenzenliste vereinfacht die Projektlenkung.

2.3 Aktennotiz

Ziel: Die Aktennotiz stellt ein wichtiges Detail vorwiegend technischer Natur dar.

Jede Aktennotiz sollte nur ein Thema behandeln. In einer Aktennotiz sollten mindestens die folgenden Informationen enthalten sein:
1. Themengebiet
2. Zusammenhang zum Projekt wie Projektschritt oder Meilenstein
3. Wichtigkeit für das Projekt
4. Herkunft der Information
5. Weiterführende Informationen

Zusammen mit den Protokollen sollte bei einer Projekt-Review durch unabhängige Stellen der Projektablauf sichtbar und nachvollziehbar sein.

2.4 Bericht

Ziel: Zusammenfassung der im Projekt erarbeiteten Resultate in einer zusammenhängenden Form.

Der Bericht verkörpert die vom Auftraggeber bestellte Dienstleistung. Im Bericht sollte in ausführlicher und strukturierter Art auf die im Projekt erarbeiteten Resultate eingegangen werden. Die Resultate sollten mit anschaulichen Beispielen, Grafiken und Tabellen untermauert werden. Mindestens die folgenden Informationen sollten in einem Bericht enthalten sein:

1. Übersicht
2. Arbeitsumfang
3. Ausgangslage und Problemstellung
4. Projektziele
5. eingesetze Methoden
6. Resultate
7. Empfehlungen

Der Bericht stellt eine subjektive Darstellung des Projektablaufes aus der Sicht des Projekteams dar. Nachfolgend wird auf die Strukturierung des Abschlussberichts genauer eingegangen.

3 Aufbau Abschlussbericht

3.1 Zusammenfassung (Management Summary)

Dies ist das wichtigste Kapitel des ganzen Berichts. Es wird mit hoher Wahrscheinlichkeit vom oberen Management des Auftraggebers gelesen. Daher ist es die Stelle, das Hacking-Projekt der Geschäftsleitung zu verkaufen.

In der Regel werden Zusammenfassungen in Randstunden oder als Lückenfüller gelesen. Daher ist bei der Redaktion dieses Teils besonders auf den Schreibstil und die Verständlichkeit der Erläuterungen zu achten.

Die Zusammenfassung beschreibt kurz und informativ folgende Fragenstellung des Hacking-Projektes:

1. Was war das Problem?
2. Wo liegen die Schwerpunkte?
3. Was für Methoden und Hilfsmittel wurden verwendet?
4. Was wurde festgestellt?
5. Welchen Einfluss haben die Resultate auf den Auftraggeber?

Der Umfang sollte eine Seite nicht übersteigen. Alle wichtigen Erkenntnisse mit ihren Auswirkungen sollten in einer kurzen und prägnanten Weise wiedergegeben werden. Jeder Satz sollte dabei nur einen Sachverhalt erläutern. Die Zusammenfassung muss vom Leser mühelos innerhalb von Minuten gelesen werden können.

3.2 Arbeitsumfang (Scope)

Der Projektrahmen wird klar dargestellt. Insbesondere wird das Projekt klar abgegrenzt. Es wird dargelegt, worauf verzichtet worden ist und welches die Gründe dafür sind. Grundsätzlich kann nach dem folgenden Raster vorgegangen werden:

1. strategische Ausrichtung
2. Vorselektion bei der Risikoanalyse
3. Handlungsbedarf
4. Fokus
5. Hemmschwellen
6. Barrieren

Oft treten während des Projektes Sachverhalte auf, welche nicht durch den Vertrag gedeckt sind, und deren Wichtigkeit der Auftraggeber nicht erkennen will oder für das Projekt tatsächlich nicht von Bedeutung sind. Diese Einschränkungen sollten entsprechend dargelegt werden. Solche "Barrieren" könnten folgende Sachverhalte sein:

- Einschränkungen durch Technologie;
- Probleme infolge von Inkompatibilität z.B. bei der Auswertung der Protokolle;
- Mangel an Ressourcen technischer und personeller Art.

3.3 Ausgangslage und Problemstellung

Dieses Kapitel beschreibt die Situation, wie sie vor der Lancierung des Projektes angetroffen wurde. In der Regel basiert die Ausgangslage auf einer zuvor erstellten Grundlagenanalyse und der daraus erkannten Problemstellung, wie sie im Rahmen der Offertenstellung gesehen wurde.

Dieses Kapitel ist die Grundlage für die Tätigkeit des Auftraggebers und die Bemessung seines Erfolges. Bei der Formulierung sollten die folgenden Punkte beachtet werden:

- Probleme auf Sachzwänge zurückführen und nicht auf Personen beziehen;
- nur offizielle Quellen des Auftraggebers oder öffentliche Medien verwenden, zitieren und referenzieren.

3.4 Projektziele

Dieses Kapitel beschreibt die Erwartungshaltung des Auftraggebers. Nach Möglichkeit sind die Formulierungen des Auftraggebers zu übernehmen. Eine Aufzählung nach dem folgenden Muster ist zu empfehlen:

1. Darstellung der übergeordneten Projektziele
2. Darstellung der unmittelbaren Projektziele, welche aus der Offertstellung hervorgehen
3. Darstellung der Kernziele

3.5 Vorgehen und eingesetzte Methoden

Dieses Kapitel beschreibt die unternommenen Tätigkeiten, wie sie in der Offerte formuliert worden sind. Der oberflächliche Beschrieb aus der Offerte wird in diesem Teil genau ausgeführt und entsprechend mit Tabellen, Grafiken untermauert. Es wird das nachfolgende Raster empfohlen:

1. Beschreibung des Vorgehens und Begründung desselben, wie es in der Risikoanalyse festgelegt worden ist
2. Beschreibung der eingesetzten Tools und ihrer Wirkungsweise und Untermauerung mit echten Daten aus dem Projekt
3. Darlegung der Grenzen der eingesetzten Mittel

3.6 Resultate (Diagnose)

Dieses Kapitel ist der Kern des Berichtes. Es ist direkt an den Auftraggeber gerichtet, der brennend an den Inhalten interessiert ist. Auf eine umfassende, strukturierte und folgerichtige Darstellung der Resultate sollte daher besonders geachtet werden. Die Aussagen (z.B. über mögliche Auswirkungen) sollten mit Grafiken, Tabellen und Präzedenzfällen untermauert werden.

Feststellungen

Feststellungen sollten einzeln aufgeführt werden. Jede Feststellung hat bestimmte

1. Merkmale
2. Ursachen
3. Auswirkungen

Die Darstellung der Begründung der einzelnen Befunde wird dadurch erschwert, dass viele Befunde auf statistischen Daten basieren. Aussagen, welche auf Wahrscheinlichkeiten basieren, sind keine eindeutige Aussagen und können nicht verbürgt werden. Dieser Sachverhalt ist sehr deutlich hervorzuheben.

Mögliche Auswirkungen

Die einzelnen Befunde können einzelnen oder in ihrer Verbindung unterschiedliche Konsequenzen für den Auftraggeber haben. Die Wertung der einzelnen Befunde und ihre Abhängigkeit sind dem Auftraggeber darzustellen. Für die Verdeutlichung können auch ähnlich gelagerte Fälle aus öffentlichen Quellen hilfreich sein So werden von Fachorganisationen oder statistischen Ämtern regelmässig umfassende statistische Daten veröffentlicht.

Die Auswirkungen der einzelnen Befunde können entweder im einzelnen oder in ihrer Verbindung unterschiedliche Konsequenzen für den Auftraggeber haben. Die Wertung der einzelnen Befunde und ihre Abhängigkeit ist dem Auftraggeber darzustellen. Für die Verdeutlichung können auch ähnlich gelagerte Fälle aus öffentlichen Quellen hilfreich sein. So werden von Fachorganisationen oder statistischen Ämtern regelmässig umfassende statistische Daten veröffentlicht.

Empfehlungen mit Dringlichkeit und Wichtigkeit

Die einzelnen Befunde deuten auf Schwachstellen hin. An dieser Stelle ist es in der Regel möglich, punktuelle Abhilfemassnahmen zu benennen. Häufig ist aber die Ursache in einem fehlenden übergreifenden Konzept zu suchen. Eine solche Neukonzeption ist in der Regel mit grossem Aufwand verbunden und daher nicht Gegenstand eines Hacking-Projektes.

Sehr wohl kann aber aufgrund der Kenntnisse über den Aufwand zur Überwindung einer Sicherheitshürde und den daraus resultierenden Auswirkungen eine grobe Prioritätenliste für die Behebung der Sicherheitslöcher erstellt werden.

Stellungnahme des Auftraggebers

Der Auftraggeber sollte zu den vorgefundenen Befunden, Empfehlungen und Dringlichkeiten aus seiner Sicht Stellung nehmen. Dies ist wichtig für eine Entlastung des Auftragnehmers.

Geplanter Fertigstellungstermin

Sofern möglich, ist ein genereller Massnahmenplan aufzustellen, in welchem die vorzunehmenden Korrekturmassnahmen nach Etappen und Meilensteinen gegliedert werden. Der zeitliche Horizont wird dabei festgelegt. Die dringendsten Massnahmen sollte dabei in der ersten Etappe eingeleitet werden.

Sofortmassnahmen

Gravierende Befunde werden benannt. Gleichzeitig wird ein Termin für die Vollendung von Sofortmassnahmen festgelegt.

4. Projektdokumentation

Im Rahmen eines Hacking-Projektes fallen Unmengen von Datenmaterial an. Für die Dokumentation der Befunde ist aber nur ein Teil dieser Daten notwendig. Das restliche Material wird in der Regel nicht mehr verwendet. Daher ist für die Aufbewahrung das Prinzip der *Wesentlichkeit* anzuwenden.

Allerdings muss vielleicht zu einem späteren Zeitpunkt infolge eines Schadenfalles oder aufgrund neuer Erkenntnisse auf das Projekt zurückgegriffen werden. In einem solchen Fall kann für die Durchführung einer Neubeurteilung die gesamte Datenmenge von Interesse sein.

Für den Auftragnehmer ist vor allem wichtig, dass diese Daten ihn und seine Arbeit entlasten könnten. Daher ist eine umfassende Messdatenmenge geeignet beim Auftragnehmer aufzubewahren.

4.1 Klassifizierung der Projektunterlagen

Eine Klassifizierung der Projektdaten ist zu empfehlen. So können brisante Erkenntnisse, welche für die taktische Schlagkraft des Auftraggebers wesentlich sind, von irrelevanten Daten getrennt werden. Diese irrelevanten Daten können dann ohne weiteres zur Publikation von Highlights in Informationsprospekten des Auftraggebers und des Auftragnehmers eingesetzt werden. Als Klassifizierung hat sich eine Dreistufigkeit bewährt:

- frei
- vertraulich
- geheim

Eine sinnvolle Zuordnung könnte wie folgt aussehen:

- Unklassifizierte Informationen sind der Öffentlichkeit zugänglich.
- Vertrauliche Informationen sind nur dem Projektteam zugänglich.
- Geheime Informationen sind nur der Geschäftsleitung zugänglich.

4.2 Kategorien der Arbeitspapiere

Arbeitspapiere sind grundsätzlich durch ihre Funktion kategorisiert. Es ist dabei unwesentlich, ob sie in elektronischer oder in Papier-Form vorliegen.

- Verträge mit Nachträgen
- Protokolle Sitzungen
- Aktennotizen
- Notizen
- Berichte/Studien/Analysen
- Messprotokolle und Logfiles

4.3 Aufbewahrung

Die Projektinformationen sind grundsätzlich als “vertraulich” zu kennzeichnen und entsprechend aufzubewahren.

Von den Projektdaten sollten mindestens die folgenden Papiere aufbewahrt werden:

- Verträge
- Protokolle von Sitzungen
- Aktennotizen
- Berichte/Studien/Analysen
- Messprotokolle

Grundsätzlich müssen die Papiere unter Verschluss aufbewahrt werden. Geheime und vertrauliche Dokumente sind zusätzlich zu verpacken, damit ein unbefugtes Öffnen der Verpackung klar ersichtlich ist.

Besteht der Bedarf, die Dokumente in elektronischer Form aufzubewahren, wird empfohlen, sich an bewährte, stabile und produkteneutrale Standards zu halten. Nach Möglichkeit ist eine ausgedruckte Form parallel abzulegen. Allerdings bedingt die

Fülle von Logdaten, welche von Scanning-Werkzeugen generiert werden, eine Aufbewahrung in elektronischer Form.

Geheime und vertrauliche Daten müssen auf dem Server und dem Laptop mit Verschlüsselung gegen unbefugtes Einsehen geschützt werden. Hierfür gibt es eine grosse Auswahl von Verschlüsselungslösungen.

4.4 Archivierung

Die Gesetze schreiben minimale Aufbewahrungszeiten für Projektdaten vor. Für die Dauer der Archivierung ist die Verjährungsfrist des Projektes zu berücksichtigen. Grundsätzlich gelten für die Archivierung dieselben Sicherheitsgrundlagen wie für die Aufbewahrung.

Ein grosser Teil der Projektdaten wird in elektronischer Form abgelegt. In einem solchen Fall ist zu bedenken, dass der Innovationszyklus gemäss dem Gesetz von Moore bei der elektronischen Datenverarbeitung nur ca. 18 Monate beträgt – das heisst, dass eine neue Technologie bereits nach kurzer Zeit von ihrem Nachfolger abgelöst wird. Sollten auf diese Weise Daten geschützt werden, welche länger wie 18 Monate aufbewahrt werden müssen, so muss eine Wiederherstellung gewährleistet werden können. Sinnvoll aber nicht immer möglich ist, einen Arbeitsplatz in Originalform zu konservieren. Die Abstützung auf Marktleader Quasistandards hat sich in der Vergangenheit als wenig erfolgsversprechend bewiesen, da diese oft in sich selbst nicht kompatibel sind.

Die Dokumentation, welche dem Kunden mit dem Projektabschluss übergeben wird, beinhaltet nicht die vollständige Datensammlung. In der Projektdokumentation werden nur relevante Daten abgegeben. Daher sollten umfassende Ablagen der eigenen Notizen und Messprotokolle angelegt werden. Diese könnten zu einem späteren Zeitpunkt bei allfälligen Streitfällen Informationen beinhalten, welche für eine Entlastung des Auftragnehmers sehr wichtig sind.

5 Anhang

5.1 Beispiel eines Projektdokumentes: Protokoll

Protokoll			
Protokoll Nr.:			
Kunde:			
Projekt:			
Phase:			
Datum:			
Zeit:			
Ort:			
Teilnehmer	Name	Firma	E-Mail
Verteiler	Teilnehmer		
Inhalt			
1. Stand Projekt			
2. Durchgeführte Aktivitäten			
3. Zwischenresultate			
4. Problematik			
5. Weiteres Vorgehen			
6. Pendenzen			

Fortsetzung des Beispiels

Pendenzen, offen

Nr.	Bezeichnung	Zuständig	Termin	Status

Pendenzen, erledigt

Nr.	Bezeichnung	Zuständig	Termin	Status

Fallbeispiel Gefahrenanalyse Client-Software

1 Einleitung

Dieses Kapitel beschreibt an einem Beispiel die Gefahrenanalyse einer Client-Software mit Hilfe von Tiger-Teams.

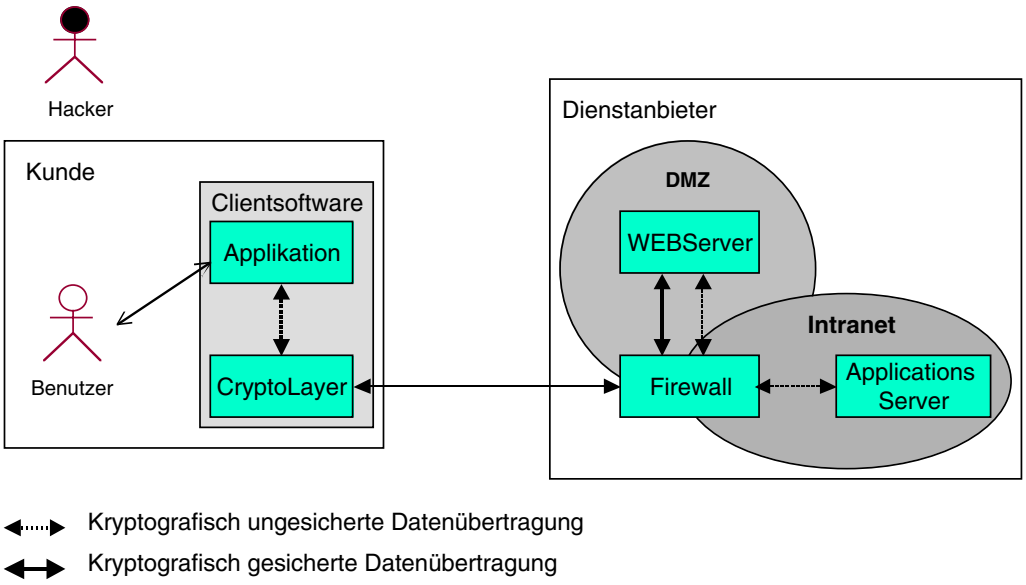
2 Definitionen

Die folgenden Abschnitte definieren den Einsatzbereich der Client-Software sowie die Betriebsumgebung.

2.1 Übersicht

Ein Standardisierungsgremium verwaltet Standards von verschiedenen Bereichen und bietet diese auf dem Internet zum Download an. Das Abstrakt eines Standards kann jeweils unentgeltlich über HTTP oder HTTPS bezogen werden. Den ganzen Standard können aber nur die Mitglieder des Gremiums beziehen, die über ein persönliches Benutzerzertifikat verfügen, welches über das HTTPS Protokoll verifiziert wird. Dieses Zertifikat wird verwendet, um den Download zu verrechnen.

2.2 Firewall



Die Firewall grenzt die DMZ und das Intranet vom Internet ab. Eine Attacke auf die Konfiguration und Segmentierung des Netzwerks sowie auf die Firewall werden mit *"Erfolg unwahrscheinlich (1)"* eingestuft.

2.3 WEB-Server

Der Server ist das Eingangsportal des Standardisierungsgremiums. Er steht in der DMZ der Firewall. Die Scripts und Servlets auf dem WEB-Server sind gut implementiert und weisen keine offensichtlichen Sicherheitslücken auf. Die Erfolgschancen für eine Attacke auf den WEB-Server und dessen Scripts werden mit *"Erfolg möglich (2)"* eingestuft.

2.4 Applikations-Server

Der Applikations-Server verwaltet die Dokumente und verrechnet die Downloads. Er steht im gesicherten Bereich der Firewall. Die Erfolgschancen für eine Attacke auf den Applikations-Server werden mit *"Erfolg unwahrscheinlich (1)"* eingestuft.

2.5 Client-Software

Die Client-Software ist das Mensch-Maschinen-Kommunikationsinterface. Sie verarbeitet die Eingaben des Benutzers, visualisiert Daten und steht in Verbindung mit einem Server. Der Client verwaltet zudem das persönliche Zertifikat des Benutzers.

2.6 Hacker

Der Hacker möchte die kostenpflichtigen Dienste in Anspruch nehmen, ohne dafür zu bezahlen.

3 Analyse möglicher Attacken

In diesem Kapitel werden mögliche Attacken und deren Erfolgschancen aufgezeigt.

3.1 Sniffing, Spoofing und Source-Routing

Da die kostenpflichtigen Dienste kryptografisch gesichert sind, kann mit Sniffing nichts erreicht werden. Im weiteren wird davon ausgegangen, dass die Client-Software gegen Spoofing und Source-Routing Attacken resistent ist. Dies kann durch eine entsprechende Implementation gewährleistet werden.

3.2 Hacken des WEB-Servers und des Applikationsservers

Der WEB-Server steht in der DMZ der Firewall. Der Applikations-Server steht im gesicherten Bereich der Firewall. Das Protokoll zwischen dem WEB-Server und dem Applikations-Server ist proprietär. Falls der WEB-Server erfolgreich attackiert würde, müsste der Hacker das proprietäre Protokoll zwischen dem WEB-Server und dem Applikations-Server reengineeren oder kennen. Der Aufwand dafür wird als hoch eingestuft und steht in keinem Kosten-/Nutzen-Verhältnis.

3.3 Social Engineering

Social Engineering ist eine sehr effiziente Methode, ein System zu attackieren. Dieses Beispiel geht nicht auf die möglichen Praktiken und Erfolgschancen ein.

3.4 Kompromittieren der Client-Software

Oftmals werden die Erfolgschancen möglicher Attacken auf der Serverseite genau analysiert und gewichtet. Dabei wird die Clientseite vernachlässigt oder fast ganz ausser acht gelassen. Das folgende Kapitel beschreibt zwei mögliche Attacken auf die Client-Software.

4 Kompromittierung der Client-Software

4.1 Definition

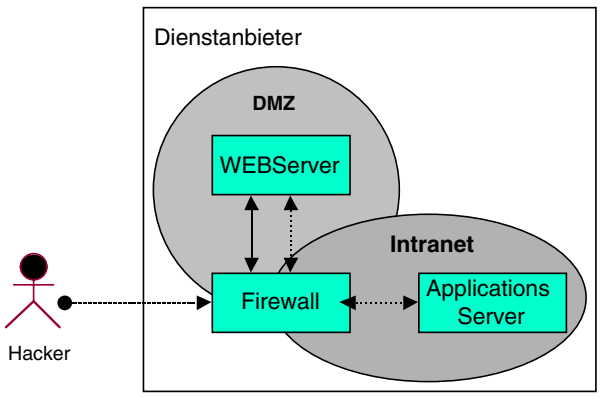
Die Kompromittierung der Client-Software hat das Ziel, die Identität des jeweiligen Benutzers anzunehmen.

4.2 Integritätsschutz der Client-Software

Eine Applikation kann man begrenzt gegen Viren oder Trojanische Pferde schützen. Die Applikation kann z.B. bei jedem Aufstarten die eigene Integrität prüfen, um allfällige Manipulationen am Code zu entdecken. Grundsätzlich ist es aber nicht möglich, eine Applikation hundertprozentig gegen Manipulationen zu schützen. Durch Reengineering ist es immer möglich, einen bestehenden Schutzmechanismus zu umgehen. Der Aufwand für das Reengineering kann lediglich erhöht werden.

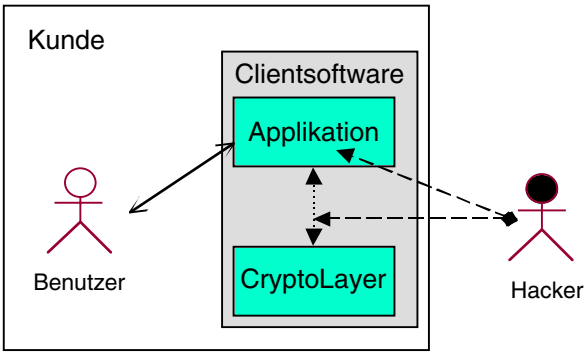
4.3 Motivation

Die Server-Komponenten eines Dienstanbieters sind meist gut konzipiert und entsprechend gegen Attacken gesichert. Diese erfolgen über das Internet und können mit entsprechendem Aufwand zurückverfolgt werden. Hat ein Hacker die Sicherungen der Server-Komponenten erfolgreich umgangen, muss er Zugriff auf den Applikations-Server erlangen, um einen Nutzen aus der Attacke zu ziehen. Dies verlangt oftmals Insiderwissen, da die dort verwendeten Protokolle häufig proprietär sind.



Daher kann es attraktiv sein, die Client-Software zu attackieren. Der Hacker hat beliebig lange Zeit, um die Client-Software zu reingeneeren. Er muss sich nicht um die darunterliegenden Schutzmechanismen kümmern, sondern kann sich auf die Nutzdaten der Applikation konzentrieren.

4.4 Durchführung

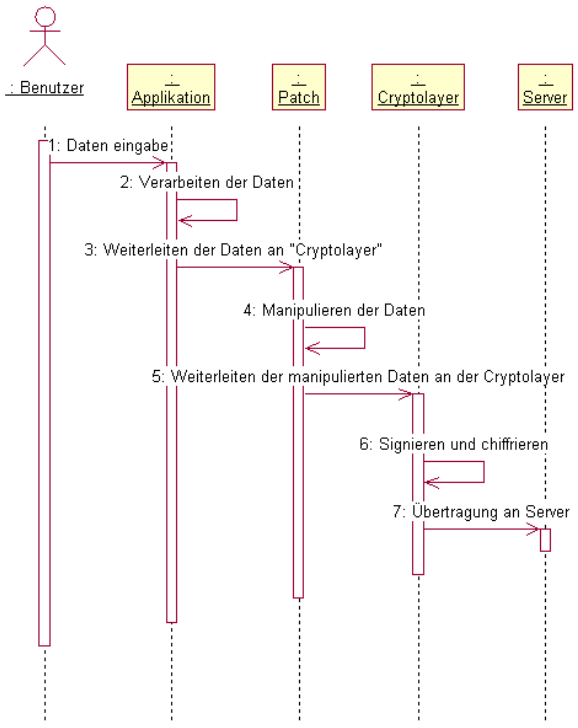


Ein Client-Software kann auf verschiedene Weise kompromittiert werden. Die kompromittierende Software kann ein ausführbares File, ein Macro einer Applikation, eine ActiveX-Komponente oder ein signiertes Java-Applet mit erweiterten Rechten sein, die der Benutzer auf seinem PC installiert und ausführt. Nachfolgend sind zwei Beispiele aufgeführt.

4.4.1 Shared library interception

Falls die Client-Software “shared libraries” benutzt, können Funktionsaufrufe abgefangen oder in eine shared library des Hackers umgeleitet werden.

4.4.2 Applikations Patch



Die Client-Software wird durch das Angreiferprogramm gepatched.

- Der Patch manipuliert gezielt Daten, die vom Benutzer eingegeben werden. Die manipulierten Daten werden vom Crypto-Layer mit dem Private-Key des Benutzers signiert, chiffriert und an den Server gesendet.
- Die Client-Software empfängt signierte und chiffrierte Daten vom Server. Der Crypto-Layer prüft die Integrität, dechiffriert die Daten und leitet diese an die Applikation weiter. Der Patch kann die dechiffrierten Daten an eine anonyme Adresse des Hackers weiterleiten.

4.5 Schlussfolgerung

Die Client-Software ist eine sensitive Komponente einer verteilten Applikation. Falls die Client-Software erfolgreich kompromittiert wurde, helfen auch kryptografische Protokolle nicht, die Manipulation der Daten zu erkennen. Implementationstechnisch kann aber der Aufwand für eine erfolgreiche Attacke beliebig erhöht, nicht aber ausgeschlossen werden.

5 Hacking-Planung

Die in diesem Beispiel geschilderten Gefahren werden nach den Empfehlungen des Kapitels *Gefahrenanalyse* analysiert. Der Bedrohungsgrad wurde in diesem Beispiel mit höchstens "kritisch für das System (3)" gewichtet, da ein möglicher Erfolg einer Attacke nur geringe Kosten für die Betroffenen verursacht.

5.1 Beispiel einer Liste

			Gefahrenanalyse des Systems			
1	2	3	4	5	6	7
Nr.	**BSI Nr.**	**Gefährdung**	**Bedrohungsgrad (1–4)**	**Hackervoraussetzung (1–4)**	**int./ ext.**	**Go/ NoGo Planung**
	G 2	**Gefährdungskatalog Organisatorische Mängel**				
1	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	2	2	i, e	NoGo
2	G 2.45	Konzeptionelle Schwächen des Netzes (Segmentierung)	3	3	i	NoGo
3		Platzhalter (nicht benötigt)				
4		"				
5		"				
	G 3	**Gefährdungskatalog Menschliche Fehlhandlungen**				
6	G 3.10	Falsches Exportieren von Dateisystemen unter Unix	1	4	i	NoGo
7	G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten	2	2	i	NoGo
8	G 3.29	Fehlende oder ungeeignete Segmentierung	2	3	i, e	NoGo
9		Schlechte Konfiguration des OS	2	3	i, e	NoGo
10		Schlechte Konfiguration des Netzwerkes	2	3	i, e	NoGo
11		Schlechte Konfiguration der Firewallsysteme	3	2	i, e	Go
	G 4	**Gefährdungskatalog Technisches Versagen**				
12	G 4.10	Komplexität der Zugangs-möglichkeiten zu vernetzten IT Systemen	3	3	E	Go
13	G 4.22	Schwachstellen oder Fehler in Standardsoftware	2	2	E	Go
14		Ausnützen von Schwachstellen des OS	3	2	E	Go
15		Ausnützen von Schwachstellen Standard SW	2	2	E	Go
16		Ausnützen von Schwachstellen von Applikationen	3	2	E	Go

Fortsetzung der Tabelle auf der nächsten Seite.

			Gefahrenanalyse des Systems			
1	2	3	4	5	6	7
Nr.	**BSI Nr.**	**Gefährdung**	**Bedro-hungs-grad (1–4)**	**Hacker-voraus-setzung (1–4)**	**int./ ext.**	**Go/ NoGo Planung**
	G 5	**Gefährdungskatalog Vorsätzliche Handlungen**				
17	G 5.7	Abhören von Leitungen				NoGo
18	G 5.9	Unberechtigte IT-Nutzung				NoGo
19	G 5.10	Missbrauch von Fernwartungszugängen				NoGo
20	G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal	1	2	1	NoGo
21	G 5.17	Gefährdung bei Wartungs-arbeiten durch externes Personal	1	2	1	NoGo
22	G 5.18	Systematisches Ausprobieren von Paßwörtern	3	2	E	NoGo
23	G 5.19	Missbrauch von Benutzerrechten				Go
24	G 5.20	Missbrauch von Administratorrechten				NoGo
25	G 5.21	Trojanische Pferde	3	2	E	Go
26	G 5.23	Computer-Viren	3	2	E	Go
27	G 5.24	Wiedereinspielen von Nachrichten (userid, PW, ...)				NoGo
28	G 5.25	Maskerade				NoGo
29	G 5.26	Analyse des Nachrichtenflusses				NoGo
30	G 5.38	Missbrauch der Fernabfrage				NoGo
31	G 5.39	Eindringen in Rechnersysteme über Modem				NoGo
32	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon				NoGo
33	G 5.41	Missbräuchliche Nutzung eines Unix-Systems				NoGo
34	G 5.42	Social Engineering	3	2	E	NoGo
35	G 5.43	Makro-Viren	3	2	E	Go
36	G 5.48 – G .51	Missbrauch von Netzwerk und Protokoll-Schwachstellen (IP-Spoofing, Source-Routing, etc.)	1	2	E	NoGo
37	G 5.54	Vorsätzliches Herbeiführen eines Abnormal End (denial of service)				NoGo
38	G 5.56	Temporär frei zugängliche Accounts				NoGo
39	G 5.61	Missbrauch von Remote-Zugängen für Management-funktionen von Routern				NoGo
40	G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme (Telearbeitsplätze)				NoGo
41	G 5.66	Unberechtigter Anschluß von IT-Systemen an ein Netz				NoGo
42	G 5.67	Unberechtigte Ausführung von Netzmanagementfunktionen				NoGo
43	G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten				NoGo
44	G 5.73	Vortäuschen eines falschen Absenders				NoGo
45	G 5.78	DNS-Spoofing				NoGo
46	G 5.79	Unberechtigtes Erlangen von Administratorrechtenunter Windows NT	2	2	E	Go
47		Unberechtigtes Ändern von Firewall-Konfigurationen	2	3	E	NoGo
48		Unberechtigtes Ändern von Netzwerk-Konfigurationen	2	3	E	NoGo

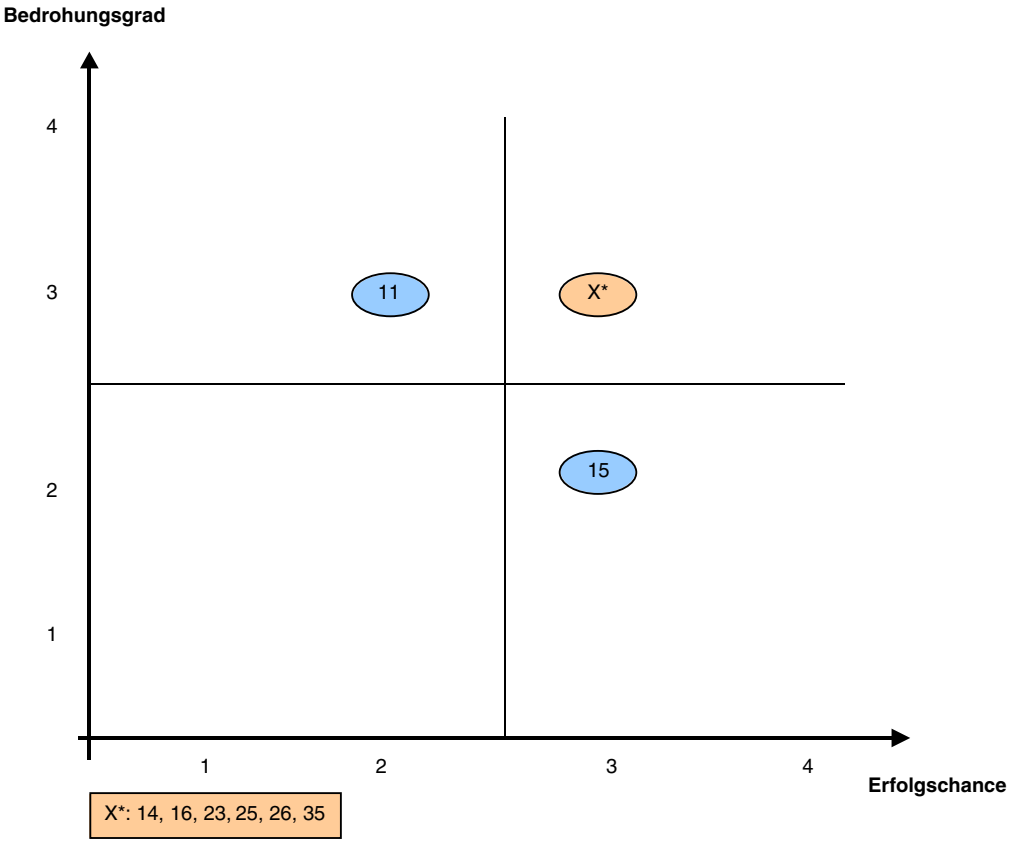
Im Schritt “Gefahrenanalyse des Systems” wurde also entschieden, dass nur die Punkte 11–16, 23, 25, 26, 35 und 46 weitergeführt werden.

Gefahrenanalyse Hacking-Einsatz

7	8	9	10	11	12	13
Nr.	**Go/ NoGo Planung**	**Angriffsmethode**	**Erfolgs-chance (1–4)**	**Aufwand**	**Risiko-beur-teilung (1–4)**	**Gegenmass-nahme**	**Go/ NoGo Definitiv**
11	Go	1. Direkter Zugriff auf Systeme, die in der DMZ liegen. 2. Direkter Zugriff auf Systeme, die im Intranet liegen.	2	Bei schlechter Konfiguration der Firewall wird der Aufwand als gering eingeschätzt, die dahinterliegenden Systeme zu attackieren, da diese nicht speziell geschützt sind.	3	Review und Test der Firewall	Go
12	Go	Attacken auf die Firewall, den WEB-Server und den Applikations-Server.	2	Es wird davon ausgegangen, dass die Firewall gut konfiguriert ist. Der Aufwand für eine solche Attacke wird als hoch eingeschätzt.	1	Review und Test der Firewall	NoGo
13	Go	Fehlverhalten der Standardsoftware ohne äussere Einwirkung.	1	–	1	Testen der am Prozess beteiligten Standard-software.	NoGo
14	Go	Schwierig abzuschätzen, da Schwachstelle an verschieden-sten Orten auftreten können.	3	Schwierig abzuschätzen, da allfällig neu auftretende Schwachstellen nicht bekannt sind.	3	1. Abklären, welche am Prozess beteiligten Schwachstellen bekannt sind. 2. CERT Advisories verfolgen und entsprechende Gegenmass-nahmen einleiten.	Go
15	Go	Schwierig abzuschätzen, da Schwachstelle an verschiedensten Orten in der Standardsoftware auftreten können.	3	Schwierig abzuschätzen, da allfällig neu auftretende Schwachstellen nicht bekannt sind.	3	1. Abklären, welche am Prozess beteiligten Schwachstellen bekannt sind. 2. CERT Advisories verfolgen und entsprechende Gegenmass-nahmen einleiten.	Go
16	Go	Mögliche Attacken auf die Applikation (Client-Software) sind beschrieben in Kapitel 4.	3	Der Aufwand korrelliert mit dem Aufwand, den man in den Integritätsschutz der Client-Software gesteckt hat.	3, 4	Implementation eines komplexen Integritäts-schutzes.	Go
23	Go	Ein Trojanisches Pferd kann die Client-Software so manipulieren, dass ein Dritter die Identität und somit die Benutzerrechte eines autorisierten Benutzers annehmen kann.	3	Der Aufwand, um die Client-Software zu reengineeren, wird als hoch eingeschätzt. Da dies aber offline durchgeführt werden kann, wird davon ausgegangen, dass das Re-engineering zum Erfolg führt.	3, 4	Implementation eines guten Integritätsschutzes in der Clientsoftware.	Go
25	Go	Ein Trojanisches Pferd kann die Client-Software so manipulieren, dass ein Dritter die Identität und somit die Benutzerrechte eines autorisierten Benutzers annehmen kann.					Go
26	Go	Ein Trojanisches Pferd kann die Client-Software so manipulieren, dass ein Dritter die Identität und somit die Benutzerrechte eines autorisierten Benutzers annehmen kann.					Go
35	Go	Ein Trojanisches Pferd kann die Client-Software so manipulieren, dass ein Dritter die Identität und somit die Benutzerrechte eines autorisierten Benutzers annehmen kann.					Go
46	Go	Der Angreifer hätte die volle Kontrolle über die Client-Software.	1	Da wir keine Kontrolle haben, wo die Client-Software eingesetzt wird, kann keine Aufwandschätzung gemacht werden.	2	Die Client-Software ist ein Massenprodukt. Der Kunde kann darauf aufmerksam gemacht werden, wie er sein System zu schützen hat oder wie er seine Passwörter verwalten soll. Diese Methode wird aber als wenig erfolgreich eingeschätzt.	NoGo

5.2 Entscheide für die Durchführung

Als Entscheidungshilfsmittel für die Auswahl der durchzuführenden Testmethoden, werden die Informationen der Tabelle Hacking-Planung graphisch dargestellt. Die untenstehende Grafik zeigt den Zusammenhang zwischen der Erfolgschance eines Angriffs und der Bedrohung für das System. Die Grafik kann somit als erstes Selektionskriterium für die Durchführungsplanung verwendet werden. Wichtig dabei ist, dass nach dieser Vorselektion für jeden Angriff die Risikobeurteilung (Kolonne Nr. 11 der Tabelle) sowie die entsprechenden Gegenmassnahmen (Kolonne Nr. 12) beurteilt werden.



Die Auswertung zeigt, dass die unter X* aufgeführten Gefahren den höchsten Bedrohungsgrad und die höchsten Erfolgschancen aufweisen. Diese Gefahren sollten durch ein Spezialistenteam behoben oder entschärft werden.

Eine Kosten-/Nutzenabschätzung kann entscheiden, ob die unter den Nummern 11 und 15 aufgeführten Gefahren zu entschärfen sind oder nicht.

Gesetze und Verordnungen

1 Memorandum zum schweizerischen “Computer-Strafrecht”

Mit seiner Tätigkeit beabsichtigt der Hacker, in Datenverarbeitungssysteme zu gelangen, die vor unberechtigtem Zugriff besonders geschützt wurden. Unproblematisch ist die Hackertätigkeit, die im Auftrag erfolgt, weil sie dadurch erlaubt wird. Dringt der Hacker durch seine Tätigkeit jedoch unerlaubter Weise in fremde Datenverarbeitungssysteme ein, kann dies strafrechtliche Konsequenzen haben.

Nachstehend sollen die für die Hackertätigkeit eventuell relevanten Tatbestände aufgeführt werden.

Unbefugte Datenbeschaffung (“Datendiebstahl”), Art. 143 des StGB

> *“Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.*
>
> *Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.”*

Dieser Tatbestand schützt primär den an den Daten Berechtigten in seinen Vermögensrechten gegenüber den an den Daten nicht Berechtigten. Er ist vordergründig also kein Persönlichkeits- oder Geheimnisdelikt. Die Tathandlung ist das Beschaffen von Daten wie etwa das Kopieren ab einem Computer. Eine blosse Kenntnisnahme der Daten, ohne die Möglichkeit, den Datenbestand in die eigene Verfügungsgewalt zu überführen, gilt nicht als Beschaffen im Sinne von Art. 143 StGB. Der Täter muss die Daten ausserdem vorsätzlich in der Absicht sich oder einen anderen zu bereichern, beschaffen. Ausserdem muss der Täter die Absicht haben, die Daten dauernd in seiner Verfügungsgewalt zu behalten.

Ein Hacker erfüllt diesen Tatbestand dann nicht, wenn er sich die Daten nicht “aneignet”, das heisst, wenn er die fremden Daten nicht kopiert und/oder sich oder einen andern mit diesen Daten nicht bereichern will.

Unbefugtes Eindringen in ein Datenverarbeitungssystem (“Hackertatbestand”) Art. 143bis StGB.

> *“Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder Busse bestraft.”*

Dieser Tatbestand schützt vor Hackern, die sich einen Sport daraus machen, Sicherungen zu knacken und in gesicherte Datensysteme einzudringen, ohne damit weitere, insbesondere wirtschaftliche Zwecke zu verfolgen. Ein solches Hacken ist in Deutschland oder Österreich nicht stafbar.

Art. 143bis bestraft aber auch nur das vorsätzliche Eindringen in eine fremde Datenverarbeitungsanlage. Ein irrtümliches Eindringen wird nicht bestraft, auch nicht, wenn der Hacker nach dem Eindringen im fremden Datenverarbeitungssystem verweilt. Ausserdem muss das Eindringen in unbefugter Weise erfolgen. Hackt der Hacker im Auftrag des Inhabers des Datenverarbeitungssystems, so ist dieses Hacken erlaubt.

Gerät ein Hacker in ein fremdes System, für welches er keine Hackererlaubnis hat, und erfolgt daraufhin ein Strafantrag des Betroffenen, so prüft das Gericht, ob der Hacker bei seiner Tätigkeit vorsätzlich, das heisst mit Wissen und Willen gehandelt gehandelt hat. Dabei genügt es, dass der Hacker bei seiner Tätigkeit in Kauf genommen hat, in das fremde System einzudringen. Ein Inkaufnehmen könnte man etwa annehmen, wenn der Hacker, bevor er den letzten Schritt unternahm um in das fremde System einzudringen, erkannt hat, dass dies passieren könnte, und er trotzdem, ohne weitere Vorsichtsmassnahmen in seiner Tätigkeit fortfuhr.

Datenbeschädigung Art. 144bis StGB

> *"1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder Busse bestraft.*
>
> *Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus erkannt werden. Die Tat wird von Amtes wegen verfolgt.*
>
> *2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.*
>
> *Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden."*

Ziffer 1 dieses Tatbestandes bestraft die vorsätzliche Datenbeschädigung oder Vernichtung. In Bezug auf den Vorsatz kann auf das Obenstehende verwiesen werden. Schädigt der Hacker Daten des Vertragspartners durch seine Hackertätigkeit, so kann grundsätzlich davon ausgegangen werden, dass der Vertragspartner sich der Gefahr einer Beschädigung von Daten im Zusammenhang mit dem Hacken bewusst war und er eine Schädigung deshalb in Kauf nahm. (Als anschauliches Beispiel: Begeben sich zwei Boxer in den Ring, nehmen sie beide eine Körperverletzung, auch wenn sie durch den Gegner absichtlich verursacht wurde, in Kauf. Nicht in Kauf nehmen sie ein absichtlich abgebissenes Ohr, da bei einem Boxkampf nicht damit gerechnet werden muss).

Ziffer 2 dieses Tatbestandes schützt vor der Herstellung oder in Umlaufbringung von Computerviren. Auch die Herstellung oder in Umlaufbringung von Computerviren muss, damit sie strafbar ist, vorsätzlich, das heisst mit Wissen und Willen erfolgen.

Unbefugtes Beschaffen von Personendaten Art. 179^{novies} StGB

> *"Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Gefängnis oder mit Busse bestraft."*

Geschützt durch diese Norm ist die Persönlichkeit der betroffenen Person. Als besonders schützenswerte Personendaten gelten Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgungen oder Sanktionen.

Als Beschaffung gilt auch nur schon die Kenntnisnahme solcher fremden Daten, weil dadurch schon der Persönlichkeitsschutz durchbrochen ist.

Eine Bereicherungsabsicht ist entgegen dem Tatbestand der unbefugten Datenbeschaffung gemäss Art. 143 StGB nicht erforderlich. Allerdings bedarf es auch hier eines Vorsatzes zum Eindringen in die Datensammlung der besonders schützenswerten Daten. Da gemäss Rechtslehre eine Kenntnisnahme der Daten genügt, um diesen Tatbestand zu erfüllen, ist mit grosser Wahrscheinlichkeit die Dauer des Verweilens in der Datensammlung relevant. Ein kurzes (versehentliches) Eindringen und der danach schnellstmögliche Ausstieg erfüllt höchstwahrscheinlich das Tatbestandsmerkmal der "Beschaffung" nicht.

2 Die Gesetzgebung im Überblick

2.1 Schweiz

- *Datenschutzgesetz*
  Beide Parteien müssen dafür besorgt sein, dass die Datenschutzgesetze nicht verletzt werden. Neben der Information der möglicherweise Betroffenen (z.B. Mitarbeiter im untersuchten Unternehmen) ist ein sorgfältiger Umgang mit den gewonnenen Informationen wichtig.

- *Strafgesetzbuch*
  Das Eindringen in fremde Systeme ist grundsätzlich strafbar. Es ist deshalb zu empfehlen, dass Angriffe nur auf diejenigen Systeme ausgeführt werden, für welche der Auftragnehmer ausdrücklich die entsprechende Bewilligung dazu hat. Kritisch ist die Situation insbesondere dann, wenn Outsourcing-Organisationen involviert sind (z.B. Netzbetreiber), welche nicht kooperieren.

- *Obligationenrecht*

2.2 Europa

Neben den einzelnen Ländern ist auch Europa-Recht zu beachten. Im Bereich des Datenschutzes gelten in Europa in allen Ländern ähnliche Gesetze wie in der Schweiz. Im Zweifelsfall oder bei besonders sensitiven Arbeiten ist es grundsätzlich empfehlenswert, Rechtsberatung von Experten mit einschlägiger Erfahrung einzuholen.

2.3 USA

In USA existieren Gesetze sowohl auf Stufe Bundesstaat als auch auf Stufe der einzelnen Staaten. Bei sensitiven Arbeiten in USA ist es grundsätzlich empfehlenswert, Rechtsberatung von Experten mit einschlägiger Erfahrung einzuholen.

2.4 Übrige Länder

Bei sensitiven Arbeiten in Ländern ausserhalb Europa ist generell Rechtsberatung von Experten mit einschlägiger Erfahrung einzuholen.

Ethische Grundsätze

Wir als Beauftragte erkennen und akzeptieren unsere persönliche und berufliche Verantwortung bei der Durchführung unserer Aufträge. Wir verpflichten uns daher zu den folgenden ethischen und beruflichen Grundsätzen.

Wir wollen:

- die im Verlaufe unserer Tätigkeit erhaltenen Informationen schützen und diese weder zum persönlichen Vorteil nutzen noch unberechtigten Parteien zugänglich machen;
- bei unseren Tätigkeiten gebührende Vorsicht walten lassen;
- nur solche Aufgaben übernehmen, für die wir durch Ausbildung oder Erfahrung genügend qualifiziert sind;
- laufend das Verständnis und die Fachkompetenz für Methoden und Technologien, ihre korrekte Anwendung und die möglichen Konsequenzen verbessern;
- Informationen mit genügender Professionalität sammeln und auf der Basis dieser Informationen ehrlich und realistisch sein bei der Deklaration von Feststellungen und Empfehlungen;
- unsere Aufgaben unabhängig und objektiv durchführen;
- echte und empfundene Interessenskonflikte wo immer möglich vermeiden und sie den Betroffenen mitteilen, wenn solche vorkommen;
- jegliche Handlungen vermeiden, welche Dritte in ihrem Besitz oder ihrem Ruf verletzen;
- Bestechungen in jeglicher Form ablehnen und nie wissentlich an illegalen oder inkorrekten Handlungen teilnehmen;
- ehrliche Kritik der Arbeiten suchen und akzeptieren; Fehler bestätigen und korrigieren und fair die Leistungen Dritter erwähnen;
- die Aufstellung und Einhaltung angemessener Standards, Verfahren und Kontrollen für unsere Tätigkeiten unterstützen;
- unsere Kollegen und Mitarbeiter in ihrer professionellen Entwicklung unterstützen und ihnen bei der Einhaltung dieser ethischen Grundlagen helfen.

Diese Seite bleibt aus technischen Gründen leer.

Glossar

Awareness	Sensibilisierung. Hier gemeint ist Security-Awareness = Sicherheitsbewusstsein. Sicherheitsbewusstes Verhalten bedeutet nicht der Verzicht auf sämtliche gefährlichen Handlungen sondern dass bewusste Inkaufnehmen von Risiken unter Treffen aller notwendigen Massnahmen.
Brute-Force Attacke	Versuch, Passwörter mittels “roher Gewalt”, das heisst durch systematisches Ausprobieren sämtlicher möglichen Buchstabenkombinationen zu finden. Der Aufwand für solche Angriffe hängt vom verwendeten Zeichensatz ab (alpha, alphanummerisch, Gross- und Kleinschreibung, Sonderzeichen).
Carrier Scan	Ein Carrier Scan ist die computerunterstützte Suche nach einem Modem. Durch systematisches Durchprobieren des Telefonnummernbereichs eines Unternehmens wird versucht, ein eingeschaltetes Modem zu finden. Nimmt am “anderen” Ende ein Modem ab, so kann das Trägersignal (carrier) vom Anrufer erkannt werden. Die Nummer des Anschlusses wird in einem Protokoll festgehalten. In einem späteren Schritt kann versucht werden, über diesen Anschluss ins System einzudringen.
Cracker	Angreifer oder Eindringling, der über ein Kommunikationsnetz Daten zur Kenntnis nimmt, verändert oder auch zerstört. Auch ein Begriff für einen Raubkopierer, der ein Sicherheitssystem “knackt” (*siehe* brute force attack, *siehe* dictionary attack, *siehe* password cracking)
Denial of Service	Angriffsmethode, in welcher versucht wird, das Zielsystem zu sabotieren. Mögliche Vorgehensvarianten sind: Übermitteln ungültiger Informationen (z.B. Escape-Sequenzen), Übermitteln zu langer Datensätze, Übermitteln Tausender von Meldungen innert kürzester Zeit, wiederholtes Login mit ungültigen Passwörtern usw.
Dictionary Attack	Systematisches Durchprobieren möglicher Passwörter. Im Gegensatz zur (*siehe*) Brute-force Attacke werden nur Passwörter aus einem oder mehreren Wörterbüchern durchprobiert.
DMZ	*siehe* de-militarized zone
De-militarized Zone	(DMZ): Teilnetz eines Firewallkonzeptes, dass sowohl vom Internet als auch vom internen Netz mit je einem Firewall abgetrennt ist. In der DMZ stehen in der Regel alle von aussen her zugänglichen Server sowie sämtliche Komponenten, welche eine Verbindung zwischen innen und aussen erlauben.
Ethical Hacking	Hacken im Auftrag eines berechtigten Auftraggebers und unter Einhaltung aller ethischen und rechtlichen Regelungen.
Firewall	Ein System (z.B. Paketfilter, Proxies), dass zwei verschiedene Netze voneinander trennt. Der Firewall schützt sich selbst gegen Angriffe von Aussenstehenden und überprüft den Verkehr zwischen dem internen und externen Netz.
Gefahrenanalyse	Systematische Erfassung und Beurteilung der Gefahren (eigentlich: Gefährdungen) eines Systems. Kombination der Untersuchung der Verletzbarkeit des Systems auf Angriffe Dritter und der durch die Tiger-Teams verursachten Gefährdungen.

Hacker	Ein Computerbegeisterter, der sein Wissen und Werkzeuge einsetzt, um unberechtigten Zugriff zu geschützten Ressourcen eines Systems zu erhalten.
Intranet	Unternehmensinternes Netz, das technisch mit dem Internet vergleichbar ist.
Malicious Software	Bösartige Software oder Firmware, die absichtlich verändert und in ein System eingeschleust wird mit dem Zweck, dort Schaden anzurichten oder Ressourcen unberechtigterweise zu verwenden (z.B. Virus, Wurm, …).
Missbrauch	Unberechtigter Zugriff auf oder Verwendung von IT-Ressourcen (Hardware, Software, Netzwerke usw.).
Password Cracking	Der Versuch, ein Passwort für eine bestimmte Benutzerkennung zu “knacken” (erraten, finden).
Phreaking	Hacken eines Telefonsystems: a) um auf Kosten der Telefonfirma unbeschränkt telefonieren zu können; b) um über das Telefonnetz in ein anderes System einzudringen.
Recovery	Rekonstruktion der ursprünglichen Daten oder Programme durch Zurückladen von Sicherungskopien oder durch die Analyse von “Datenüberresten” auf Massenspeichern mittels Einsatz von speziellen Tools.
Risikoanalyse	Ermittlung oder Abschätzung eines Risikos mit wissenschaftlichen Methoden, insbesondere durch Ermittlung von Wahrscheinlichkeit eines schädigenden Ereignisses und des damit verbundenen Schadenausmasses.
Scanning	Automatisierte Analyse von Daten(strömen), um Informationen (z.B. Passwörter) sowie mögliche Schwachstellen herauszufinden.
Schwachstelle	Verletzbarkeit eines Systems bezüglich einer Gefährdung.
Security Review	Systematische Analyse eines vorgegebenen Zustand hinsichtlich der vorhandenen Risiken und Sicherheitsmassnahmen. Oft als Vergleich zwischen dem Ist und einem standardisierten Soll.
Sniffing	Abhören eines Netzwerks an einer Schnittstelle zum Sammeln von Nachrichtenpaketen. Wenn ein Paket den definierten Kriterien entspricht, wird es in einem Protokoll festgehalten. Am häufigsten wird nach der Anmeldenachricht gesucht, welche die Benutzerkennung und das zugehörige Passwort enthält.
Social Engineering	Verfahren zum Ausforschen sensitiver Informationen von Personen (z.B. Ausfragen verärgerter Mitarbeiter).
Tiger-Team	Von Dritten beauftragtes Spezialistenteam, das mittels Hacking in ein Computersystem des Auftraggebers eindringen soll.
Zertifizierung	Technische Bewertung von Sicherheitsmassnahmen eines Systems durch eine offizielle Instanz unter dem Aspekt der Erfüllung von Sicherheitsanforderungen hinsichtlich Design und Implementierung.