

Objektorientierte Risikoanalyse für die IT-Sicherheit

Von Michael Haack, Berlin

*Durch den Einsatz der Informationstechnologie existieren für jedes Unternehmen und jede Behörde jeweils spezifische Bedrohungen, die sowohl in hardware- und softwaretechnischen als auch in organisatorischen Bereichen zu finden sind. Um mit der technologischen Entwicklung, die stetig neue Risiken schafft, Schritt halten zu können, benötigen Unternehmen und Behörden eine kontinuierliche bzw. fortgeschriebene Bewertung dieser Risiken. Wie sollte ein Werkzeug *) aussehen, das die Beratung in diesem Bereich verbessern könnte?*



Immer noch rasch wachsenden Maße werden Bedrohungen durch den Einsatz von Client-Server-Architekturen und der damit zusammenhängenden Netzstruktur (LAN, WAN, Internet und Intranet) festgestellt. Im einzelnen handelt es sich hierbei um die folgenden Teilaspekte:

- die Tendenz zu integrierten, unternehmensweiten IT-Anwendungen aus Groupware-, Workflow- und Dokumentenmanagement-Systemen;
- die Einführung umfassender Auswertungs- und Informationssysteme wie Data Warehouse und Data Mining;
- die Öffnung der unternehmensinternen Informationsinfrastruktur für Außenstehende (Kunden, Lieferanten etc.), zum Beispiel bei Homebanking-, Electronic Commerce- und Electronic Marketplace Anwendungen;

*) Die UBIS Unternehmensberatung für integrierte Systeme entwickelt zur Zeit ein solches Werkzeug, das im methodischen Vorgehen und als Prototyp bereits auf der CeBIT 1998 vorgestellt wurde und inzwischen auch im konkreten Projekt erprobt wird. UBIS stellt dieses Tool hier zur Diskussion.

- die Dezentralisation von Systemen und Daten (verteilte Systeme, agentenorientierte Techniken);
- die Verbindung der Datenverarbeitungsinfrastruktur mit anderen Technologien im Unternehmen, beispielsweise Computer-Telephony-Integration (CTI);
- die allgemein zunehmende Kommunikation nach außen (Internet), unternehmensextern (Extranet) und unternehmensintern (Intranet);
- der Zusammenschluß einzelner lokaler Netzwerke zu einem virtuellen unternehmensweiten Netzwerk („Virtual Private Network“);
- der Zugriff auf unternehmensinterne Systeme von außen („Remote Access“), unter anderem von Heimarbeitsplätzen oder mobilen Arbeitsplätzen;
- die wachsende Relevanz der Verschlüsselungsproblematik auf Netzwerkverbindungen;
- die Absicherung externer Netzzugänge (z. B. mit Firewall-Systemen).

Das unternehmensspezifische Risikopotential kann mit Hilfe einer Risikoanalyse ermittelt werden. Ergebnis dieser Analyse ist

die Bestimmung der Risiken für das Unternehmen, um geeignete Sicherheitsmaßnahmen zu nennen und im Unternehmen einzusetzen. Eine weit verbreitete Vorgehensweise zur Risikoanalyse gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem IT-Sicherheits- und IT-Grundschutzhandbuch vor. Dieses Standardwerk definiert thematische Grundlagen und prägt Begriffe. Im praktischen Einsatz zeigen sich jedoch einige „Lücken“, die Verfahren eventuell unhandlich werden lassen können.

Ein Aspekt ist die fehlende Übersichtlichkeit. Bei größeren Analysen werden die Ergebnisse in Tabellenform schnell sehr umfangreich und damit schwer überblickbar. Das Ausmaß von Veränderungen und damit der Anpassungsbedarf für ein IT-Sicherheitskonzept wird vielfach noch unterbewertet. Aber allgemein gilt: Gerade beim aktuellen Innovationstempo ändern sich die bestehenden Bedrohungen häufig. Auch die bestehenden Maßnahmen müssen nach Umbauten oder Umstrukturierungen zeitnah neu bewertet werden, um das aktuelle Risikopotential zu beobachten.

Vor allem im Bereich der Client-Server-Umgebungen werden oftmals sehr flexibel neue Anwendungen und Systeme eingeführt. Und nicht zuletzt ändern sich auch die Anforderungen, die ein Unternehmen und dessen Untergliederungen (Abteilungen, Arbeitsprozesse) an die Informations- und Kommunikationstechnik stellt. Dieses ist insbesondere der Fall bei Änderungen der gesetzlichen Rahmenbedingungen. In diesen Fällen muß sofort überprüfbar sein, ob sich aus den steigenden Anforderungen - d. h. dem erhöhten Schutzbedarf - auch gravierende Risikoerhöhungen ergeben, die schnelles Handeln erfordern.

In Anbetracht dieser Hintergründe gilt es, ein Verfahren zu generieren, das neben der einfachen Durchführbarkeit insbesondere großes Augenmerk auf die Pflege und Fortschreibung legt. Wer weiterhin auf die Aussage „Einmal sicher - immer sicher!“ vertraut, der findet sich früher oder später in einer der mit zunehmender Anzahl auftretenden Medienmeldungen mit der Schlagzeile „Computerausfall kostete Unternehmen Millionen“ wieder. Ein IT-Sicherheitskonzept darf nicht durch schwierige und aufwendige Analyseverfahren zum reinen Alibi verkommen, mit dem Geschäftsführung, Vorstand und Aufsichtsstellen beruhigt werden.

Objekte

Im Zentrum des hier vorgestellten objekt-orientierten Ansatzes stehen die Objekte. Als Objekte kommen sämtliche Komponenten der IuK-Infrastruktur in Frage - das heißt IT-Anwendungen, IT-Systeme, Netzwerke, Räume und Gebäude. Die Grundeigenschaften der Objekte sind die auf sie wirkenden Bedrohungen und die vorhandenen bzw. nicht vorhandenen Sicherheitsmaßnahmen.

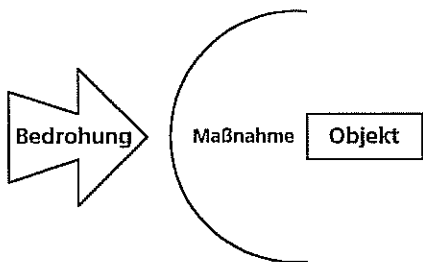


Abb. 1: Grundkonstellation

Die Objekteigenschaften Bedrohung und Maßnahme sind immer in einem Zusammenhang zu betrachten (s. Abb. 1). Nur diese „Dreierbeziehung“ ergibt einen Sinn, da eine Maßnahme nicht pauschal (gegen eine beliebige Bedrohung) an einem Objekt wirkt und auch nicht pauschal (an einem beliebigen Objekt) vor einer Bedrohung schützt (Abb. 2).

Nun reicht es allerdings nicht aus, einem Objekt eine Menge von Bedrohungen und Maßnahmen zuzuordnen. Die Größe bzw. Stärke der Bedrohung sowie die Wirksamkeit der bereits vorhandenen Maßnahmen ist konkret zu bewerten und zu beziffern.

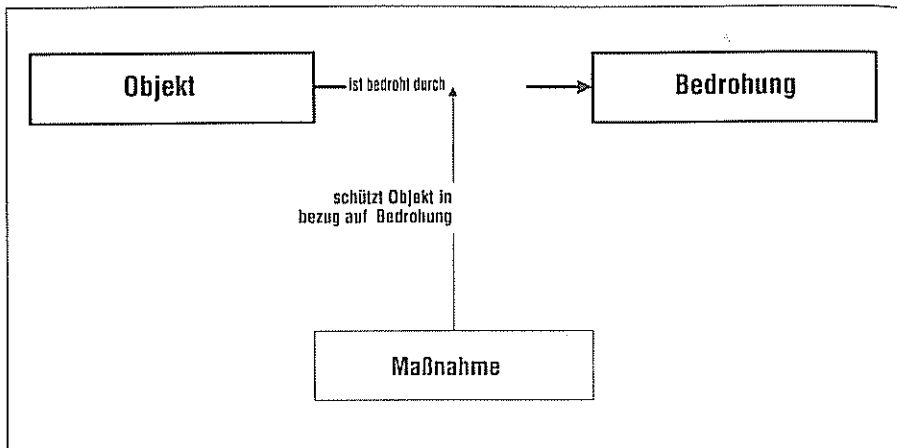


Abb. 2: Dreierbeziehung Objekt - Bedrohung - Maßnahme

Als größtes Bewertungsschema läßt sich null für „nicht vorhanden“ und eins für „vorhanden“ definieren. In den meisten Fällen reicht dieses schon aus, da insbesondere bei den Maßnahmen oft gar nicht weiter untergliedert werden kann und muß. Sollte dieses notwendig werden - beispielsweise, wenn Maßnahmen zwar vorhanden, aber schlecht implementiert sind - so können natürlich beliebige Unterklassen im Intervall [0,1] festgelegt werden.

Relationen

Die einzelnen Objekte werden im Schichtenmodell durch Verbindungen miteinander in Beziehung gesetzt (siehe Grafik 3).

Die Bedeutungen dieser Beziehungen sind zunächst zwischen den Ebenen unterschiedlich:

- Ein Prozeß verarbeitet Informationen/ Daten
- Informationen/Daten werden verarbeitet mit Anwendungen
- Anwendungen laufen auf Systemen
- Systeme befinden sich in Infrastrukturelementen

Als übergreifende Bedeutung der Relationen kann die „Weitergabe von Anforderungen“ definiert werden. Im Schichtenmodell stehen die Objekte mit ihren Bedrohungen und Maßnahmen zunächst für sich. Sie sind zwar untereinander über die Relation verbunden, aber es können trotzdem noch keine Aussagen über Schwachstellen gemacht werden, da noch nicht klar ist, welche Anforderungen an das einzelne Objekt gestellt werden. Selbst wenn die vorhandenen Maßnahmen nicht ausreichen, vor der Bedrohung zu schützen, so ergibt sich - wenn überhaupt - nur eine sehr geringe Schwachstelle, wenn an das Objekt keine oder nur geringe Anforderungen gestellt werden.

Die Höhe der gestellten Anforderungen definiert also den Schutzbedarf dieses Objektes. Allerdings kann der Schutzbedarf nicht für sämtliche Objekte festgelegt werden. Er ergibt sich vielmehr aus dem globalen Schutzbedarf der verarbeiteten Daten an die Vertraulichkeit und die Integrität sowie der Prozesse und Abläufe an die Verfügbarkeit. Die Bewertung des konkreten Schutzbedarfs orientiert sich dabei an den Aspekten:

- Gegen welche Gesetze oder Vorschriften wird im Fall einer Sicherheitsverletzung verstoßen?
- Wie wird die Aufgabenerfüllung im Fall einer Sicherheitsverletzung beeinträchtigt?

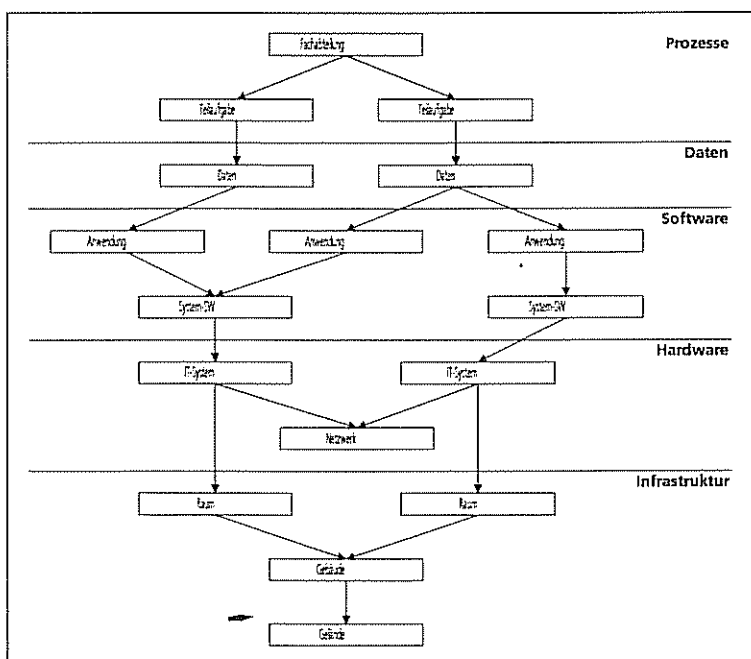


Abb 3: Schichtenmodell

- Welche Außenwirkung tritt im Fall einer Sicherheitsverletzung ein?
- Welche Innenwirkung tritt im Fall einer Sicherheitsverletzung ein?
- Welche finanziellen Auswirkungen hat eine Sicherheitsverletzung?
- Wie groß ist die Dauer der Verzichtbarkeit des Systems?

In diesem Punkt zeigt sich eine relative Übereinstimmung mit der Stufe 1 aus dem IT-Sicherheitshandbuch.

Es zeigt sich, daß die Definition des Schutzbedarfs im Schichtenmodell auf den obersten beiden Ebenen geschieht. Auf diesen Schichten befinden sich gerade die Objekte, denen keine Bedrohungen und Maßnahmen sinnvoll zugeordnet werden können. Es ergibt sich also eine Zweiteilung der Objekte in diejenigen, die Anforderungen stellen, und diejenigen, die Anforderungen im Sinne der IT-Sicherheit erfüllen müssen.

Die definierten Anforderungen werden über die Objektverbindungen an die Nachfolgeobjekte weitergegeben. Zusätzlich zur Bewertung der Bedrohungen und Maßnahmen erhält jedes Objekt nun einen Anforderungswert, der sich aus dem Maximum der Anforderungswerte seiner Vorgängerobjekte ergibt. Stehen beispielsweise in einem Raum mehrere IT-Systeme, so stellen sich an den Raum dieselben Anforderungen, die an das System mit dem höchsten Schutzbedarf gestellt werden.

Auf dieser Basis ist es möglich, für jedes Objekt zu ermitteln, ob die Anforderungen durch die bestehenden Maßnahmen erfüllt werden können oder ob einzelne Bedrohungen zu hoch sind und damit Schwachstellen vorliegen. Diese Einzelsicht reicht allerdings noch nicht aus, da Schwachstellen in einzelnen Bereichen Auswirkungen auf die gesamte IuK-Infrastruktur zeigen können. Ein fehlendes Backup-Konzept für ein bestimmtes IT-System erhöht beispielsweise das Risiko für alle davon abhängigen Objekte - also Anwendungen, Daten und Prozesse.

Aufgrund dieser Tatsache erscheint es sinnvoll, daß die Objekte ihre Anforderungs-Erfüllungs-Werte an die von ihnen abhängigen Objekte über die Objektverbindungen weiterleiten. Es ergibt sich dabei die entgegengesetzte Richtung zur Anforderungsübertragung. Allerdings ist hierbei nicht das Maximum aller ankommenden Werte, sondern deren Summe zu wählen, da sich die etwaig vorhandenen Schwachstellen aufsummieren.

Neben den Bedrohungen, Maßnahmen und Anforderungen besitzt jedes Objekt nun einen vierten Wert, der als Risikowert bezeichnet sei. Auf der Ebene der Prozesse zeigt dieser Wert an, welcher das höchste Risiko trägt, weil er von Objekten abhängig ist, die mit Schwachstellen behaftet sind. Um eine angemessene Aussagekraft der Ergebnisse zu erhalten, sind bei der Berechnung der einzelnen Werte noch entsprechende Gewichtungen, Skalierungen und Korrekturterme anzubringen, auf die hier nicht im einzelnen eingegangen werden soll.

Implementation

Diese Vorgehensweise eignet sich besonders gut zu einer Umsetzung als IT-Anwendung. Neben der zentralen Pflege der Objekte, Bedrohungen und Maßnahmen in Form von Taxonomien in einer Wissensbasis ergeben sich die folgenden Vorteile:

- Übersichtlichkeit und leichte Bedienung durch grafische Modellierung
- Vermeidung von Routinetätigkeiten

- Möglichst große Freiheit beim Modellieren
- Einfache Fortschreibung möglich
- Wiederverwendbarkeit von Wissen
- Anschauliche Präsentation der Ergebnisse

Der beschriebene objektorientierte Ansatz für eine Risikoanalyse und dessen Realisierung als computerunterstütztes Werkzeug läßt hoffen, daß im Sinne der IT-Sicherheit eine Abkehr von den vielfach in Verwendung befindlichen Inventarlisten und Alibi-Werkzeugen erfolgt, die lediglich das Gewissen beruhigen, aber keine signifikanten Sicherheitsgewinne erzielen.

Michael Haack ist Diplom-Informatiker und seit 1995 als Berater im Bereich Unternehmenssicherheit bei der UBIS GmbH tätig.