atsec the information security provider
NEWS 03/11

Komplexität und Sicherheit

Heutige Informationssysteme bieten unzählige Features, die den Konsumenten mit immer interessanteren Möglichkeiten locken. Die von den Entwicklern betriebene Philosophie, immer mehr dieser Funktionen bereitzustellen, führt allerdings zu einer immer schlechteren Situation der Technik. Anstatt auf bewährte Komponenten zu vertrauen, werden neue Bestandteile, Produkte oder Techniken in Produktivsystemen eingesetzt, sobald sie verfügbar sind, wodurch komplexe Architekturen und Implementierungen entstehen. Dies führt nicht nur zu Schwierigkeiten in der Wartung der Systeme, sondern stellt auch eine große Angriffsfläche dar.
Risiko berechnet sich aus Eintrittswahrscheinlichkeit eines Schadens und seinem Ausmaß. Angreifer nutzen dabei Schwachstellen des Systems, und je mehr Funktionen und Schnittstellen ein System bietet, desto mehr Schwachstellen können wahrscheinlich ausgenutzt werden. Dabei ist der Angreifer gegenüber dem Entwickler im Vorteil: Der Entwickler müsste alle Lücken stopfen, während der Angreifer letztlich nur eine einzige Lücke finden muss.

Entwickler müssen alle Lücken schließen, Angreifer aber nur eine einzige finden.

Diesem hilft auch, dass die Hersteller – mit Zustimmung der Kunden – in gewisser Weise resigniert haben: Ziel ist nicht mehr, ein fehlerfreies Produkt auf den Markt zu bringen; Schwachstellen werden nicht beseitigt, sondern „gemanagt“. Man hat sich damit abgefunden, dass am „Patchday“ die in letzter Zeit aufgetauchten Lücken geschlossen werden. Befremdlich dabei ist, dass die Kunden dieses Stopfen von Lücken auch noch als besonderen Ausdruck des Sicherheitsbewusstseins des Herstellers werten, anstatt sich zu fragen, warum dessen Entwicklungsrichtlinien überhaupt solch unsicheren Code zuließen.
Unsichere Banken-, Hersteller- oder Telefonanbieter-Webpages sind Beispiele, die in letzter Zeit Schlagzeilen machen. In all diesen Fällen handelt es sich um komplexe Systeme, kombiniert mit Komponenten, die nicht für diesen Einsatzzweck entwickelt wurden.
Das Wissen, dass traditionelle Ansätze (etwa Penetrationstests) nur das Vorhandensein von Schwachstellen zeigen, nicht aber deren Abwesenheit, wurde im Sicherheitsbereich im Konzept der Angriffsfläche umgesetzt. Durch Analyse der Angriffsmöglichkeiten kann eine Aussage über das Sicherheitsniveau eines Systems getroffen werden. Dies darf jedoch nicht mit „security by obscurity“ verwechselt werden. Jede gewollt oder ungewollt öffentliche Schnittstelle muss als für den Angreifer zugänglich angesehen werden. Systeme müssen daher zur Minimierung der Angriffsmöglichkeiten von vornherein mit dem Gedanken an Sicherheit konstruiert werden. Das UNIX-Prinzip von kleinen Komponenten mit begrenzten, aber bewährten Funktionen, ist eine Idee für die Bausteine eines Systems. Durch deren Kombination ist es möglich, Schnittstellen zu erstellen, die nur die minimal benötigte Funktionalität exponieren. Dies hält auch die generelle Komplexität des Systems in Grenzen.
Für die Sicherheitsanalyse bedeutet dies: statt Schwachstellenanalyse und nachfolgendem Ausbessern der Fehler, muss die Komplexität des Systems gemeinsam mit der exponierten Angriffsfläche behandelt werden, also ein Wandel von Komponenten orientierter Aufgabe zu einer holistischen Systemanalyse stattfinden.

Robert Hoffmann
Sicherheitsberater atsec

atsec lädt ein


Foto: Heiko Stahl

Die größte IT-Sicherheitsmesse im deutschsprachigen Raum öffnet vom 11. – 13. Oktober 2011 in Nürnberg ihre Pforten. Mit über 300 Ausstellern und mehr als 7000 erwarteten Besuchern etablierte sich die itsa als wertvolle Informations- und Präsentationsplattform für den Austausch zwischen IT-Experten. Die Messe adressiert alle Aspekte der Informationssicherheit von A wie Abhörschutz und Applikationssicherheit bis Z wie Zertifizierung und Zugriffsschutz. Speed-Live-Hacking, Kriminalgeschichten mit dem Titel „Datendieben auf der Spur“ oder provokante Diskussionsrunden, wie „Ihre Daten sind sicher – und die Erde ist eine Scheibe“ stehen auf dem Programm.
atsec präsentiert sich zum ersten Mal mit einem eigenen Messestand und bietet ein umfassendes Repertoire an Beratungsthemen und Informationen durch Ihre IT-Security-Spezialisten. Dies möchten wir zum Anlass nehmen, all unsere geschätzten Geschäftspartner und Interessenten zu diesem besonderen Messe-Highlight einzuladen. Beigelegtes Gastticket ermöglicht den kostenfreien Eintritt.

Besuchen Sie den Stand Nr. 463 von atsec – wir freuen uns auf Sie!

Risiko: Analyse

Wer zum Return on Invest (ROI) beim Thema Sicherheit befragt wird, flüchtet oft genug in Allgemeinplätze – erhöhte Sicherheit, verbesserte Prozesse – allesamt kaum messbare Größen. Dabei gibt es einen probaten Weg, Sinn und Notwendigkeit von Sicherheitsmaßnahmen zu bestimmen: die Risikoanalyse. Hier werden Kosten und Wahrscheinlichkeit eines Schadensfalls dem Aufwand zur Abwendung gegenübergestellt – also ähnlich, wie die Entscheidung für eine Versicherung fällt.

„Unternehmenseigene Werte“

Der englische Begriff **„Asset“** lässt sich nur recht hölzern ins Deutsche übertragen, bezeichnet aber den wichtigen ersten Schritt jeder Risikoanalyse: eine Zusammenstellung der Werte im Unternehmen, ohne die ein geregelter Geschäftsbetrieb nur schwer weiterzuführen ist. Neben den klassischen materiellen Werten wie Gebäuden, Produktionsanlagen und Waren sind dies vor allem Informationen – Konstruktionspläne, Verfahrensbeschreibungen, Kunden- und Finanzdaten. Zu den Assets gehören auch Dienstleistungen (Rechenzentrum, Telekommunikation, Personalabteilung, Wachdienst, usw.), Prozesse und Verfahren (Fertigung, Entwicklung, Vertrieb, Logistik), Mitarbeiter (und deren Fähigkeiten, Wissen und Erfahrung) sowie natürlich die Informationstechnik (IT).

Diese Assets sind zusammenzustellen und zu klassifizieren, also nach folgenden Kategorien zu bewerten:

- **Wert** des Assets – quantitativ oder qualitativ („niedrig“/„mittel“/„hoch“)
- **Schutzziele:** Einstufung nach Vertraulichkeit, Integrität und Verfügbarkeit
- **Schadenskategorien** bei Verletzung der Schutzziele
- **Schadenshöhe** je Kategorie (entspricht dem Schutzbedarf)

Jedes Asset ist einem Eigentümer zugeordnet.

Der Schaden lässt sich in Kategorien einteilen und die Schadenshöhe wie folgt bezeichnen:

- **Verlust** (Wert des Assets, Aufwand für Wiederbeschaffung/-herstellung)
- **Beeinträchtigung des Geschäftsbetriebs** (qualitativ)
- **Verstoß gegen Gesetze und Verträge** (Höhe der Strafe)
- **Ansehen bei Kunden, Kreditwürdigkeit** (qualitativ)

Der höchste Schadensbetrag ergibt den Schutzbedarf des Assets.

Risikoanalysen werden zuerst für die hier als kritisch identifizierten Assets, also jene mit einem hohen zu erwartenden Schaden, durchgeführt.

Gelegentlich stellt sich die Frage, welche Risiken den IT Systemen an sich zugeordnet sind. Hier ergibt sich der Schutzbedarf offensichtlich nicht aus dem Wert des IT-Systems als solchem, sondern anhand der Geschäftsprozesse, die auf diesen Systemen verarbeitet werden, genauer aus den Risiken für den Geschäftsprozess selbst, wenn Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigt werden.

Begriffe

Ein paar Begriffe sind vorab zu erläutern – der wichtigste: **Risiko**. Ein Risiko ergibt sich, wenn einerseits eine **Schwachstelle** existiert, und andererseits eine **Bedrohung** vorhanden ist. Im Umkehrschluss bedeutet dies, fehlt die zu einer Schwachstelle passende Bedrohung, oder gibt es eine Bedrohung, aber keine geeignete Schwachstelle, so besteht auch kein Risiko (vgl. Tabelle 1, quasi eine dünn besetzte Matrix). Diese Erkenntnis reduziert die Anzahl der zu betrachtenden Risiko-Szenarien erheblich!

An dieser Stelle sei die Theorie durch ein wenig Praxis entzaubert: ein Erdbeben stellt eine Bedrohung dar, die (unzureichende) bauliche Struktur eine Schwachstelle; das resultierende Risiko wäre, je nach Art des Gebäudes, Einsturz, Feuer, Kernschmelze, etc. Fehlt die Bedrohung, hier die Gefährdung durch Erdbeben, ist die Risiko-Betrachtung für dieses Szenario bereits beendet.

Eintrittswahrscheinlichkeit

Zur Vollständigkeit der Risiko-Betrachtung wird die sogenannte **Eintrittswahrscheinlichkeit** eines Schadensfalls beurteilt. Diese gibt an, wie oft das Eintreten eines Schadensfalls in einem bestimmten Zeitraum angenommen wird. Die Skala hierfür ist logarithmisch (etwa: Stunde, Tag, Monat, Jahr, 100 Jahre), um Fehler bei der Abschätzung auf höchstens eine Größenordnung (also etwa „Stunde“ statt „Tag“) zu reduzieren.

Die Eintrittswahrscheinlichkeit ist größtenteils abhängig von der Exponiertheit des Assets. Einerseits ist die Anzahl und Vertrauenswürdigkeit der Nutzer, die sich grob in drei Größenkategorien einteilen lassen, relevant: anonym (etwa alle Internet-Benutzer), pseudonym (z. B. Benutzer eines Forums mit eigener Kennung) und persönlich identifiziert (d.h. die Identität wurde verifiziert). Andererseits ist die Mächtigkeit der Schnittstellen ausschlaggebend: welche Funktionen sind verfügbar und inwieweit unterliegt der Zugriff einer Autorisierung (also einer Berechtigungsstruktur).

Wichtig ist hierbei, dass die Eintrittswahrscheinlichkeit **unabhängig von der Motivation** eines Angreifers ist! Die Motivation ist bereits implizit in der Schadenshöhe (=Schutzbedarf) enthalten – ist diese(r) als „hoch“ anzusetzen, muss davon ausgegangen werden, dass sich immer **mindestens ein Angreifer** mit genügend Ressourcen (Zeit, Wissen, Technologie) findet.

Szenarien

Bedrohung	Verfügbarkeit				Vertraulichkeit		Integrität		
Schwachstelle	Ausfall	Elementar-Ereignis	Umwelt	Diebstahl	Kenntnisnahme	Weitergabe	Zutritt	Zugang	Manipulation
Prozesse	●			●	●	●	●	●	●
Mensch	●			●	●	●	●	●	●
Umgebung		●	●	●			●		●
IT-Architektur	●				●			●	●
Konfiguration	●				●			●	●
Hardware	●				●			●	●
Software	●				●			●	●

Tabelle 1: Risiko-Szenarien

Was ist eine **Bedrohung**? Eine Bedrohung wirkt immer gegen eines der drei Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit (Authentizität wird gerne als viertes Schutzziel dazu genommen, ist aber tatsächlich nur ein Aspekt der Integrität).
Eine Schwachstelle bezeichnet eine Schwäche eines organisatorischen Prozesses oder eines technischen Systems.

Methodik

Bevor mit den Risiko-Analysen begonnen wird, sind die Assets hinreichend zu beschreiben und einzuordnen. Unter anderem sind hier Klassifizierung, vorhandene Schutzmaßnahmen und Schnittstellen wichtig.
Bei den Risiko-Analysen der verschiedenen Assets lassen sich Redundanzen vermeiden, indem die Analysen modular aufgebaut werden: Assets wie *Rechenzentrum, Betriebssystem, Netzwerk, Middleware* (Datenbanken, Webserver, etc.) werden vorab **einmal** allgemeingültig analysiert. Danach konzentriert sich die Risiko-Analyse bspw. einer Applikation auf die **spezifischen** Risiken, statt sämtliche Betrachtungen über die Umgebung erneut abzuhandeln.

Risiko = Schadenshöhe x Eintrittswahrscheinlichkeit

Risiko-Analysen erfolgen am besten in **drei Stufen**: zuerst eine *initiale Analyse*, hierauf folgt die *Definition* und *Implementierung* von *Sicherheitsmaßnahmen*, die von einer *Analyse* der *Wirksamkeit* dieser Maßnahmen abgeschlossen wird.
Sofern keine konkreten Zahlen für eine quantitative Analyse vorhanden sind, ist immer ein qualitativer Ansatz anzuraten – also etwa eine Einteilung in *„niedrig“*, *„mittel“* und *„hoch“*. Insbesondere ist eine zu feine Granularität zu vermeiden – eine Risiko-Analyse wird nicht exakter, je mehr Parameter einfließen, dies führt im Gegenteil zu erheblichen Ungenauigkeiten.
Des Weiteren sollen bei allgemeingültigen Risiko-Analysen nicht verschiedene Risiko-Szenarien verkettet, also Abhängigkeiten mehrerer Schwachstellen und Bedrohungen betrachtet werden, weil sonst kaum noch sinnvolle Aussagen zur Eintrittswahrscheinlichkeit getroffen werden können. Für Sonderprüfungen, in denen eine *konkrete Gefahr* zu analysieren ist – beispielsweise ein Exploit, für den kein Patch verfügbar ist – ist eine solche Aneinanderreihung dagegen durchaus zulässig und sinnvoll.

Risiko-Analyse

Literatur zur Methodik von Risikoanalysen gibt es im Überfluss – leider wird aber die *eigentliche Analyse* nur selten so beschrieben, dass es eine direkte Umsetzung erlaubt. Daher sei hier der konkrete Aufbau einer Risiko-Analyse skizziert. Zuerst ist das Asset zu beschreiben, also seine Verwendung sowie seine Schnittstellen und Abhängigkeiten zur Umgebung. Des Weiteren sind die Annahmen bzgl. der (vorhandenen) Sicherheitsmaßnahmen des Assets und seiner Umgebung zu dokumentieren. Hierauf erfolgt eine erste Risiko-Einschätzung bezüglich der Schutzziele, also bezüglich der Gefährdung von Vertraulichkeit, Integrität, Verfügbarkeit.
Die eigentliche Risiko-Analyse definiert im ersten Schritt die für das Asset relevanten Schwachstellen und Bedrohungen, die in einer Matrix gemäß →*Tabelle 1* dann die relevanten Szenarien ergeben. Zu jedem Szenario ist nun die Eintrittswahrscheinlichkeit und die jeweilige Schadenshöhe (die möglicherweise niedriger ist als die Gesamt-Schadenshöhe des Assets) festzulegen. Der zweite Schritt besteht in der Festlegung geeigneter Gegenmaßnahmen zu den Szenarien. Schritt drei prüft die *Wirksamkeit* der Risiko-Behandlung: bei Gegenmaßnahmen also auf ausreichende Minderung der Eintrittswahrscheinlichkeit, bei der Vermeidung von Risiken, ob die relevanten Bedrohungen tatsächlich nicht mehr vorhanden sind.

Risk Treatment

Nach der Erhebung der Risiken ist zu entscheiden, wie diesen zu begegnen ist. Vier Arten der Risiko-Behandlung werden unterschieden:

- Anwendung von *Gegenmaßnahmen*, etwa das Schließen von Schwachstellen
- *Vermeidung* von Risiken, z. B. der Verzicht auf eine bestimmte Technologie
- *Übertragung* von Risiken, bspw. durch Abschluss einer Versicherung
- *Akzeptanz* des verbleibenden Risikos („Restrisiko“)

Beispiele für technische Gegenmaßnahmen sind Zugangs- und Zugriffskontrollen (Authentifizierung, Berechtigungsstufen), Schutz von Kommunikationswegen (z. B. durch Verschlüsselung) oder der physikalische Schutz von Komponenten (Zutrittskontrolle, etc.).
Zu beachten ist, dass Gegenmaßnahmen oft lediglich die Eintrittswahrscheinlichkeit reduzieren, aber ein Restrisiko verbleibt. Ein solches Restrisiko ist akzeptabel, wenn in einem bestimmten Zeitraum (ein Jahr, zehn Jahre) die Kosten für Gegenmaßnahmen den erwarteten Schaden übertreffen (Versicherungsprinzip). Verantwortlich für die Finanzierung von Gegenmaßnahmen bzw. die Übernahme des Restrisiko ist der Eigentümer des betroffenen Assets.

Risiko Management

Im Rahmen des Informationssicherheits-Managements weisen Risiko-Analysen einen relativ hohen Abstraktionsgrad auf – sie betrachten Prozesse und Verfahren, weniger einzelne IT-Systeme (*top-down* Ansatz). Konkrete, technisch detailliertere Risiko-Analysen werden im Rahmen von Sicherheitsaudits oder Sonderprüfungen bei Auftreten einer neuen Bedrohung (etwa „Schweinegrippe“ oder „Aschewolke“) durchgeführt (*bottom-up*).

Fazit

Der relativ hohe Aufwand zur Erfassung der Assets als Voraussetzung für Risiko-Analysen amortisiert sich durch die sinnvolle Steuerung der Investitionen in Sicherheit recht schnell. Wichtiger ist eine sinnvolle, den Erfordernissen eines Unternehmens angepasste Methodik, um ohne zu großen Aufwand zu verwertbaren Ergebnissen zu gelangen.

Scheinsicherheit virtueller Maschinen

Die Frage nach der Sicherheit von virtuellen Maschinen (VM) und deren Virtualisierungssoftware (**Virtual machine monitor**, VMM) beschäftigt derzeit weite Teile der IT-Welt. Das aktuelle Thema „Cloud Computing“, das auf virtuellen Maschinen aufsetzt, heizt die Debatte weiter an, eine genauere Überprüfung ist unumgänglich. Zu diesem Zwecke präsentieren Hersteller, IT-Analysten und Regierungsstellen Checklisten und Diskussionen, die die VMs absichern sollen.

Auch atsec engagiert sich auf diesem Gebiet und führt eine Reihe von Common Criteria Evaluierungen im speziellen Umfeld der virtuellen Maschinen durch. Die Sicherheitsproblematik von VMMs scheint also ausreichend adressiert zu werden. Neben dem offensichtlichen Aspekt der Separierung gibt es allerdings einen wunden Punkt, der kaum Erwähnung findet: die Sicherstellung, dass die dem Gast-Betriebssystem zur Verfügung gestellte Rechenumgebung sich genau so verhält, wie die reale Hardware.

Die Architektur eines VMMs besteht aus Hypervisor, Administrationsapplikationen und einem weiteren komplexen Softwareteil. Dieses „virtuelle Motherboard“ virtualisiert, simuliert oder emuliert die Hardware für das Gast-Betriebssystem. Beispiele in verschiedenen VMMs sind hierfür:

- Microsoft HyperV: Worker Prozesse
- KVM / Xen: QEMU
- VMWare: VMX Prozesse

Die Schwäche dieser „virtuellen Motherboards“ liegt allerdings in der Bereitstellung einer IT-Umgebung für Gast-Betriebssysteme, die sich identisch zur realen Hardware verhält. Typische Szenarios für den Einsatz von virtuellen Maschinen nehmen an, dass das Betriebssystem vertrauenswürdig ist – es werden üblicherweise Standardbetriebssysteme wie BSD Varianten, Linux, oder MS Windows eingesetzt. Diese Gast-Betriebssysteme kämpfen gegen die geläufigen Bedrohungen des Internets oder der Konzernnetzwerke, wie vertrauensunwürdige Benutzer und externe Angreifer. Zur Verteidigung nutzt ein Gast-Betriebssystem verschiedene Hardwarefunktionen. Da in VMM-Umgebungen eine Reihe dieser Funktionen von eben diesen „virtuellen Motherboards“ verarbeitet werden, kann sich ein Gast-Betriebssystem nur schützen, wenn die „virtuellen Motherboards“ sich genau so verhalten, wie die virtualisierte Hardware. Ein Betriebssystem, das auf reiner Hardware ausgeführt wird und keine Sicherheitsprobleme hat, sollte auch als Gast in einem VMM ausgeführt, sicher sein. Bei Fehlern in der komplexen Implementierung des „virtuellen Motherboards“ besteht nun aber die Gefahr, dass unprivilegierte Gastprogramme Sicherheitsfunktionen des Gast-Betriebssystems unterlaufen.

Derzeit konzentrieren sich die Untersuchungen vor allem auf die Sicherheit des Hypervisors. Zur Vermeidung unangenehmer Überraschungen empfiehlt sich jedoch, Augenmerk auf die Verbesserung der Implementierung der „virtuellen Motherboards“ zu richten. Hier genügen schon kleine Schritte, um grundsätzliche Probleme ganz aus der Welt zu schaffen. Eine Reduktion der Funktionalität durch die Hersteller wäre ein Beispiel. Es ist ausreichend, wenn ein „virtuelles Motherboard“ ein Hardwaregerät für einen bestimmten Zweck mit möglichst geringer Komplexität bereitstellt.

Allein das Wissen, dass die heutigen VMM-Implementierungen dem Gast-Betriebssystem keine äquivalente Sicherheit zur reinen Hardware bieten, stellt einen wertvollen Schutz dar. Angriffe auf ein Gast-Betriebssystem können, auch wenn dieses selbst keine Sicherheitsfehler enthält, durch die unzureichende Absicherung der „virtuellen Motherboards“ nicht wirklich ausgeschlossen werden.

Sicherheits-Audits bei der E-Plus Gruppe

Seit 2010 führt atsec im Auftrag der E-Plus Gruppe regelmäßig Sicherheitsaudits bei E-Plus Konzerngesellschaften und Dienstleistern durch, die Infrastruktur und Applikationen von E-Plus betreiben. Eine Kombination aus Desktop- und System-Audit prüft die Einhaltung der von E-Plus definierten Sicherheitsrichtlinien und Sicherheitsstandards. Zudem werden sowohl eventuell vorhandene sicherheitsrelevante Abweichungen in Prozessen und Verfahren des IT-Betriebs als auch technische Schwachstellen identifiziert und aufgezeigt. Die Ergebnisse der Sicherheitsaudits verwendet die E-Plus Gruppe im Rahmen des kontinuierlichen Verbesserungsprozesses zum Erhalt und zur Weiterentwicklung ihres hohen Sicherheitsniveaus.

Die E-Plus Gruppe ist mit über 21,5 Mio. Kunden der drittgrößte Mobilfunknetzbetreiber in Deutschland und seit dem Jahr 2000 Teil des niederländischen KPN-Konzerns. Zur E-Plus Gruppe gehören beispielsweise die Marken BASE, simyo und AY YILDIZ. Darüber hinaus sind viele weitere Marken wie MEDIONmobile (ALDI Talk), der ADAC oder MTV Partner der E-Plus Gruppe.

IMPRESSUM

atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson

Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG: DE205370914
Verantwortlich für den Inhalt:
Peter Wimmer (Anschrift s.o.)