Analyse von Informationssicherheit anhand von Geschäftsprozessmodellen[1]

Sascha Alpers, FZI Forschungszentrum Informatik, Karlsruhe
Yves Chassein, PROMATIS software GmbH, Ettlingen

Schlüsselworte
Informationssicherheit, Geschäftsprozessanalyse

1. Einleitung

Die Gewährleistung von Informationssicherheit ist eine wichtige Anforderung an betriebliche Informationsverarbeitung. Weil die betriebliche Informationsverarbeitung zunehmend mittels automatisierter bzw. teilautomatisierter Prozesse erfolgt, ist eine integrierte Betrachtung von Prozessen und Informationssicherheitsanforderungen für die Gestaltung von wirtschaftlichen (d. h. angemessenen) Maßnahmen zur Gewährleistung der Informationssicherheit zielführend. Sowohl Geschäftsprozess- als auch Informationssicherheitsverantwortliche können dadurch einfacher Sicherheitsprobleme identifizieren und gezielter Schutzmaßnahmen definieren. Hierdurch wird nicht nur die Sicherheit erhöht, sondern durch gezieltere Maßnahmen (anstatt Sicherheit im "Gießkannenprinzip" zu gewährleisten) auch die Sicherheitsökonomie verbessert.

Eine werkzeuggestützte, integrierte Betrachtung ermöglicht es zudem, die Verantwortlichen auf mögliche Sicherheitsprobleme hinzuweisen. Hierzu werden erfasste Modelle hinsichtlich der Informationssicherheit analysiert. Zwar ist es gegenwärtig nicht vorgesehen, mittels automatischer Analyseverfahren Sicherheitsprobleme jeden Typs offenzulegen, aber für gängige Problemtypen wie bspw. Vertraulichkeitsverluste stehen Analyseverfahren zur Verfügung.

2. Voraussetzung: aussagekräftige Geschäftsprozessmodelle

Geschäftsprozessmodelle müssen, um eine Analyse zu ermöglichen, bestimmte Informationen bereits beinhalten. Dies wird nachfolgend am Beispiel des Schutzzieles Vertraulichkeit verdeutlicht. Um die Gewährleistung der Vertraulichkeit prüfen zu können, ist es notwendig, dass Informationen über die verarbeiteten Objekttypen und die an der Verarbeitung beteiligten Subjekte vorliegen.

Je Objekttyp muss die Vertraulichkeit klassifiziert werden. Dazu kann eine Ordinalskala von 0 bis 4 verwendet werden. Zudem muss bekannt sein, welche Aktivitäten eines Prozesses auf welche Objekte zugreifen. Da Aktivitäten von Menschen und anderen Ressourcen (z. B. IT−Systemen) durchgeführt werden, muss jeweils bekannt sein, welche so genannten Subjekte an der Durchführung einer Aktivität beteiligt sind. Für jedes Subjekt muss dann die Vertrauenswürdigkeit klassifiziert werden. Auch hierzu kann eine Ordinalskala von 0 bis 4 verwendet werden.

Abbildung 1 zeigt als Beispiel den als Petrinetz[2] modellierten, vereinfachten Auftragsbearbeitungsprozess[3]. Die notwendigen Objekttypen sind in der Darstellung jeweils an den Objektspeichern notiert. Die Notation ist hier jeweils Ausdruck einer formalen Verknüpfung eines Objektspeichers mit einem Objekttypen. Die Objekttypen sind in einem Objekttypenmodell für das

---

[1] Manuskript zum Vortag im Rahmen der DOAG Konferenz und Ausstellung 2014 (2014.doag.de), 18.-20. November 2014, Nürnberg

[2] Eine Einführung in Petrinetze ist z. B. [Reisig, W.: Petrinetze: Modellierungstechnik, Analysemethoden, Fallstudien. Vieweg+Teubner Verlag, Wiesbaden (2010).].

[3] Der Prozess wurde mit dem Horus Business Modeler (http://www.horus.biz) modelliert. Dieses Werkzeug unterstützt bei der Umsetzung der Horus-Methode [Schönthaler, F., Vossen, G., Oberweis, A., Karle, T.: Geschäftsprozesse für Business Communities: Modellierungssprachen, Methoden, Werkzeuge. Oldenbourg Wissenschaftsverlag (2011).]. Die Stellen der Petrinetze werden hier als Objektspeicher und die Transitionen als Aktivitäten bezeichnet. Eine funktionseingeschränkte kostenlose Version kann unter http://www.horus.biz/download heruntergeladen werden.

Beispiel festgelegt und beschrieben. Konkret kann aus der Darstellung bspw. entnommen werden, dass im Objektspeicher Auftragseingang nur Objekte des Typs Auftrag liegen können.

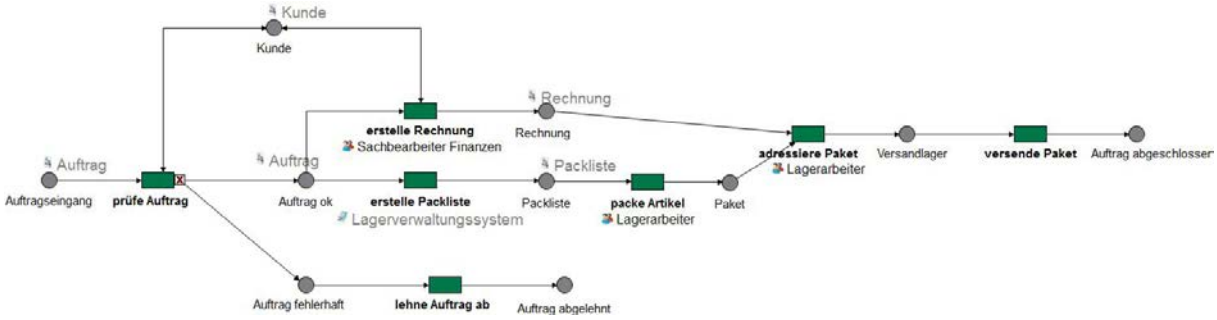

Abbildung 1: Beispielprozess Auftragsbearbeitung

3. Geforderte Eigenschaften

3.1 Geforderte Eigenschaft: Ablaufvertraulichkeit auf Objektebene

Die Ablaufvertraulichkeit fordert, dass keine unzulässige Kenntnisnahme von Informationen im Prozessablauf stattfinden darf. Hierzu muss für jede Aktivität eines Ablaufes gelten, dass die Aktivität nur Objekte von Objektspeichern konsumieren darf, deren Vertraulichkeit maximal der eigenen Vertrauenswürdigkeit entspricht (Bedingung für den Vorbereich einer Aktivität). Hierdurch wird verhindert, dass vertrauliche Informationen von nicht ausreichend vertrauenswürdigen Aktivitäten verarbeitet werden. Zudem ist zu fordern, dass Aktivitäten nur Objekte produzieren dürfen, deren Vertraulichkeit maximal der eigenen Vertrauenswürdigkeit entspricht (Bedingung für den Nachbereich). Der aufnehmende Objektspeicher bestimmt mit seiner Vertraulichkeit die Klassifizierung des produzierten Objektes. Eine Aktivität kann also die Vertraulichkeit eines Objektes durch die Verarbeitung reduzieren, beispielsweise wenn Daten gekürzt werden (z. B. gekürzte Kreditkartennummer). Für Petrinetze lassen sich diese Bedingungen formal als Erweiterung der Schaltregel beschreiben. Sei $C(p)$ die Vertraulichkeit einer Stelle $p \in P$ und $TW(t)$ die Vertrauenswürdigkeit einer Transition $t \in T$, dann lässt sich die Schaltregel einer Transition t um folgende Bedingungen erweitern:

$\forall\, p \in {}'t$: $C(p) \leq TW(t)$ (Vorbereich)
$\forall\, p \in t'$: $C(p) \leq TW(t)$ (Nachbereich)

Durch die Formalisierung können Eigenschaften und Analyseverfahren, welche bereits für Petrinetze beschrieben sind, auch auf die Sicherheitsanalysen übertragen und eingesetzt werden.

Für den Prozess aus Abbildung 1 bedeutet dies beispielsweise, dass wenn die Vertraulichkeit des Objektspeichers "Auftrag" 2 und des Objektspeichers "Kunde" 3 ist, die Aktivität prüfe Auftrag mindestens die Vertrauenswürdigkeit von 3 besitzen muss. Nehmen wir an, sie hat diese Vertrauenswürdigkeit und die Aktivität ist somit ausführbar. Die nachgelagerten Objektspeicher "Kunde", "Auftrag ok" und "Auftrag fehlerhaft" dürfen dann maximal die Vertrauenswürdigkeit 3 besitzen. Möglich wäre z. B., dass der Objektspeicher "Auftrag ok" die Vertraulichkeit von 2 besitzt, wohingegen der Objektspeicher "Auftrag fehlerhaft" nur die Vertraulichkeit von 1 besitzt (weil Daten gekürzt oder entfernt wurden).

3.2 Geforderte Eigenschaft: Vertrauenswürdigkeit einer Aktivität

Die Vertrauenswürdigkeit einer Aktivität darf maximal dem Minimum der Vertrauenswürdigkeit der beteiligten Subjekte entsprechen. Ist keine Vertrauenswürdigkeit explizit angegeben, kann implizit die Vertrauenswürdigkeit als das Minimum der Vertrauenswürdigkeiten der beteiligten Subjekte angenommen werden (sofern jeweils dort angegeben). Für den Prozess aus Abbildung 1 bedeutet dies,

dass die Aktivität "erstelle Rechnung" maximal die Vertrauenswürdigkeit der verknüpften Subjekte haben darf. Im Beispiel ist dies nur die Rolle "Sachbearbeiter Finanzen" bzw. ein Mitarbeiter, welcher diese Rolle zum Aktionszeitpunkt ausübt. Höhere Vertrauenswürdigkeiten sind nicht zulässig, niedrigere dagegen schon, weil dem Modellierer Zusatzwissen bekannt sein kann (wie die Ausführungsumgebung), welches die Vertrauenswürdigkeit der konkreten Aktivität reduziert.

3.3 Geforderte Eigenschaft: Vertraulichkeit eines Objektspeichers

Die Vertraulichkeit des Objektsspeichers muss mindestens der Vertraulichkeit des verknüpften Objekttyps entsprechen. Wenn keine Vertraulichkeit explizit angegeben ist, kann implizit die Vertraulichkeit des verknüpften Objektes angenommen werden. Bei Aggregaten von Objekttypen ist das Aggregat mindestens so vertraulich wie das Maximum der enthaltenen Objekttypen. In der Beispielaggregation aus Abbildung 2 Kunde bedeutet dies, dass das Aggregat "Kunde" mindestens so vertraulich sein muss wie der Objektwurzeltyp "Kunde" und die Objekttypen "Zahlart" und "Adresse".

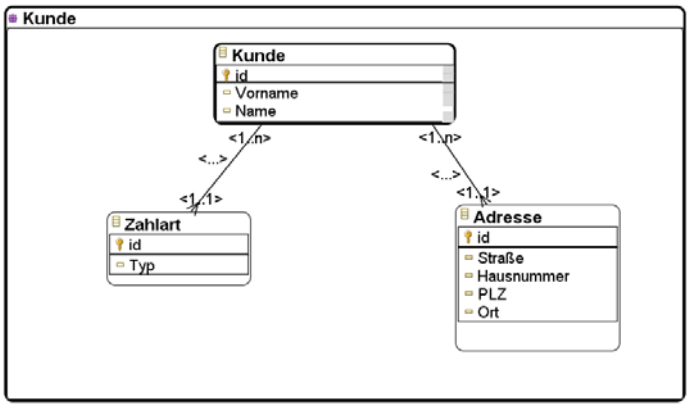

Abbildung 2: Beispiel einer Aggregation von Objekten

3.4 Geforderte Eigenschaft: Ablaufvertraulichkeit auf Attributebene

Das Schutzziel Vertraulichkeit lässt sich nicht nur auf der Ebene von Objekttypen bzw. Objekten, sondern auch feingranularer auf der Ebene von Attributen betrachten. Hierzu kann für jedes Attribut eines Objekttypen eine eigene Vertraulichkeit festgelegt werden. Im Beispiel aus Abbildung 2 heißt dies für den Objekttyp "Adresse", dass die Attribute "id"[4], "Straße", "Hausnummer", "PLZ" und "Ort" jeweils eine eigene Vertraulichkeitsstufe zugewiesen bekommen. Die Vertraulichkeit eines Objekttypen ist dann mindestens das Maximum der Vertraulichkeit seiner Attribute. Höhere Werte sind möglich und aufgrund der Kombination von Informationen in bestimmten Fällen auch sinnvoll. Beispielsweise kann bei einer Kreditkarte die Vertraulichkeit von Kreditkartennummer, Gültigkeit und Prüfziffer insgesamt höher sein als die Vertraulichkeit der einzelnen Elemente.

Die Durchführung von Aktivitäten benötigt oft nicht alle Attribute eines Objekttypen. Daher muss auf jeder Eingangskante einer Aktivität für jedes Attribut eines Objekttypen festgelegt werden, ob es benötigt wird. Dabei sind mindestens die folgenden Fälle zu unterscheiden:

- Attribut wird von der Aktivität verwendet.
- Attribut wird nur durchgereicht. In diesem Fall erfolgt keine Kenntnisnahme des Attributs bzw. insbesondere des Attributwertes eines konkreten Objektes durch die Aktivität bzw. die an ihrer Durchführung beteiligten Subjekte. Das Attribut wird – ohne Änderung –

[4] "id" ist für den Objekttyp "Adresse" Primärschlüssel, also ein besonderes Attribut. Bzgl. der Vertraulichkeitseinstufung wird es jedoch wie andere Attribute auch behandelt.

wieder dem Ausgangsobjekt hinzugefügt. Es ist somit Teil eines Objektes in einem Objektspeicher des Nachbereichs und kann von nachfolgenden Aktivitäten auch verwendet werden.

- Attribut wird nicht verwendet und nicht durchgereicht. Faktisch wird das Attribut folglich ohne Kenntnisnahme durch die Aktivität gelöscht. Es ist somit nicht Bestandteil eines Objektes in einem Objektspeicher des Nachbereichs und kann von nachfolgenden Aktivitäten auch dementsprechend nicht verwendet werden.

Zudem können Attribute durch Aktivitäten in unterschiedlicher Weise bearbeitet werden. Deswegen muss auf jeder Ausgangskante für jedes Attribut des Zielobjektspeichers einer der folgenden Punkte festgehalten werden:

- Attribut unverändert von Eingangsobjektspeicher p übernommen. Dabei ist anzugeben, von welchem Eingangsobjektspeicher übernommen wurde. Dabei wird keine Aussage darüber getroffen, ob das Attribut der Aktivität kenntlich wurde oder nicht. Dies wird ausschließlich über die Eingangskante festgelegt.
- Attribut von Eingangsstelle p mit Änderung übernommen. Die Unterscheidung, dass hier (möglicherweise) eine Änderung erfolgte, ist notwendig, da nur im Falle einer Änderung eines Attributes dieses Attribut in einem neuen Objekttyp nun eine niedrigere Vertraulichkeit besitzen darf. Der Attributwert wurde durch die Aktivität z. B. gekürzt, so dass die Vertraulichkeit des gekürzten Attributwertes geringer ist.
- Attribut neu angelegt. Das Attribut bzw. der Attributwert wurden nicht von einem Eingangsobjekt übernommen, sondern wurden durch die Aktivität erzeugt.
- Attribut bleibt leer. Attribut ist vom Objekttyp des Zielobjektspeichers vorgesehen, wird aber weder durch Eingangsobjekte noch von der Aktivität bereitgestellt.

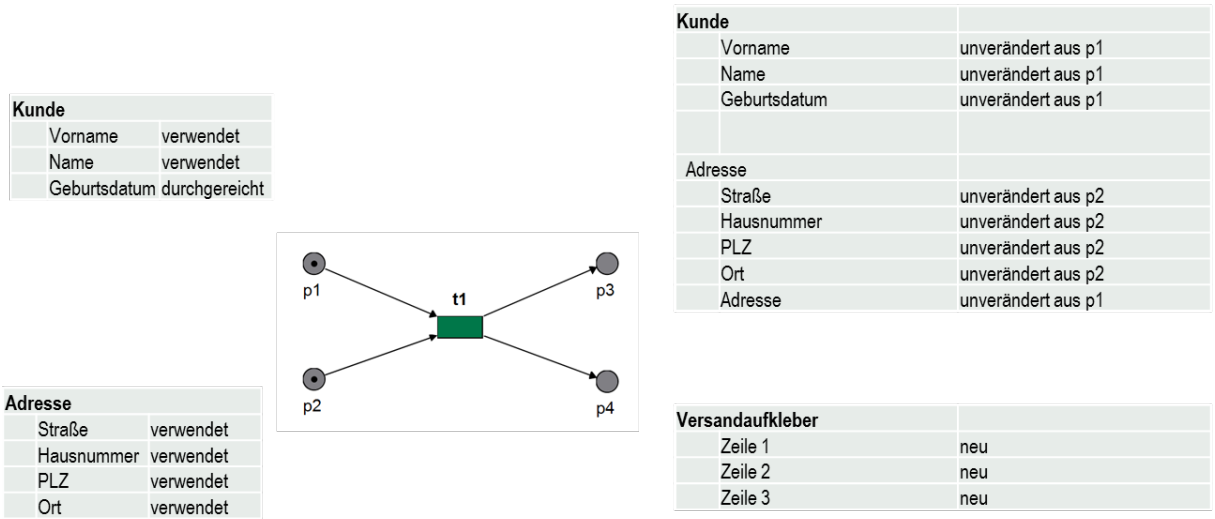

Abbildung 3: Beschriftung von Eingangs- und Ausgangskanten einer Beispielaktivität

4. Werkzeugunterstützung

Die entsprechend aussagekräftigen Geschäftsprozesse können mittels Horus Business Modeler auch hinsichtlich der beschriebenen Eigenschaften analysiert werden. Dabei wurde die Analyse von der Modellerstellung losgelöst. Während die Modellerstellung mittels Horus Business Modeler erfolgt (eine Freeware-Version kann unter http://www.horus.biz/download heruntergeladen werden), wird die Analyse innerhalb des Horus GRC Managers durchgeführt. Dieses Werkzeug wurde mittels Oracle

APEX erstellt. Es ermöglicht einerseits die Erzeugung statischer Prüfberichte hinsichtlich ausgewählter Modelle und der beschriebenen Eigenschaften und andererseits dynamischer Reports. Letztere bieten die Möglichkeit, einzelne Probleme mittels Drill-Down genauer zu betrachten.

5. Ausblick

Hier wurde exemplarisch die Integration des Schutzzieles Vertraulichkeit beschrieben. Die spätere Integration weiterer Schutzziele wie bspw. Prozess- und Datenintegrität, Datensparsamkeit und Zweckbindung von Daten ist ebenfalls bereits vorgesehen. Außerdem können zukünftig Sicherheitsrestriktionen optional auch mit ihrem Grund (z. B. gesetzliche Vorschriften) verknüpft werden. Dadurch können bei Änderung eines Grundes (z. B. durch den Gesetzgeber) die entsprechenden Restriktionen leichter aktualisiert werden.

Kontaktadressen:

Dipl.-Informationswirt Sascha Alpers
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe

Telefon: +49 721 9654-616
Fax: +49 721 9654-617
E-Mail: alpers@fzi.de
Internet: www.fzi.de

Dipl.-Informatiker Yves Chassein
PROMATIS software GmbH
Pforzheimer Str. 160
76275 Ettlingen

Telefon: +49 7243 2179-0
Fax: +49 7243 2179-99
E-Mail: yves.chassein@promatis.de
Internet: www.promatis.de