Manipulation von Quellcode unter Umgehung der bestehenden Berechtigungsbeschränkungen via SE30 / ATRA / ABAP_TRACE / SAT (Laufzeitanalyse / ABAP Trace)

Dipl.-Betriebswirt Christoph Wildensee, CISM, CRISC, ist IV-Revisor bei der Stadtwerke Hannover AG.

1. Einleitung

Geht man davon aus, dass im Rahmen der Arbeitsplatzrollendefinitionen im SAP die Ausprägungen der Berechtigungsobjekte stärker vorliegen und Transaktionsberechtigungen die eigentliche Trennlinie darstellen, um die Rollen voneinander abzugrenzen, und dass auch Berechtigungen wie das Ausführen von Programmen etc. (SA38, SE38, SE80, SE84 […]) – zumindest in Teilen – nicht ermöglicht werden, um nicht unerlaubt betriebswirtschaftliche Funktionen auszuüben, entsteht über die Berechtigung der zunächst harmlos klingenden **Laufzeitanalyse** wiederum die Möglichkeit, eine Aufweichung dieses bewusst restriktiven Ansatzes herbeizuführen.

Die Transaktionen **SE30 / ATRA / ABAP_TRACE / SAT** erlauben es, Programme, Transaktionen und Funktionsbausteine in ihrem Laufzeitverhalten zu analysieren.

Grundsätzlich sollte diese Funktion ausdrücklich in Rollen der Administration und ggf. auch der Revision zu finden sein, nicht selten wird sie aber auch anderen Unternehmensfunktionen wie der IT-Sicherheit oder auch Fachbereichs-Key-Usern in deren Rollen implementiert.

Bisher ist die kritische Seite dieser Funktionalität noch nicht ausreichend gewürdigt worden. Die Beschreibung „Laufzeitanalyse“ suggeriert eine gefahrlose Berechtigungsverteilung und Nutzung und stellt die damit einhergehende Problematik kaum ausreichend dar.

Der nachfolgende kurze Abriss zeigt, wie einfach es ist, über die Laufzeitanalyse ohne Change-Rechte auf die dargestellten Sourcen Quellcode einzuschleusen und ablaufen zu lassen, sofern die „Tips & Tricks“ erfolgreich im Rollenzugriff sind.

2. Vorgehen zur unerlaubten Rechte-Zuweisung

Der Aufruf der SAP-Laufzeitanalyse als Beispiel für SAP-implementierte Fehlerquellen stellt das folgende Dynpro zur Verfügung:

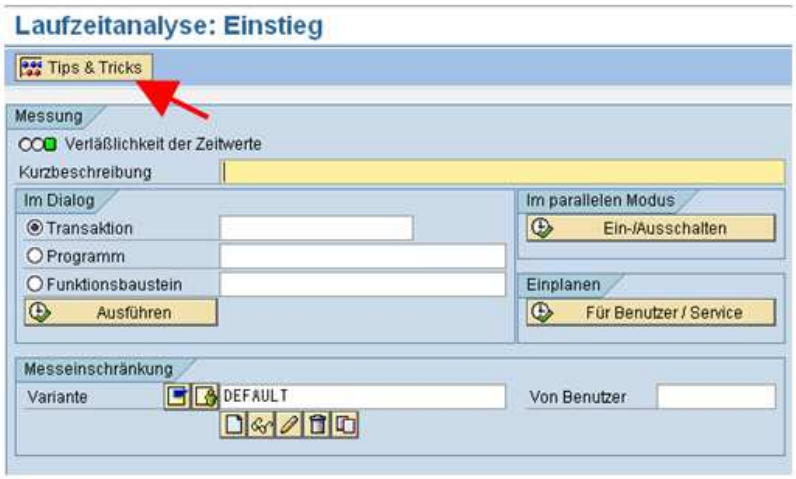

Abb. 1: Start von SE30 (auch S_DATASET-Berechtigung notwendig, nicht so bei Transaktion SAT).

Nach Betätigen des Buttons „Tips & Tricks“ und Auswahl z.B. des ersten Punktes der Laufzeitbeispiele (ABAP Objects Performance Examples) unter „SQL Interface“ erscheint SELECT-Quellcode in zwei Varianten auf die SAP-Testdatenbanktabelle SBOOK (Flug-Buchungen [die anderen Beispiele funktionieren nach dem selbem Muster]).

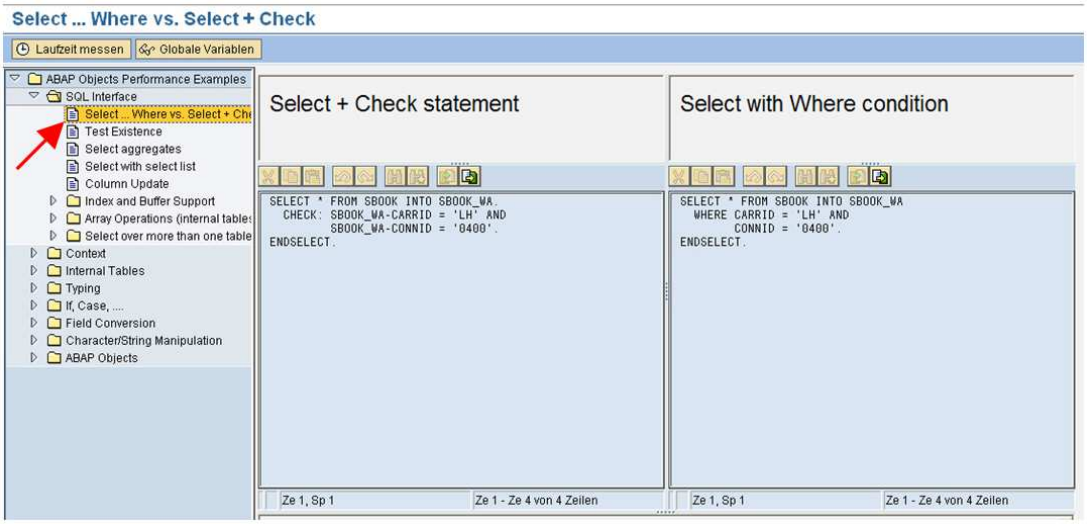

Abb. 2: Dialog „Tips & Tricks“.

Ohne Change-Rechte auf die Quelltexte können mit dem Start eines im **Internet frei verfügbaren Tools zur Manipulation von Microsoft-Windows-Fenstern** die Inhalte eines in SAP nicht änderbaren Fensters manipuliert werden. Der Menüpunkt „Send Text“ des Programms erlaubt es, einen beliebigen „Quellcode-Schnipsel“ an das Fenster zu senden (Überschreiben).

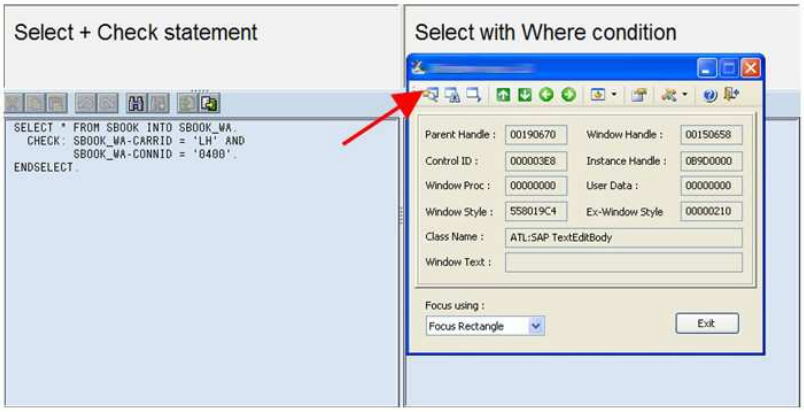

Abb.3: Start der Manipulation.

Das erste Icon („Find Window Under Cursor“) ermöglicht die Auswahl eines Fensterbereiches, der manipuliert werden soll. Nach Auswahl des Fensters mit dem Quellcode (mittleres Fenster mit Code-Fragment) erhält das Programm alle notwendigen Informationen, um den eigentlich nicht manipulierbaren Fensterbereich zu verändern.

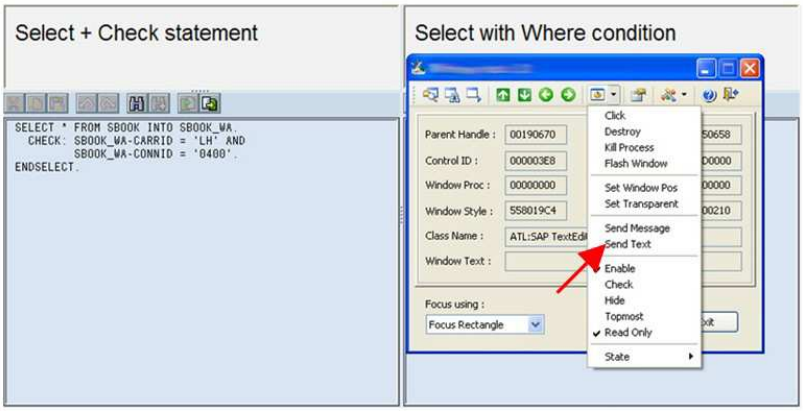

Abb. 4: Alle Informationen stehen zur Manipulation des Fensters zur Verfügung.

Der Menüpunkt **„Send Text“** erlaubt nun, den gewünschten „Quellcode-Schnipsel“ an das Fenster zu senden, um diesen neuen Code auszuführen.

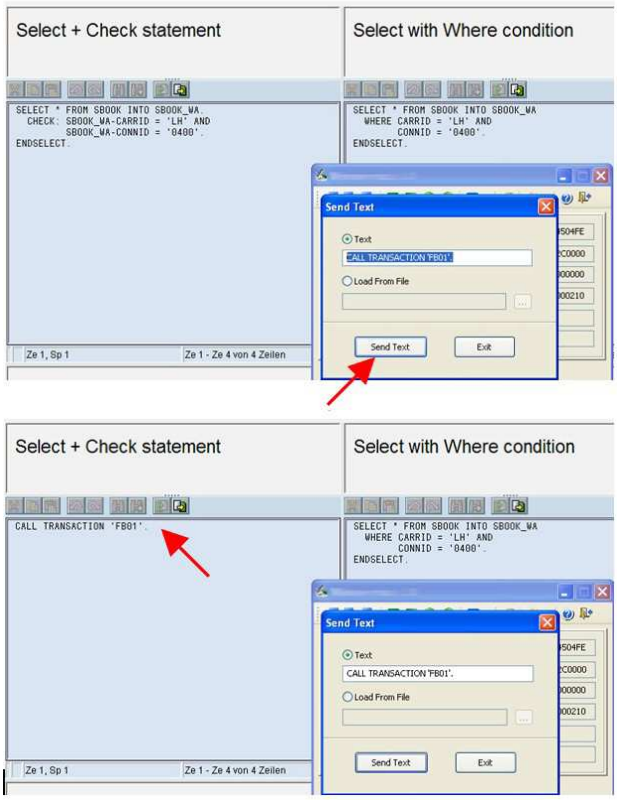

Abb. 5: Beliebiger Codeschnipsel wird aufgerufen.

Nach Betätigung des Buttons **„Laufzeit messen“** springt die Programmabfolge nach Ausführung von „CALL TRANSACTION ’FB01’.“ in die Transaktion FB01 (Beleg buchen). Sofern die dort geforderten Objekt-berechtigungen vorhanden, die Ausprägungen der Berechtigungsobjekte also umfangreich gegeben sind (in diesem Fall z.B. weitreichend in F_BKPF* und F_FAGL_SEG), **kann über diesen Weg ein Buchungsvorgang ermöglicht werden, obwohl eigentlich keine Transaktion FB01 im Berechtigungsstammsatz vorhanden ist**.

„CALL TRANSACTION“ führt nur einen Authority-Check für Transaktionen durch, wenn dies explizit über die Tabelle TCDCOUPLES und den Parameter „auth/check/calltransaction“ aktiviert wurde.

3. Zerstörung und Manipulation im System

In ihrer Wirkung erheblich bedenklichere Text-/Quellcode-Mitgaben sind hier jedoch auch **ohne weit reichende Modulberechtigungsobjektausprägungen** möglich.

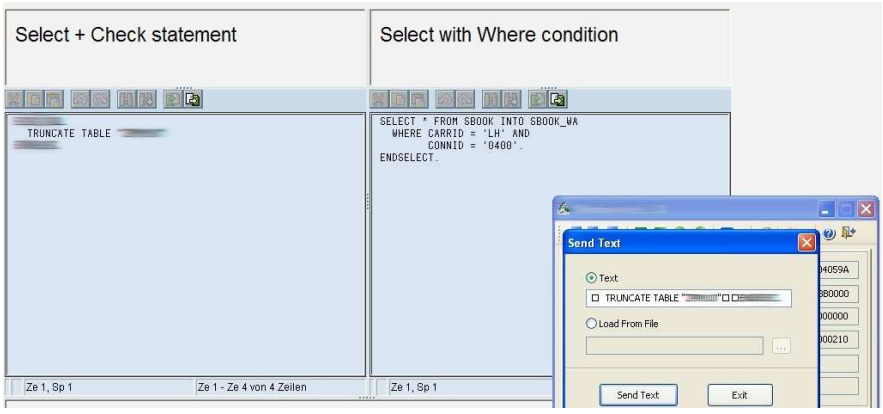

Abb. 6: Löschen von Tabelleninhalten.

Eine „EXEC SQL“-Einbettung des „TRUNCATE TABLE“-Befehls entfernt nach Betätigung des Buttons „Laufzeit messen“, sofern der Code fehlerfrei übergeben wurde, **ohne Protokollierung sämtliche Inhalte aus der angegebenen Tabelle.** Es ist auch möglich, Tabellen- / Feldinhalte (z.B. auch Protokollsätze) selektiv zu entfernen oder lediglich zu verändern, ohne dass dies (zunächst) ersichtlich ist. Hierüber ist also auch eine Inhaltsfälschung möglich.

4. Berechtigungsherkunft

Eine Transaktion, die eine direkte Quellcodeansicht und die weitere Ausführung des **angezeigten** Codes offeriert, ohne dass der zugrundeliegende Quellcode vor dem Anstarten nochmals geladen wird, sollte in produktiven SAP-Systemen in keiner Arbeitsplatzrolle zu finden sein. Während Transaktionen wie SE38, SE84 usw. die Programmaufrufe vor der Ausführung aus der Programmbibliothek aktualisieren und somit eine Mitgabe von Quellcode-Fragmenten nicht zulassen, ist dies über die Transaktionen SE30 / ATRA / ABAP_TRACE / SAT möglich.

SE30, ATRA und ABAP_TRACE erhalten die Berechtigungsprüfung über die Methode „check_trace_authority“ in „init_trace_files“ (SAPMS38T):

```
method check_trace_authority.
* authority check: part 1
* objtype = 'SYST' = trace authority
* (objtype = 'DEBUG' => debug authority)
  authority-check object 'S_DEVELOP'
                id   'OBJTYPE'          field 'SYST'
                id   'DEVCLASS'         dummy
                id   'P_GROUP'          dummy
                id   'OBJNAME'          dummy
                id   'ACTVT'            field '01'.    "create trace
  if sy-subrc <> 0.
    message e011 raising authority_trace.
  endif.
endmethod.
```

Wer die vom Programm geforderte Ausprägung aufweist (Berechtigungsobjekt S_DEVELOP mit Aktivität 01 und Objekttyp SYST und übriger Steuerungsfeldervollausprägung), kann die Manipulation mit SQL auslösen. Entsprechend sollten in mehrstufigen Systemlandschaften die zuvor genannten Transaktionen ausdrücklich nur in den Entwicklerrollen der Entwicklungssysteme zu finden sein. Dabei ist der Fokus aber nicht nur auf die Unterbindung des Transaktionscodes, als vielmehr auch auf die Ausprägung des hier grundlegenden Berechtigungsobjektes zu legen, die in den Rollen nicht vorkommen sollte. Das Steuerungsobjekt S_DEVELOP mit Objekttyp SYST wird z.B. nur in wenigen Funktionen angefordert, auf die in Produktivumgebungen verzichtet werden kann. **Die Objekttypausprägung SYST sollte aus allen Berechtigungen entfernt werden**, so dass hier ein hohes Maß an Sicherheit entsteht (sogar für den „indirekten“ Aufruf [Transaktion, FuBa etc.]), es verhindert bereits den Aufruf.

Für die Transaktion SAT (Programm SAPMS_ABAP_TRACE) ergibt sich eine andere Sicht. Der Grund liegt in der ungleichen Behandlung dahingehend, ob das System änderbar ist oder nicht.

Routine RSHOWTIM (Auszug)	Änderbares System	Nicht änderbares System
[...] ELSE. * system locked MESSAGE S840(TR). **EXIT.** ENDIF. AUTHORITY-CHECK OBJECT '**S_DEVELOP**' ID 'OBJTYPE' FIELD '**PROG**' ID 'DEVCLASS' DUMMY ID 'P_GROUP' DUMMY ID 'OBJNAME' DUMMY ID 'ACTVT' FIELD '**02**'. IF SY-SUBRC <> 0. MESSAGE S400(S7). EXIT. ENDIF. [...]	... ansonsten Message 840 („System auf nicht änderbar gesetzt.“). Ende ! (Wenn System änderbar, dann erfolgt eine) Berechtigungsprüfung auf S_DEVELOP **Ein Entwicklungssystem ist üblicherweise änderbar, somit Durchlaufen der Berechtigungsprüfung.**	... ansonsten Message 840 („System auf nicht änderbar gesetzt.“). Ende ! (Wenn System änderbar, dann erfolgt eine) Berechtigungsprüfung auf S_DEVELOP **Ein Produktionssystem ist üblicherweise nicht änderbar, somit kein Durchlaufen der Berechtigungsprüfung.**

In einem System wie z.B. dem Entwicklungssystem, das üblicherweise auf „änderbar“ steht, werden Berechtigungen häufig bewusst weiter gefasst und auch benötigt als in Produktionssystemen. Zur Gleichschaltung der Administratorenrechte (z.B. zur Herstellung von Systemkopien mit dann folgend geringerem Anpassungsaufwand) kann dies – und dies wäre ein schwerwiegender Fehler – auch für ein Produktionssystem gefordert werden. Dies gilt auch für das Berechtigungsobjekt S_DEVELOP mit Aktivität 02 und Objekttyp PROG. Im Quellcodeausschnitt ist zu erkennen, dass eine Berechtigungsprüfung, die in einem änderbaren System erfolgt, positiv durchlaufen wird, aber nicht wie zuvor auf Objekttyp **SYST** mit Aktivität **01**, sondern auf Objekttyp **PROG** mit Aktivität **02**. Hieran hängt die Replace-Funktion auf Tabellen.

In einem Produktionssystem erfolgt die Prüfung auf S_DEVELOP nicht, da das System üblicherweise auf „nicht änderbar“ steht. Liegen in den Rollen die Berechtigungen aber gleichermaßen vor, weil man davon ausgeht, dass das System „nicht änderbar“ ist und somit keine Berechtigung zur Manipulation gegeben sein kann, ist dies zu kurz gegriffen. In Ausnahmefällen muss auch ein Produktionssystem gelegentlich auf „änderbar“ gesetzt werden, z.B. wenn umfangreiche Dateneinspielungen im Customizing erfolgen, so dass hier ein Problem entstehen kann. Die SAP Note 1465138 erläutert: “In the "Tips & Tricks" of transaction SAT (or transaction SE30 in older releases), you can enter and execute ABAP source code if you have developer authorization S_DEVELOP (activity 02). This could be abused by malicious users to gain unauthorized access or produce incorrect behavior.” Auch die SAP Note 1661349 unterstreicht: „Ein authentifizierter Benutzer kann auf Funktionen in SE30 "Tips & Tricks" zugreifen, deren Zugang eingeschränkt sein sollte. Dies kann eine Rechteausweitung zur Folge haben.“ Nicht in allen Unternehmen werden sämtliche produktiven Systeme und Rollenausprägungen vollumfänglich aktuell gehalten, viele IT-Treuhänder arbeiten – auch je nach Risikoeinschätzung des Systems und der dort zu verarbeitenden Daten – mit älteren und höher ausgeprägten Rollenständen. Das Berechtigungsobjekt S_DEVELOP offeriert Manipulationsmöglichkeiten, die in Produktionssystemen, aber auch allgemein außerhalb der Entwicklerteams und der Entwicklungssysteme, ausgeschlossen sein sollten. Hinzu kommt die Sicht, dass eine irregulär stattgefundene Content-Manipulation mit Transaktion SAT außerhalb des Produktionssystems (z.B. im Testsystem) durch Beschäftigte außerhalb der Entwicklung und Modulbetreuung dazu führen kann, dass ohne Wissen der Entwickler und Modulbetreuer diese Inhalte in das Produktionssystem transportiert werden.

Folgende Maßnahme sollte neben der Beschränkung von S_DEVELOP mit Aktivität 01 und 02 auf den Notfalluser zusätzlich implementiert werden:

- Organisatorische Festlegung: Der Programmaufruf von SE30, ATRA, ABAP_TRACE und SAT sollte ausgeschlossen werden und nicht über weitere Wege wie der Transaktionserstellung, der Kopie-Modifikation im Kundennamensraum, dem Funktionsbausteinaufruf o.ä. genutzt werden können (Einziehen einer regelmäßigen Überprüfung)
- Die Revision sollte informiert werden, wenn das produktive SAP-System auf änderbar gesetzt wird.
- Die Revision sollte regelmäßig Code-Implementierungen im Kundennamensraum überprüfen.

5. Fazit

Nicht nur die Möglichkeit der Manipulation und Zerstörung oder Verfälschung von Inhalten an sich ist beachtenswert, sondern vielmehr auch der unkomplizierte Zugang zu einer von SAP implementierten Funktion als Verursacher. Es steht eine zunächst unschädlich wirkende Funktionalität zur Verfügung, die schwerwiegende Möglichkeiten der Manipulation via Hack-Tool eröffnet. **Ein Aufweichen der gewollt rollenbasierten Berechtigungsbeschränkungen und sogar ein Destabilisieren des Systems** sind über einen solchen Innentäter-Angriff (und dies ggf. sowohl in rechnungslegungsrelevanten als auch personalwirtschaftlichen Systemen) möglich. Weit reichende Modulberechtigungsobjektausprägungen sind, wenn es rein um die Zerstörung oder Verfälschung von Inhalten geht, nicht notwendig. Werden die Rollen mit Ausnahme des Notfallusers im **Objekt S_DEVELOP** ausdrücklich beschränkt **auf die Aktivität 03**, ist eine Manipulation wie beschrieben in keinem Fall mehr möglich und durch den Rollenausschluss der **manipulierenden Berechtigung für hinreichende Sicherheit an dieser Stelle gesorgt.**

Zu beachten:
SAP Note 1465138 (Change mode in SAT / SE30 “Tips & Tricks”) und
SAP Note 1661349 (Fehlende Berechtigungsprüfung in SE30 „Tips & Tricks“).

(Need more information: mailto: christoph (at) wildensee.de)

http://www.wildensee.de/wh30.exe

Christoph Wildensee.