



IBM Cognos 8 BI – Sicherheits Grundlagen

Sebastian Mai . BI-Consultant . 19.06.09

Dieser Artikel soll als Leitfaden beim Aufbau einer Security Umgebung für IBM Cognos Umgebungen verstanden werden. Er befasst sich mit den wichtigsten Grundlagen und Überlegungen in Zusammenhang mit verschiedenen Sicherheitsaspekten von IBM Cognos 8 BI Umgebungen. Von der Auswahl des richtigen Providers und einem Benutzer / Gruppen / Rollen Konzept bis hin zu Empfehlungen für sicherheitsrelevante Einschränkungen und Deployments beleuchtet er verschiedene Aspekte, die für den Aufbau einer Cognos 8 BI Lösung berücksichtigt werden sollten.

1. Die richtige Wahl des Providers

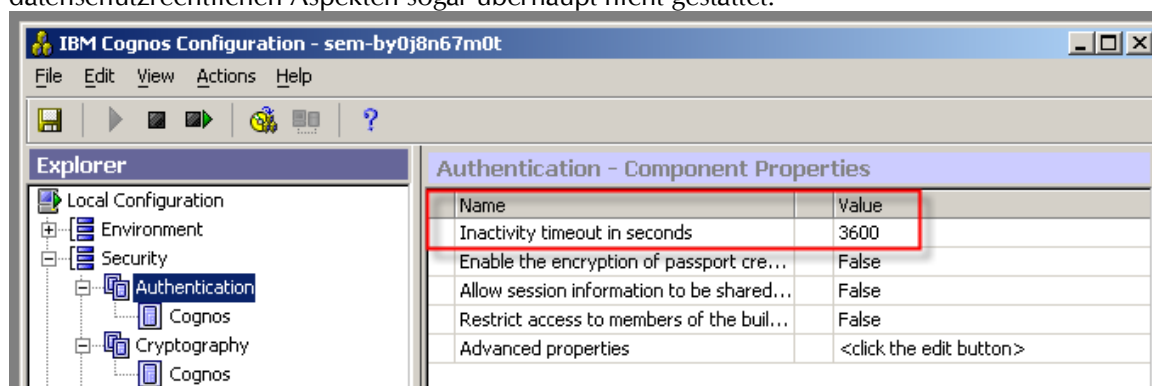
Die richtige Wahl der Authentifizierungsquelle hat meist größeren Einfluss auf die spätere Projektarbeit als angenommen. Hauptsächlich unterstützt IBM Cognos in der Version 8.4 die folgenden Quellen.

1. Active Directory Services
2. IBM Cognos Series 7
3. LDAP
4. NTLM
5. SAP

Auch wenn die Sicherheitsquelle IBM Cognos Series 7 mittlerweile in die Jahre gekommen ist, so kann der große Vorteil bei der Wahl dieser Quelle in einem großen Unternehmen die einfache und unbürokratische Verwaltbarkeit von Anwendern sein.

Die Rechte für die Administration liegen i.d.R. in der eigenen Hand, dies erhöht die Flexibilität und Unabhängigkeit enorm, da es in größeren Unternehmen durch bürokratische Prozesse beim Anlegen / Ändern von Benutzern / Gruppen leicht zu Verzögerungen kommen kann.

Meist ist der Zugriff auf Benutzer und Gruppen Administrationswerkzeugen z.B. innerhalb einer bestehenden Windows- oder LDAP-Struktur aufgrund von Sicherheits- oder datenschutzrechtlichen Aspekten sogar überhaupt nicht gestattet.



Hat man sich nun für einen Provider entschieden sollte man beachten, den Session Ticket Timeout in der IBM Cognos Configuration möglichst nicht höher als Standard einzustellen. (60 Minuten)

Der Session Ticket Timeout ist die Zeit in Sekunden, die ohne Aktivität in Cognos Connection ablaufen muss, bis das Ticket ungültig wird (respektive zur erneuten Anmeldeaufforderung des Anwenders führt).



Des Weiteren werden für die Dauer des Session Ticket Timeouts auch Ports im Java Application Server zur Authentifizierungsquelle aufgebaut und offengehalten.

Wird nun der Timeout höher als normal eingestellt, kann dies unter ungünstigen Umständen bei einer hohen Nutzerzahl über mehrere Tage hinweg dazu führen, dass dem Java Prozess irgendwann nicht mehr genügend Ressourcen zur Verfügung stehen, da die Session Tickets nicht schnell genug abgebaut werden können. Im Ernstfall kann dies dazu führen, daß Ports nicht mehr vollständig freigegeben werden können und der gesamte Application Server neu gestartet werden muss.

Ein zu niedriger Wert kann wiederum zu einer höheren Last auf Seiten der Authentifizierungsquelle (z.B. des LDAP Servers) und einer schlechteren Akzeptanz der Endanwender führen (weil sie sich ständig neu anmelden müssen – außer es handelt sich um eine Single Sign On Umgebung).

Der vorgeschlagene Wert von 60 Minuten ist daher als ein guter Kompromiß zu verstehen und führt in den seltensten Fällen zu Problemen.

1.1 Grundregeln im Umgang mit Cognos Connection

Folgende Grundsatzregeln haben sich in der Praxis als hilfreich erwiesen.

- **Vermeidung der Gruppe „Jeder“ oder „Everyone“**
Standardmässig ist nach der Installation allen Cognos Rollen diese Gruppe zugewiesen. Diese sollte man schnellstmöglich entsprechend durch die notwendigen Gruppen ersetzen.
- **Vermeidung von Rechtevergabe für einzelne Benutzer**
Ein Security Konzept steht und fällt mit seiner Anwendung. Ein System, das zum großen Teil auf Einzelzuweisungen basiert, kann nicht vollständig durchdacht sein und sollte dringend nachgebessert werden. Einzelzuweisungen von Rechten auf Ordner, Packages, Datenquellen und alle anderen wichtigen Objekte sind unbedingt zu vermeiden!
- **Vermeidung der Funktion „Verweigern“ oder „Deny“**
Anfangs wird diese Option gerne verwendet um „auf Nummer sicher zu gehen“. Dies führt in komplexeren Sicherheitsmodellen allerdings zu einem „Alptraum-Szenario“ der Wartbarkeit. Ein klar durchgezogenes Projektkonzept hilft bei der Vermeidung dieser Funktionalität.
- **Sonderfall Systemadministrator**
Eine klare Sonderrolle stellen Systemadministratoren in Cognos Connection dar. Unabhängig davon, ob überhaupt Rechte oder Deny Rechte vergeben wurden, dürfen Benutzer aus dieser Rolle **immer** alles. Dies hilft insbesondere dann, wenn man sich selbst ausgesperrt hat oder ein Verhalten auftritt, welches auf Sicherheitsbeschränkungen schließen lässt. Meist kann man dann das Verhalten mit dem Systemadministrator testen und kann somit schnell feststellen ob es sich tatsächlich um ein Problem wegen unzureichender Berechtigungen handelt.

1.2 Aufteilung in Projekte und Regionen

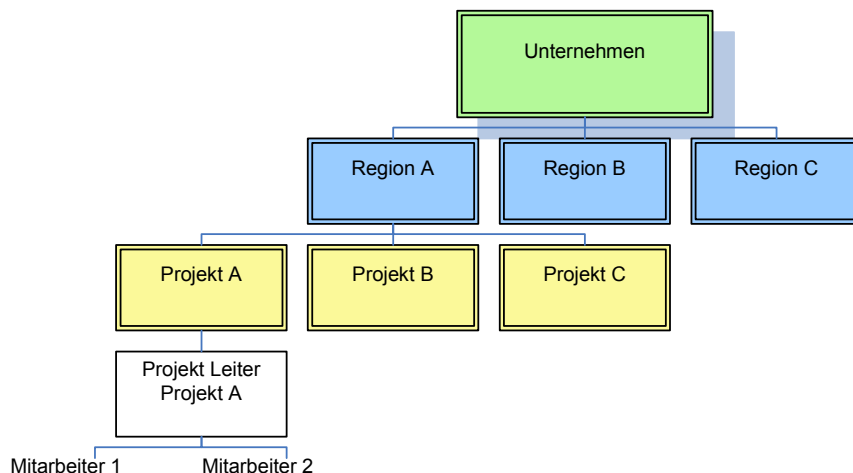


Abb. 1

Das in der Abb.1 dargestellte Organigramm einer Unternehmens- oder Projektstruktur ist auf die meisten Alltagsanforderungen anwendbar und soll uns in diesem Fall als Vorlage dienen. Die Regionen oder Bereiche sollten einen treffenden Namen besitzen und nach Möglichkeit auf **physischen** Zuordnungen (z.B. geographischen Informationen – Land / Region) basieren. Oft werden diese notwendigen Unterteilungen gerade am Anfang in den Projekten vernachlässigt. Bei internationalen Unternehmen und/oder Unternehmen mit Mitarbeiterzahlen über 100 Mitarbeiter ist eine solche Struktur für Cognos Connection zu empfehlen.

2. Gruppen / Rollenkonzepte

Entscheidend ist natürlich bei der Wahl der Zuordnungen in Cognos Connection und Framework Manager auch, ob man Rollen oder Gruppen verwendet.

Prinzipiell unterscheiden sich Rollen und Gruppen vom „Look und Feel“ nur in Details. Umso wichtiger ist es, daß man in der Praxis eine transparente Strategie bei Zuordnungen von Benutzern verwendet. Zu empfehlen ist hier die Trennung von fachlichen und technischen Einschränkungen.

2.1 Gruppen für fachliche Einschränkungen

Soll z.B. eine fachliche Einschränkung (auf die Sicht der Daten) stattfinden, so ist die Verwendung von Gruppen zu empfehlen.

Dies hat u. a. auch den Vorteil, dass die Gruppen als Mailverteiler verwendet werden können.

2.2 Rollen für funktionelle Einschränkungen

Rollen eignen sich besonders für technische / funktionelle Einschränkungen.

Als Beispiel eignet sich hier z.B. die Rolle der Systemadministratoren.

Diese Art von Trennung der Rollen macht es später deutlich einfacher, herauszufinden, welche Benutzer / Gruppen z.B. das Recht haben, HTML-Items in Report Studio Berichten zu betrachten.

3. Praxisbeispiel

Eine Firma XY hat 2 Aussenstellen in Deutschland und der Schweiz. Die Firma hat insgesamt 500 Mitarbeiter. Da die Außenstelle der Schweiz erst vom kurzem aufgekauft wurde, besteht noch keine durchgehende IT Infrastruktur und kein durchgängiges Securitykonzept. Der Kunde befindet sich gerade in der Migrationsphase der Umgebungen und bevorzugt übergangsweise daher eine



autarke Security-Umgebung mit einem LDAP Namespace. Der Kunde ist nun mit 2 Projekten in Deutschland und der Schweiz gestartet.

Auf Basis der gesammelten Informationen könnte der Entwurf für den Security Namespace wie folgt aussehen (Abb. 2).

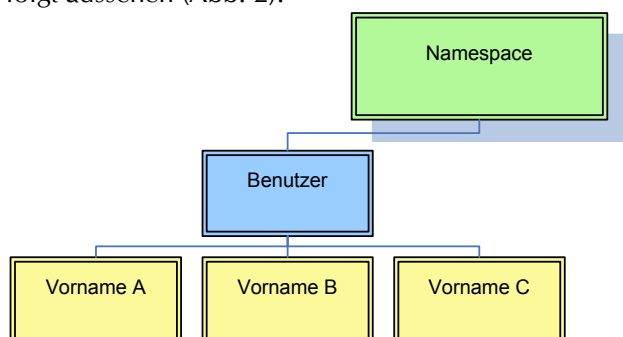


Abb. 2

In diesem Beispiel erfolgt eine Einteilung nach dem 1. Buchstaben im Vornamen der Benutzer (z.B. Ordner A für Anton Schmitt). Der Vorname eignet sich deshalb besonders, weil sich dieser im Laufe des Lebens in der Regel nicht mehr ändert (wohingegen sich der Nachname durch eine Heirat oder Scheidung durchaus ändern kann).

Weiterer Vorteil ist, dass man den Benutzer meist auch mit Vornamen kennt, wenn man ihn innerhalb der Authentifizierungsquelle sucht. Die Funktion oder das genaue Aufgabengebiet des Benutzers ist aber meist nicht bekannt bzw. nicht eindeutig. Hinzu kommt noch, dass sich die Aufgabengebiete und Funktionen einzelner Mitarbeiter innerhalb einer Firma oft ändern. Sollten nicht zu viele Benutzer auf das System zugreifen, ist es aber durchaus auch möglich, keine Aufteilung nach Regionen oder Anfangsbuchstaben der Vornamen vorzunehmen.

Sollte es sich um ein großes Unternehmen handeln, kann es zudem notwendig werden, die Benutzer zusätzlich nach ihrem Land oder ihrer Region zu ordnen.

3.1 Besonderheiten bei der Einschränkung auf Daten

Leider wird, was die Einschränkung der Daten angeht, oft nur sehr begrenzt mit einem Bewusstsein für Datensicherheit gearbeitet.

Oft höre ich vom Kunden die Aussage „Die Benutzer sind doch eh nicht schlau genug, um das herauszufinden“. Erfahrungsgemäß sollte man die Endbenutzer der BI Anwendungen aber in keinem Fall unterschätzen!

Als fatale Sicherheitsfallen stellen sich meist sogenannte benutzereingeschränkte Eingabeaufforderungen dar, die zumeist noch den Business Key als Übergabewert für den auszuführenden Bericht nutzen und es somit dem potentiellen „Angreifer“ besonders leicht machen, Berichte auszuführen, die nicht für Sie bestimmt sind. Dasselbe gilt natürlich auch für die sogenannten Drill-Through-Berichte, deren Aufruf auf gleiche Weise gelöst ist. Ursache ist hier meist eine fehlende Einschränkung auf allen Query Subjects im zugrunde liegenden Framework Manager Modell. Einschränkungen auf Daten sollten somit immer in dem zugrundeliegenden Datenmodell z.B. über ParameterMaps auf alle notwendigen Query Subjects gemacht werden und **nicht** innerhalb der Abfrage in Report Studio.

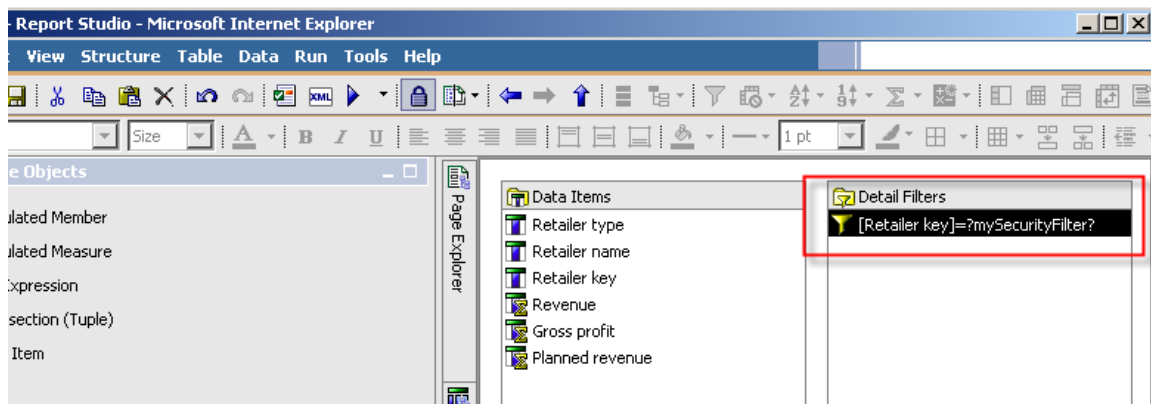


Abb. 3

Security Filter als Parameter in Report Studio sollten nicht verwendet werden.

Auch wenn der zugrundeliegende Prompt eine Auswahlbox ist!

Fazit: Wird man vom Kunden gebeten die Einschränkungen aufgrund von Sicherheitsbeschränkungen hinzuzufügen und nicht als „nice to have“, empfiehlt es sich, den Filter im Modell und nicht in Report Studio zu hinterlegen.

3.2 Deployment

Plant man den Aufbau mehrerer Umgebungen, z.B. einer Produktiv- und einer Entwicklungsumgebung, so ist es wichtig zu wissen, dass eine Übernahme der Benutzereinschränkungen von der Entwicklungs- oder Testumgebung zur Produktivumgebung nur dann möglich ist, wenn exakt die selbe Authentifizierungsquelle (gleicher Server, gleiche Namespace-ID, etc.) in Cognos 8 verwendet wird. Verwendet man Authentifizierungsquellen z.B. testweise und übernimmt die Sicherheitseinstellungen beim Deployment (Option) so bekommt man im Zweifel für jeden verwendeten Benutzer, der beim Import nicht gefunden wird, einen Fehler. Dies verzögert nicht nur den Importvorgang auf der Produktionsumgebung erheblich, sondern führt zudem noch zu einer gewissen Unübersichtlichkeit des Deployment-Vorgangs.

3.3 Framework Manager Packages in Cognos Connection per Standard verbergen

Ein oft angesprochenes Thema beim Kunden ist die Sichtbarkeit von neu publizierten Packages in Cognos Connection. Viele Benutzer fühlen sich von neuen Packages gestört. Sie wundern sich, warum diese in Cognos Connection auftauchen, obwohl Sie ja doch keine Berechtigung haben, dort hinein zu schauen oder dort Berichte auszuführen. In Cognos 8.4 gibt es zwar mittlerweile die Option, Elemente zu verstecken, aber die Verwendung dieser Option empfiehlt sich nicht für den angesprochenen Fall. Bereits in früheren Versionen konnte man sehr elegant über die Änderung eines Eintrages in der System.xml die Sichtbarkeit von neuen und bestehenden Packages ohne Ausführungsberechtigung ändern.

Die Datei befindet sich im Cognos 8 Verzeichnis unter templates\ps\portal\system.xml und der zu ändernde Eintrag sieht wie folgt aus.

```
<!-- CM filter added to content requests to only return objects "visible" to  
the current user -->  
<param name="visible">[permission(&quot;read&quot;); or  
permission(&quot;write&quot;); or  
permission(&quot;execute&quot;); or  
permission(&quot;traverse&quot;); or  
permission(&quot;setPolicy&quot;); ]</param>
```

Abb. 4



Diese Einstellung ist natürlich auch in der derzeit aktuellen Version (IBM Cognos 8.4) möglich
Hierbei entfernt man die Berechtigung "traverse" (vorletzte Zeile in Abb. 4).

4. Fazit

Ein vollständiges Sicherheitskonzept berücksichtigt sowohl Integrations-, Wartungs- als auch Datenaspekte und orientiert sich stark an der Struktur des Kunden. Meist führen nicht vollständig durchdachte oder schnelle Lösungen bei wachsenden Projekten zu Problemen. Die Komplexität von einer gut durchdachten vollständigen Sicherheitslösung wird oftmals unterschätzt. Mit Lösungsansätzen bietet dieser Leitfaden die Möglichkeit, den Start eines IBM Cognos BI Projektes gleich in die richtige Richtung zu lenken und beleuchtet gezielt unterschätzte, Themen die meist erst im Laufe eines BI Projektes kritisch werden.

Sebastian Mai

Trivadis AG

Elisabethenanlage 9

CH-4051 Basel

Internet: www.trivadis.com

Tel: +41-79 264 88 46

Fax: +41-61 279 97 56

Mail: sebastian.mai@trivadis.com
<http://sebastianmai.blogspot.com>