Sicherheitsaspekte bei dem Betrieb von ORACLE Forms- und Reports 11g

Ziele1

So wenig Informationen wie möglich nach draußen rausgeben, um einen Angriff so schwierig wie möglich zu machen. Keine Informationen zu Datenbanken, SIDs, Ports und Sicherheitsprüfungen veröffentlichen.

Ziel2

So wenig Ports wie möglich in das Intranet oder Internet öffnen. Lediglich einen HTTP (80)oder HTTPS Port (443) mit einer ADRESSE zum Formsserver öffnen. Das kann über einen REVERSE Proxy Server realisiert werden.

Ziel3

So viele Informationen wie möglich von den angemeldeten Anwendern sammeln um einen Angriff lokalisieren und protokollieren zu können. Bei strengem Datenschutz wenigstens für einen Tag.

Ziel4

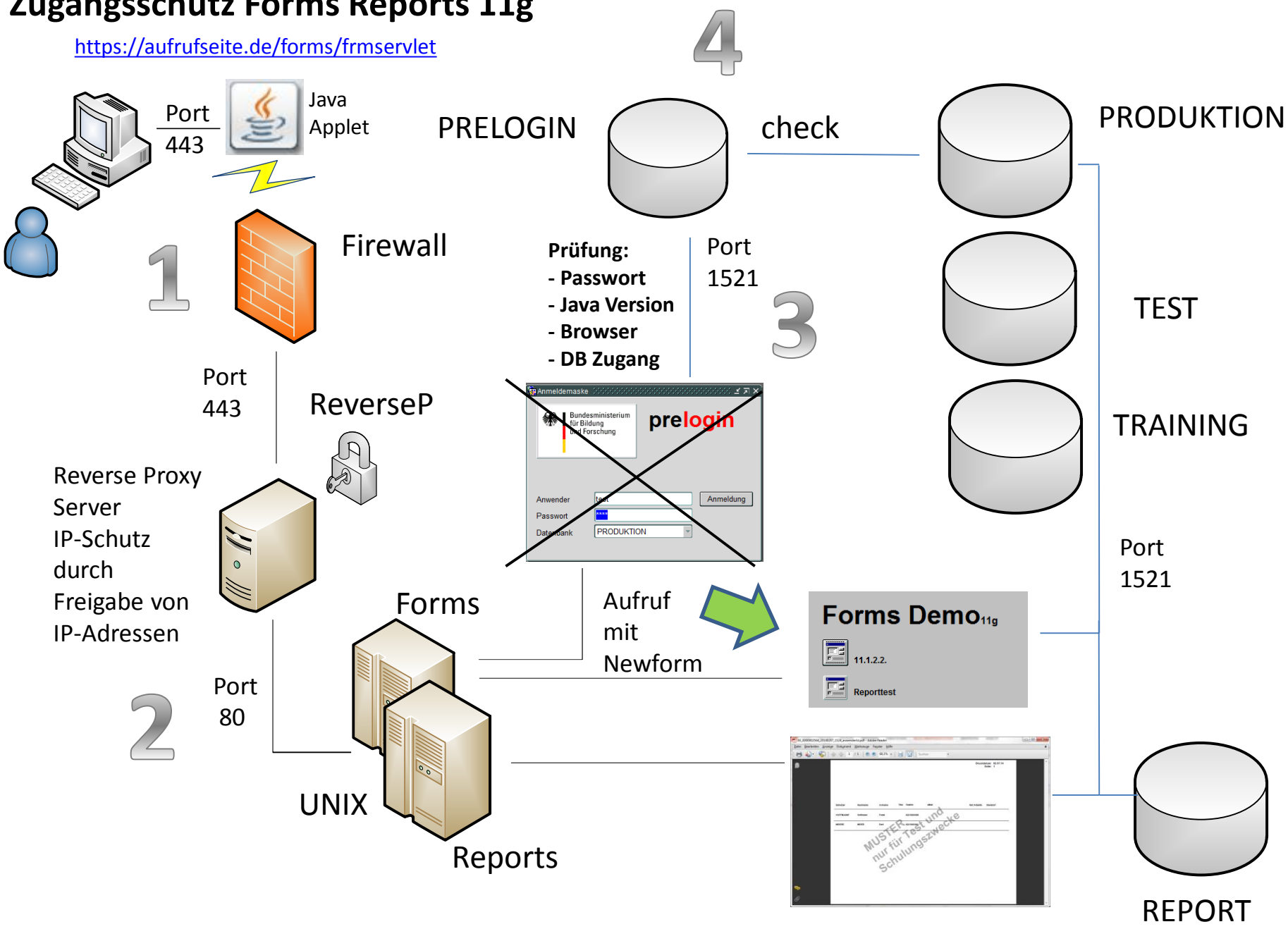
Alle sicherheitsrelevanten Prüfungen vor der Anmeldung an das Produktionssystem durchführen

Ziel5

Sicherheitsanforderungen definieren und automatisch überwachen. Möglichkeit einer Warnfunktion durch SMS oder E-MAIL an die verantwortliche Seite vorsehen.

Zugangsschutz Forms Reports 11g

https://aufrufseite.de/forms/frmservlet



Sicherheitsaspekte bei dem Betrieb von ORACLE Forms- und Reports 11g

TIPP1: formsweb.cfg restrictedURLparams=config,forms,module usw.

Nur „default“ Konfiguration verwenden und alle sicherheitsrelevanten Parameter sperren. Keine direkten Modulaufrufe zulassen.

TIPP2: report destype: BLOBDESTINATION

Reportserver unsichtbar machen. Report nach Fertigstellung als BLOB in die Datenbank schreiben und von dort runterladen – keine Aufrufe wie http://xxxx:8889/ reports/rwservlet/getjob_id… die Rückschluss auf den Reportserver und andere sicherheitsrelevante Reports geben könnten.

TIPP3: timeoutjar aus Demo als Kommunikationskanal nutzen

Um die Kommunikation zu den Modulen ermöglichen zu können muss von Zeit zu Zeit das Modul des Anwenders ein Lebenszeichen geben. Mit Nutzung des timeout.jar besteht die Möglichkeit in Zeitintervallen Applikationen zu schließen oder mit Anwendern zu kommunizieren.

TIPP4: CLIENT Informationen aus Forms an Datenbank weiterreichen

Mit “DBMS_APPLICATION_INFO.SET_CLIENT_INFO” notwendige Informationen des Clients aus dem JAVA Applet an die Datenbank weitereichen. Nur so kann der DBA die Session zurückverfolgen. Angemeldet ist stets nur eine formsweb session des Formsservers

Kontaktdaten

Frank Hoffmann, Cologne Data GmbH

www.cologne-data.de

fch@cologne-data.de