Firebird-Sicherheitsmeldung – Einordnung & Handlungsanweisungen

Don’t Panic – und immer wissen, wer weiterhelfen kann

Bevor Sie jetzt hektisch alle Firebird-Server vom Strom trennen und in den Serverraum rennen: Ruhig bleiben!

Die aktuelle Firebird-Sicherheitsmeldung klingt dramatischer, als sie für die meisten ist. Die gute Nachricht: Wenn Ihr Firebird-Server **nicht direkt übers Internet** erreichbar ist, können Sie jetzt erstmal entspannt durchatmen.

Für alle, die tatsächlich mit offenem Port unterwegs sind – es gibt schnelle, einfache Workarounds (keine galaktischen Quantencomputer nötig). Die wichtigsten Infos finden Sie auf den nächsten Seiten.

Also: die folgende Anleitung lesen, falls erforderlich, die IBExpert Firebird Support Hotline beauftragen, und zeitnah handeln – ganz ohne hyperventilieren.

1. Kurzinfo für Management

In Firebird-Versionen vor 3.0.13, 4.0.6 oder 5.0.3 gibt es eine Schwachstelle, die nur gefährlich ist, wenn der Firebird-Serverport (Standard 3050, ggf. abweichend in der `firebird.conf`) direkt aus dem Internet erreichbar ist.
Für rein interne Server besteht kein unmittelbares Risiko.
Falls Ihr Firebird-Server öffentlich erreichbar ist: Sofort den Port schließen oder per Firewall absichern, dann in Ruhe auf eine aktuelle Version updaten.

2. Technische Anweisung für Admins

Schwachstelle: DoS-Angriff ohne Login möglich, wenn der konfigurierte Firebird-Serverport von außen erreichbar ist.

Sichere Versionen:

- 3.0.13 oder neuer
- 4.0.6 oder neuer
- 5.0.3 oder neuer

A) Version prüfen

Windows:

1. Eingabeaufforderung öffnen

2. Ausführen: `gstat -z`

→ Erste Zeile z. B.: gstat Version LI-V3.0.12 (maßgeblich ist nur V3.0.12)

3. Falls gstat nicht gefunden wird: Rechtsklick auf firebird.exe → Details → Versionsnummer prüfen.

Linux:

1. Terminal öffnen

2. Ausführen: `gstat -z` oder `/opt/firebird/bin/gstat -z`

→ Versionsnummer wie oben ablesen.

B) Handlung je nach Situation

Serverport (Standard 3050 oder abweichend) im Internet offen:

1. Schneller Workaround:

- Firebird-Dienst stoppen

- In der firebird.conf den Parameter `RemoteBindAddress` aktiv setzen und auf nicht-öffentliche IP-Adressen einschränken, z. B.:

```
RemoteBindAddress = 127.0.0.1 192.168.0.123
```

(Mehrere Adressen können mit Leerzeichen getrennt werden.)

- Firebird-Dienst neu starten

2. Clients mit externem Zugriffsbedarf:

- Falls möglich, auf aktuelle Firebird-Version updaten

- Alternativ: Zugriff über VPN absichern (z. B. mit günstigen Routern wie ASUS ab ca. 20 €, die per OpenVPN den sicheren Tunnel aufbauen)

Server nur im internen Netz:

- Kein akuter Handlungsdruck

- Update in regulären Wartungsfenstern einplanen

Firebird 2.5:

- Kein Fix verfügbar – Upgrade auf unterstützte Version planen

C) Wie macht man am einfachsten ein Update

Windows (für Version ≥ 3.0):

1. Serverdienst beenden über den Taskmanager.
2. Alle `*.conf`- und `security*.fdb`-Dateien in einen separaten Pfad sichern.
3. Firebird in der neuesten Version der bereits eingesetzten Versionsnummer von firebirdsql.org als 64-Bit ZIP-Datei herunterladen und entpacken (d. h. nicht 3.0 einfach durch 5.0-Dateien ersetzen).
4. Alle Dateien aus dem ZIP mit Administratorrechten in den bisherigen Firebird-Pfad kopieren (also dort, wo die firebird.exe ist, muss danach auch die firebird.exe liegen).
5. Die in Schritt 2 gesicherten Dateien wieder über die neu kopierten Dateien kopieren.
6. Dienst wieder starten.

Wichtig: Dieses Verfahren ist wesentlich schneller, einfacher und fehlerfreier als das erneute Durchführen des Setups, weil so auch immer alle Einstellungen sowie Benutzer und Passwörter erhalten bleiben.

Linux:

1. Serverdienst beenden über Services `firebird* stop` o. ä., je nach Version.
2. Alle `*.conf`- und `security*.fdb`-Dateien in `/opt/firebird/` o. ä. je nach Version in einen separaten Pfad sichern.
3. Firebird in der neuesten Version der bereits eingesetzten Versionsnummer von firebirdsql.org als 64-Bit `tar.gz`-Datei herunterladen und entpacken (d. h. nicht 3.0 einfach durch 5.0-Dateien ersetzen).
4. Mit Root-Rechten den Installer aus der `tar.gz` starten, alle Abfragen ggf. bestätigen, SYSDBA-Passwort nach Wahl eingeben (wird im nächsten Schritt eh durch das Alte ersetzt).
5. Dienst wieder wie oben beenden.
6. Die in Schritt 2 gesicherten Dateien erneut über die neu kopierten Dateien kopieren.
7. Dienst wieder starten. Auch hier kann man kaum etwas falsch machen.

Und für alle jüngeren, die den Zusammenhang zum Don‘t Panic Logo nicht sofort zuordnen können, ein Literaturtipp:

Hier die **kurze Handlungszusammenfassung** von *Per Anhalter durch die Galaxis* (*The Hitchhiker’s Guide to the Galaxy*), erschienen vor mehr als **42** Jahren:

Arthur Dent, ein ganz normaler Brite, wacht eines Morgens auf und erfährt gleich zwei unangenehme Dinge:

1. Sein Haus soll abgerissen werden.
2. Die Erde ebenfalls — um Platz für eine Hyperraum-Umgehungsstraße zu machen.

Kurz bevor unser Planet gesprengt wird, rettet ihn sein Freund Ford Prefect, der sich als außerirdischer Journalist für den *Hitchhiker’s Guide to the Galaxy* entpuppt. Die beiden trampen per Raumschiff durchs All und geraten in eine Reihe absurder Abenteuer:

- Begegnung mit Zaphod Beeblebrox, dem zweiköpfigen, chaotischen Präsidenten der Galaxis
- Trilli(an), die einzige andere überlebende Erdbewohnerin
- Marvin, dem chronisch depressiven Roboter
- einem Planeten, auf dem Luxusgüter auf Bestellung gebaut werden
- und der Enthüllung, dass die Erde selbst ein gigantischer Supercomputer war, der die ultimative Frage zum Leben, dem Universum und dem ganzen Rest berechnen sollte (Antwort: **42**).

Das Ganze ist eine Mischung aus Science-Fiction, britischem Humor und philosophischem Nonsens – mit der zentralen Lebensweisheit: **„Don’t Panic“**.