Dirk Fox

Backdoor

Als *Backdoor* wird in einem IT-System eine geheime ‚Hintertür' bezeichnet, mit deren Kenntnis es möglich ist, von außen auf das System zuzugreifen oder Sicherheitsmerkmale auszuhebeln. Häufig werden damit auch verborgene funktionale Eigenschaften eines IT-Systems bezeichnet, die Vertrauliches preisgeben, z. B. ausgewählte Daten ohne Wissen des Systembetreibers oder -nutzers an Dritte versenden. *Backdoors* sind eine beliebte Technik von Trojanern und Bot-Netzen und werden auch von Nachrichtendiensten eingesetzt.

Typen von *Backdoors*

Backdoors setzen – abhängig vom Ziel eines Angreifers – an unterschiedlichen Stellen eines IT-Systems an:

- **Externer Zugriff**: Soll ein System bspw. über das Internet gesteuert werden, so muss die *Backdoor* z. B. nach Eingabe eines festgelegten Passcodes den vollen Systemzugriff freigeben, zum Beispiel über einen der gut 65.000 möglichen IP-*Ports* oder auch über eine via HTTP erreichbare Web-Schnittstelle. Anschließend können von außen Systembefehle ausgeführt, Daten abgezogen oder das System als Ausgangspunkt für weitere Angriffe genutzt werden.
- **Auslösen von Spezialfunktionen**: Statt eines kompletten Systemzugriffs genügt es in vielen Fällen, eine Spezialfunktion vorzusehen, die von außen z. B. durch ein bestimmtes Datenpaket ausgelöst werden kann, und die beispielsweise Daten des Systems an eine voreingestellte Adresse schickt oder verräterische Daten wie Logfiles oder Schadprogramme nach erfolgtem Angriff spurlos löscht.
- **Deaktivierung von Schutzmechanismen**: *Backdoors* werden auch verwendet, um den eigentlichen Angriff behindernde Schutzsysteme zu umgehen. Soll die *Backdoor* bspw. eine Firewall deaktivieren, genügt eine verborgene „Spezialregel", die Zugriffe von bestimmten Absenderadressen ungefiltert durchlässt, oder ein einfacher „Schalter", der z. B. die Verschlüsselung von Daten stoppt.
- **Schwächung von Schutzmechanismen**: Soll die *Backdoor* über einen langen Zeitraum genutzt werden, ist es zum Schutz vor Entdeckung häufig besser, einen Schutzmechanismus unbemerkt zu schwächen anstatt ihn zu deaktivieren. In diese Kategorie gehören *Backdoors*, die bspw. den Algorithmus zur Schlüsselerzeugung manipulieren oder Teile des verwendeten Verschlüsselungsschlüssels z. B. im Nachrichtenkopf oder in ungenutzten Bits eines Datenpakets (*Padding*) mitsenden.

Zielsystem-Manipulation

Backdoors erfordern eine gezielte Manipulation des IT-Systems. Das kann auf sehr unterschiedliche Weise erfolgen:

- **Direkte Manipulation des Zielsystems**: Wird ein Zielsystem bereits betrieben, muss es modifiziert werden. Gängige Wege sind die Verbreitung von Schadsoftware oder das direkte Aufspielen modifizierter Software. Letzteres erfordert allerdings einen physischen Zugang zum System.
- **Manipulation der Soft- oder Firmware**: Eine größere „Breitenwirkung" lässt sich erzielen, wenn es gelingt, die Manipulation bereits beim Hersteller des Systems vorzunehmen. Das stellt außerdem sicher, dass ein Software- oder Firmware-Update die *Backdoor* nicht wieder beseitigt. Nachrichtendienste bedienen sich nachweislich gerne dieser Methode – oft flankiert von Geldzahlungen an die Hersteller. Aber auch *Open Source*-Projekte können betroffen sein, wenn es gelingt, die dem Programmcode beiliegenden direkt ausführbaren Programmversionen zu manipulieren.
- **Vorgabe schwacher Verfahren**: Besonders perfide ist die Standardisierung oder Vorgabe schwacher kryptografischer Verfahren. So geschehen bereits vor 40 Jahren im Fall des von der NSA mit einer gekürzten Schlüssellänge (56 Bit statt 128) versehenen Verschlüsselungsstandards DES, bei dem früheren US-Exportverbot für Kryptoverfahren mit einer Schlüssellänge von mehr als 40 Bit, beim vom GSM-Standard verwendeten, inzwischen gebrochenen Verschlüsselungsalgorithmus A5/1 und – wahrscheinlich – bei dem 2007 vom NIST standardisierten Zufallszahlengenerator DUAL_EC_DRBG.

Schutzmaßnahmen

Die Gefährdung von IT-Systemen durch Hersteller-*Backdoors* ist insbesondere bei IT-Infrastrukturkomponenten groß, in denen wenige Anbieter aus Ländern mit offensiven Nachrichtendiensten eine marktbeherrschende Stellung genießen. Hier können redundante, sich gegenseitig kontrollierende Systeme verschiedener Anbieter und die Prüfung des Netzwerkverkehrs auf Anomalien helfen. Auch der Einsatz von Software mit anerkanntem Sicherheitszertifkat (bspw. den *Common Criteria*) oder von *Open Source*-Software kann das Risiko reduzieren.

Bei Krypto-Verfahren sollten ausschließlich standardisierte Algorithmen und interoperable Protokolle zum Einsatz kommen – Manipulationen sind deutlich schwieriger, wenn Experten die Verfahren analysieren können. Und schließlich sollten Lösungen Verdacht erregen, bei denen Daten ohne Notwendigkeit einem Anbieter im Klartext zugänglich sind.