

Zusammenfassung

Die Anwendung eines Sicherheitspatch ermöglicht die Verbesserung der Sicherheit eines Softwareprogramms.

In diesem Dokument sind die Grundsätze der Anwendung und der Funktionsweise eines Patch als Präventivmassnahme sowie Bedrohungen, denen er entgegenwirken kann, beschrieben.

Inhalt

- 1 Was ist ein Patch? →
- 2 Wer ist betroffen? →
- 3 Wie funktioniert ein Patch? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Massnahmen →



1 Was ist ein Patch?

Ein Patch ist eine Aktualisierung in Form einer Datei oder eines Softwareprogramms, welche die Korrektur von Sicherheitslücken eines Betriebssystems oder eines Softwareprogramms zum Ziel hat.

Ein Patch korrigiert in bestimmten Fällen nicht nur die Sicherheitslücke, er kann auch neue Funktionen zum Softwareprogramm oder zum Betriebssystem hinzufügen.

Die Entwickler eines Softwareprogramms oder eines Betriebssystems bieten ein Patch häufig als Download an, um eventuell vorhandene Sicherheitslücken zu schliessen.

Die Sicherheitslücken werden ursprünglich entweder von Beta-Testern oder von den Entwicklern des Softwareherstellers entdeckt oder von externen Anwendern gemeldet.

2 Wer ist betroffen?

Privatpersonen, Unternehmen und Verwaltungen, die Geräte und Software im Zusammenhang mit den neuen Informations- und Kommunikationstechnologien verwenden, sind von der Anwendung von Sicherheitspatches betroffen.

3 Wie funktioniert ein Patch?

Die Flut der von den verschiedenen Softwareprogrammen angebotenen Funktionen und Möglichkeiten steigert die Möglichkeit, dass diese Sicherheitslücken enthalten.

Diese Sicherheitslücken können in bestimmten Fällen zu böswilligen Zwecken verwendet und ausgenutzt werden, um einen unbefugten Zugang zu dem Gerät zu erhalten, auf dem die fehlerhafte Software ausgeführt wird.

Der Lebenszyklus eines Patch beginnt meistens mit der Benachrichtigung über die Sicherheitslücke durch den Hersteller

der Software bzw. über eine direkte öffentliche Bekanntmachung. In Extremfällen kann die öffentliche Bekanntmachung ohne Genehmigung durch den Softwarehersteller, abhängig von bestimmten nationalen Gesetzen und Vorschriften, als unzulässig angesehen werden. Ist dies der Fall bestätigt der Hersteller des Softwareprogramms innerhalb einer angemessenen Zeit die Existenz der Sicherheitslücke durch eine Bekanntgabe oder durch die Veröffentlichung eines Sicherheitsbulletins.

Meistens erfolgt diese Bekanntgabe gleichzeitig mit der Bereitstellung eines korrigierenden Patch, wodurch die bestehende Sicherheitslücke geschlossen wird.

Abhängig von der Betriebsreife des Herstellers sollte jeder Patch von einem Hinweis begleitet werden, welcher die folgenden Informationen enthält:

- ➔ eindeutige ID, welche das Datum und die Version des Patch umfasst,
- ➔ Informationen über die Sicherheitslücke,

- ➔ betroffene Systeme und Softwareprogramme,
- ➔ Anweisungen zur Anwendung des Patch,
- ➔ Kontaktinformationen,
- ➔ mögliche Auswirkungen und jegliche andere Art von zu berücksichtigenden Informationen.

4

Warum sollte man sich schützen?

Die Anwendung von Patches ermöglicht hauptsächlich die Vermeidung der folgenden Bedrohungen:

- ➔ Attacken
- ➔ Würmer/Viren
- ➔ Trojanisch Pferde

Nachfolgend ist ein Auszug aus einem Sicherheitsbulletin bezüglich einer Sicherheitslücke aufgeführt, das Angaben zum Patch und zu den verfügbaren Versionen enthält:



5

Vorbeugende Massnahmen

Vor der Installation eines Patch sind immer die folgenden Punkte zu berücksichtigen:

- ➔ Sind Sie vom Patch betroffen? Wenn ja, laden Sie die Ihrer Umgebung entsprechende Version herunter.
- ➔ Ermöglicht Ihnen der Patch ein zusätzliches Mass an Sicherheit im Vergleich zu möglicherweise bereits bestehenden Gegenmassnahmen wie etwa Anti-Viren-Programmen, Firewalls oder sonstigem zu erreichen?

- ➔ In gewissen Fällen und insbesondere im Fall von Unternehmen kann ein Patch selbst zu Problemen führen. Als Beispiele können die Störung der Verfügbarkeit eines Systems oder seine Instabilität genannt werden. Es wird daher empfohlen, sofern es möglich ist, den Patch in einer Testumgebung zu überprüfen, bevor er auf die Produktionsumgebung angewandt wird.