



## EDV-Hinweise der ima Updates

Früher galt als EDV-Weisheit: „Never change a runnig system“.

Heute ist dies leider nicht mehr so: Ein aus Benutzersicht „laufendes“ System läuft aus Administratorsicht leider noch lange nicht – zumindest nicht sicher: Da heute nahezu alle Systeme irgendwie mit dem Internet verbunden sind, sind sie auch den Gefahren des Netzes – vom Hacker bis zum Virus – ausgesetzt. Solche Angriffe haben nur Erfolg, weil Programme und Betriebssysteme Sicherheitslücken und Programmierfehler aufweisen. Aus diesem Grund und um neue Funktionalitäten bereitzustellen, geben nahezu alle Hersteller und Programmentwickler Updates für Ihre Programme heraus. Bei einem durchschnittlichen, aktuellen Windows-Terminalserver werden beispielsweise für das Betriebssystem und die wichtigsten Programme ca. 2-3 Updates täglich zur Verfügung gestellt.

### Folgen und Risiken von Updates

Updates haben nun zwei divergente Eigenschaften: Zum einen – positiv – beheben sie Fehler oder bringen neue Funktionalitäten. Zum anderen – negativ – ändern sie das System und die Programmumgebung für andere Programme. Ob vom Hersteller bewusst durchgeführt oder unabsichtlich geschehen: Diese Änderungen können dazu führen, dass andere Programme nicht mehr wie bisher funktionieren. Als Benutzer oder Administrator müsste man jedes Update vorher testen, also eine zur Produktiv-EDV identische Infrastruktur nehmen, das Update dort einspielen und alle im Tagesgeschäft des Unternehmens vorkommenden Funktionen testen – eine unbezahlbare Aufgabe.

### Möglichkeiten, mit Updates umzugehen

Deswegen bleiben in der Realität drei Möglichkeiten mit Updates umzugehen:

1. Es werden keine Updates eingespielt.
2. Updates werden ohne Tests in das Produktivsystem eingespielt.
3. Updates werden auf einem Testsystem kurz getestet (z. B. ob das System nach einem Update überhaupt noch läuft) und dann auf dem Produktivsystem eingespielt. Oder es wird direkt vor dem Update eine Systemsicherung durchgeführt: Falls das System nach dem Update nicht mehr funktioniert, wird auf die



Systemsicherung zurückgegriffen.

Diese drei Möglichkeiten können nun für die verschiedenen Updatearten festgelegt werden, für

- Updates, die der Hersteller als sicherheitskritisch festlegt und die nach ihrer Beschreibung auch für das Unternehmen als sehr wichtig eingestuft werden,
- Fehlerupdates, die Fehler im System beseitigen, die nicht sicherheitskritisch sind und für
- Funktionsupdates, die keine Fehler beseitigen, sondern neue Funktionalitäten bringen.

Natürlich können die verschiedenen Updatearten auch unterschiedlich behandelt werden. Es können z.B. sicherheitskritische Updates sofort und ohne Tests eingespielt werden, sonstige Updates hingegen gesammelt und nur einmal im Monat nach einem Backup des Gesamtsystems und einem einfachen Test durchgeführt werden.

Es ist Aufgabe der EDV-Verantwortlichen oder sogar der Geschäftsleitung, die Updatestrategie festzulegen, da die Risiken eines Updates durchaus erheblich sein können. So führte z. B. ein Betriebssystemupdate von Microsoft für „Windows 7“ und „Server 2008“ Anfang März 2011 dazu, dass einige Systeme nach dem Update gar nicht mehr arbeiteten.

### **Unsere Empfehlung**

Gerne beraten wir Sie bei der Wahl der passenden Updatestrategie und kalkulieren die voraussichtlich auftretenden Kosten. Unsere Empfehlung: Spielen Sie sicherheitskritische Updates direkt ein, sammeln Sie die sonstigen Backups und spielen diese zusammen z. B. am Wochenende ein. Diese Empfehlung gilt bei täglich genutzten Systemen und bei Unternehmen, bei denen ein EDV-Ausfall von weniger als einem Tag lediglich vertretbare Kosten verursacht und bei denen tägliche Backups bereit stehen, die innerhalb eines Arbeitstages wieder eingespielt werden können. Unter anderen Umständen müssen andere Regeln erstellt werden.

Haben Sie Fragen: Rufen Sie uns an unter 0234 / 51 69 90 – 0 oder senden Sie uns unter [info@imagmbh.de](mailto:info@imagmbh.de) eine kurze Mail.



ima GmbH  
Bergmannstrasse 32 / 44809 Bochum  
0234 / 516990-0  
[www.imagmbh.de](http://www.imagmbh.de)