



**BARAMUNDI CHECKLISTS** provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: [www.baramundi.com/checklists](http://www.baramundi.com/checklists)

## Always up to date – 5 tips for efficient update management

Aside from phishing attacks, unpatched system vulnerabilities are the most common method that hackers use to compromise network and data security. Even though the number of vulnerabilities increases daily, you can detect and close security gaps quickly and efficiently by using the right tools and these 5 easy-to-implement tips.

### ✓ Identify critical hardware and software

Continuously assess current risks beginning with mission-critical systems and software applications that are essential for maintaining productivity in different departments. Prioritize patch and update deployments accordingly.

### ✓ Automate!

Updating manually is time- and labor-intensive as well as prone to errors. The key is automation. Patch and update rollouts can be configured in detail and deployed. Advanced UEM solutions also provide extensive libraries of pre-tested patch packages ready to be distributed.

### ✓ Pre-deployment testing

Updates and patches can contain bugs or introduce unexpected incompatibilities. Test patches and updates on representative devices and configurations first to spot and correct problems before wider deployment. This will minimize endpoint crashes and slowdowns.

### ✓ Manage and isolate risks

Not all updates and patches can or should be deployed immediately. Apart from buggy or incompatible updates, there are legacy systems that cannot easily be changed, especially those used in real-time production environments. It may be necessary to isolate or disconnect or secure them with other measures.

### ✓ Implement deployment rings

Create rings of endpoints or logical groups of devices that will receive applicable updates at the same time in a step-wise sequence of increasingly larger rings. The rings with the most important endpoints will receive patches or updates first.

**In short: Timely and efficient update management is crucial for eliminating unpatched vulnerabilities. Identification of critical systems, testing of updates, the ring concept, security automation and balanced risk management are essential strategies that can be quickly and reliably implemented with the baramundi Management Suite.**

#### ALL ENDPOINTS UNDER CONTROL

The baramundi Management Suite empowers IT teams with the tools and flexibility needed for managing today's hybrid computing environments from any location. Learn more about Unified Endpoint Management with baramundi at [www.baramundi.com](http://www.baramundi.com).