# Work instruction: Missing Security Updates Check

This document describes the work instruction of the monthly check “Missing Security Updates Check”. The goal of this work instruction is to check if all available security updates and service packs for all used Microsoft technologies have been deployed to all servers in the environment.

# Involved servers

|  |  |  |
| --- | --- | --- |
| Acceptance | Production | Disaster Recovery |
|  |  |  |

# Steps

|  |  |
| --- | --- |
| Step | Screenshot |
| **Important: The Microsoft Security Baseline Analyzer (MBSA) is used for this check. This tool needs to be installed on the Admin server.**  **The Windows Firewall on all servers has to be configured as specified in** [**https://technet.microsoft.com/en-us/security/cc184922.aspx**](https://technet.microsoft.com/en-us/security/cc184922.aspx) **- Section “How can I scan a computer that is protected by a firewall?”** | |
| Step 1:  Download the file wsusscn2.cab and copy it to the Admin server | http://go.microsoft.com/fwlink/?LinkId=76054 |
| Step 2:  Open a RDP session to the Admin server |  |
| Step 3:  Copy the file wsusscn2.cab to C:\Scripts\MBSAScan |  |
| Step 4:  Browse to C:\Scripts\MBSAScan and execute “RunMBSAScan.cmd” |  |
| Step 4:  The script generates an output file in which all missing updates are listed. Check if this file contains missing updates and check if these are mentioned in the “Allowed Exceptions” list.  If this isn’t the case: Create an incident to have this investigated. |  |
| Step 5:  Record your findings in the “Registration list Periodic Checks” |  |

# Automatic check

This check is part of the Periodic Checks script, which means the above checks do not have to be performed manually. Analysis will take place by reviewing the generated e-mail and taking actions if issues are reported.

# resolution

Determine if all missing updates aren’t installed on purpose or if this is a mistake, then take the following actions:

* Not installed on purpose:
  + When checking manually: Add the KB article to the “Allowed Exceptions” list.
  + When using the script: Add the KB article and reason to the file config\patchexclusions.txt, making sure the patch is excluded the next time.
* Mistake: Create a change to have this corrected.