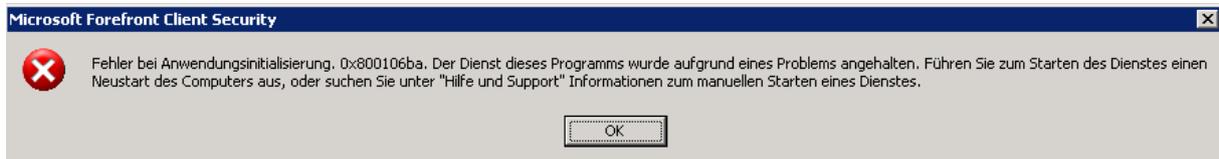
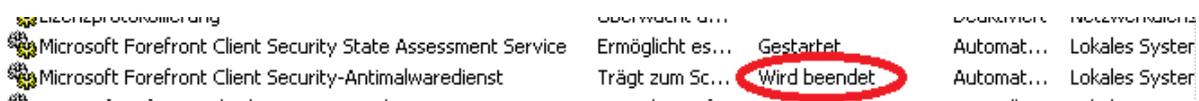


Forefront Client Security Probleme

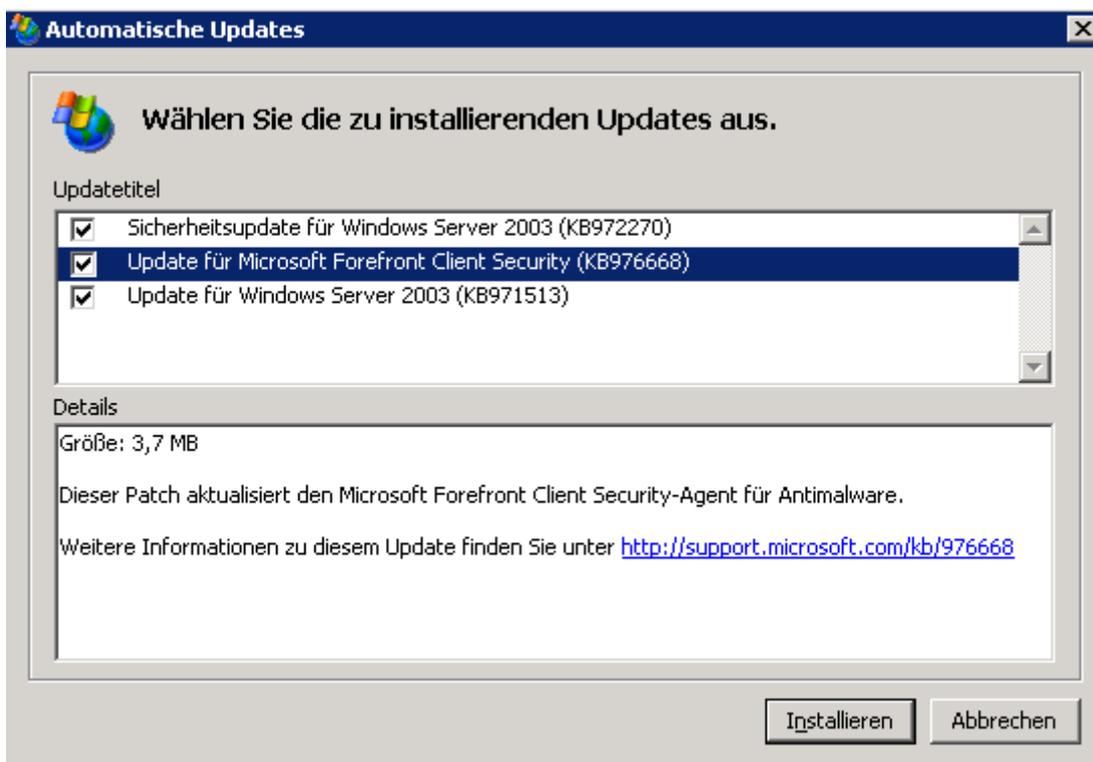
Auf einem Windows Server 2003 R2 SP2 Fileserver laeuft FCS nicht mehr rund.
Folgendes Problem tritt auf:



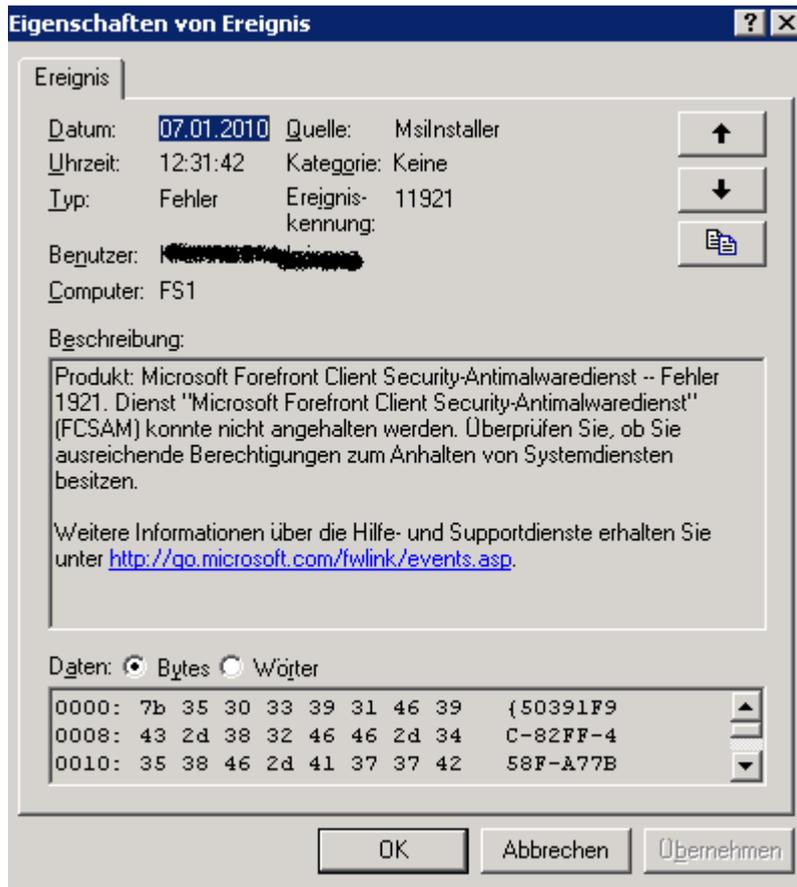
Bei dem Versuch des Updates faehrt sich der Dienst ins Nirvana und laesst sich auch mit SC.EXE nicht mehr steuern. Einzig ein Reboot hilft, doch danach taucht das Problem erneut auf.



Um dieses Update handelt es sich:



Meldung in der Ereignisanzeige:



Meldung im FCS Log:

```

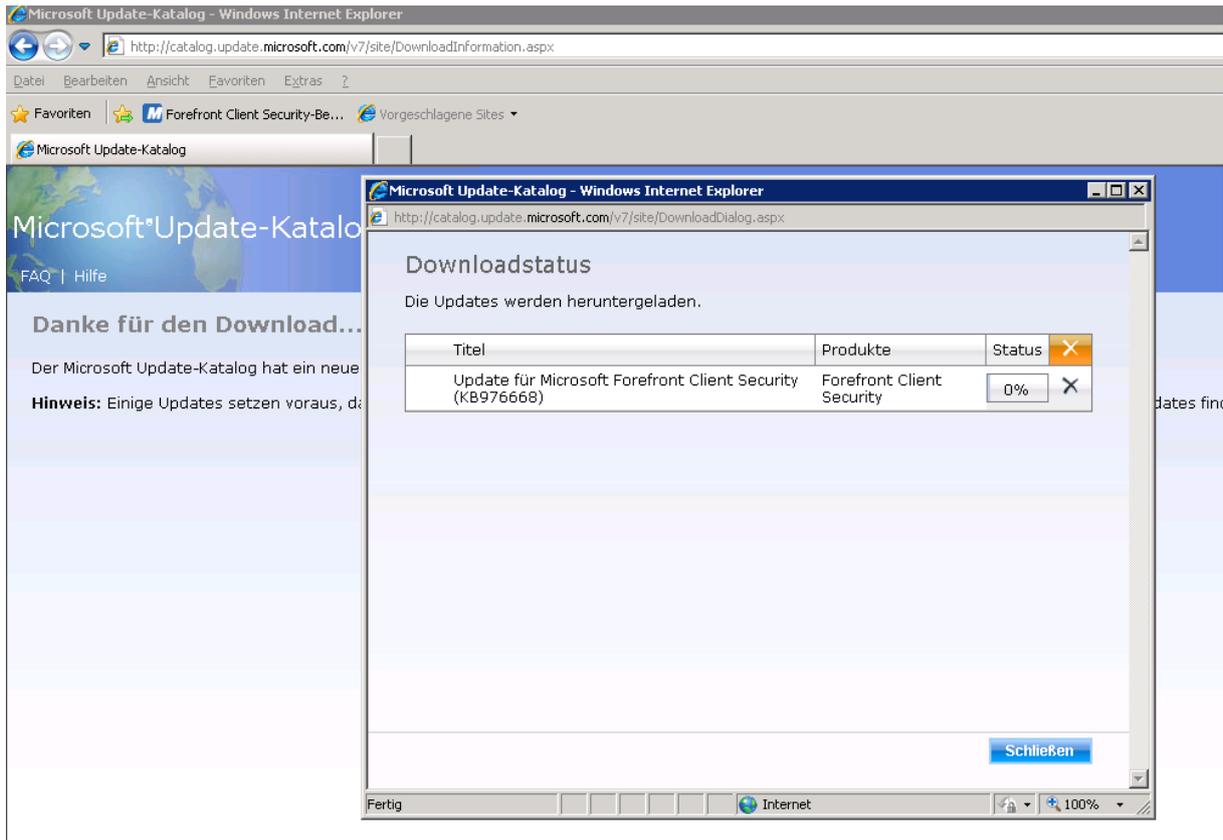
WSI (S) (18:38) [07:42:04:980]: Note: 1: 1402 2:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\C9F19305FF28F8547AB7ED7F426E41D0\Transforms 3: 2
WSI (S) (18:38) [07:42:04:980]: Executing op: End(Checksum=0, ProgressTotalHDword=0, ProgressTotalLdword=0)
WSI (S) (18:38) [07:42:04:980]: Error in rollback skipped. Return: 5
WSI (S) (18:38) [07:42:04:995]: No System Restore sequence number for this installation.
WSI (S) (18:38) [07:42:04:995]: Unlocking Server
WSI (S) (18:38) [07:42:05:074]: PROPERTY CHANGE: Deleting UpdateStarted property. Its current value is '1'.
Aktion beendet um 07:42:05: INSTALL. Rückgabewert 3.
WSI (S) (18:CC) [07:42:05:089]: Note: 1: 2205 2: 3: Control
Aktion beendet um 07:42:05: RemoveExistingProducts. Rückgabewert 3.
Aktion beendet um 07:42:05: INSTALL. Rückgabewert 3.
WSI (S) (18:CC) [07:42:05:089]: Note: 1: 1708
WSI (S) (18:CC) [07:42:05:089]: Produkt: Microsoft Forefront Client Security-Antimalwaredienst -- Die Installation ist fehlgeschlagen.

WSI (S) (18:CC) [07:42:05:089]: Das Produkt wurde durch windows Installer installiert. Produktname: Microsoft Forefront Client Security-Antimalwaredienst. F
1.5.1973.0. Produktsprache: 1031. Erfolg- bzw. Fehlerstatus der Installation: 1603.

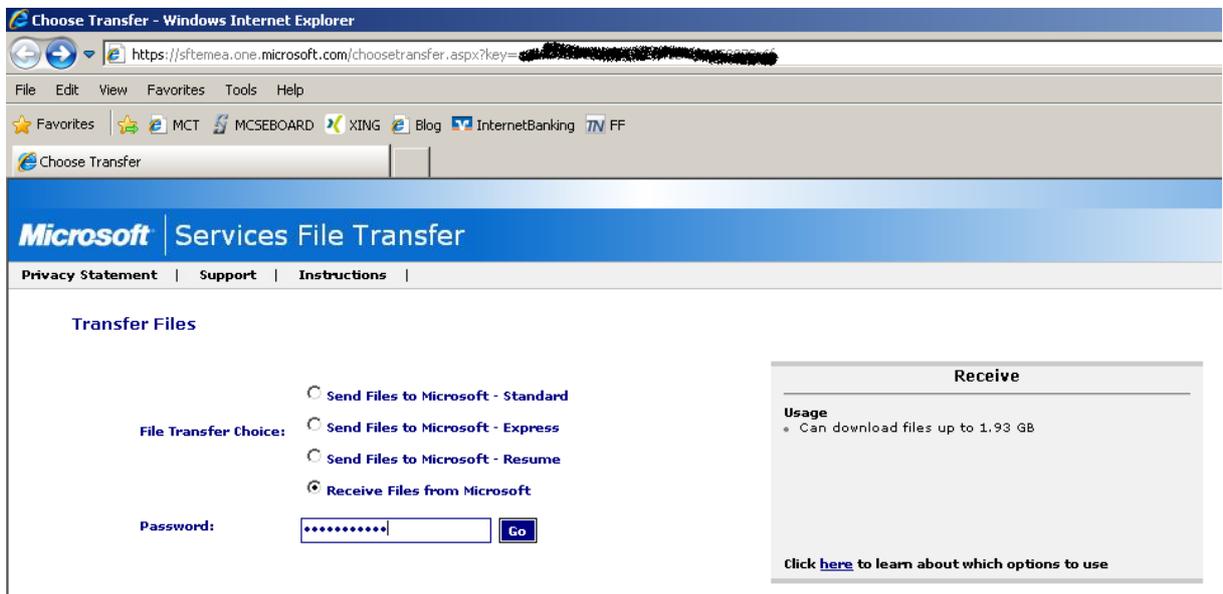
WSI (S) (18:CC) [07:42:05:089]: Cleaning up uninstalled install packages, if any exist
WSI (S) (18:CC) [07:42:05:089]: MainEngineThread is returning 1603
WSI (S) (18:A8) [07:42:05:199]: No System Restore sequence number for this installation.
=== Protokollierung beendet: 08.01.2010 07:42:05 ===
WSI (S) (18:A8) [07:42:05:199]: user policy value 'disablerollback' is 0
WSI (S) (18:A8) [07:42:05:199]: Machine policy value 'disablerollback' is 0
WSI (S) (18:A8) [07:42:05:199]: Incrementing counter to disable shutdown. Counter after increment: 0
WSI (S) (18:A8) [07:42:05:199]: Note: 1: 1402 2: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts 3: 2
WSI (S) (18:A8) [07:42:05:199]: Note: 1: 1402 2: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts 3: 2
WSI (S) (18:A8) [07:42:05:199]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied. Counter after decrement: -1
WSI (S) (18:A8) [07:42:05:199]: Restoring environment variables
WSI (C) (8c:48) [07:42:05:199]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied. Counter after decrement: -1
WSI (C) (8c:48) [07:42:05:199]: MainEngineThread is returning 1603
=== Verbose logging stopped: 08.01.2010 07:42:05 ===

```

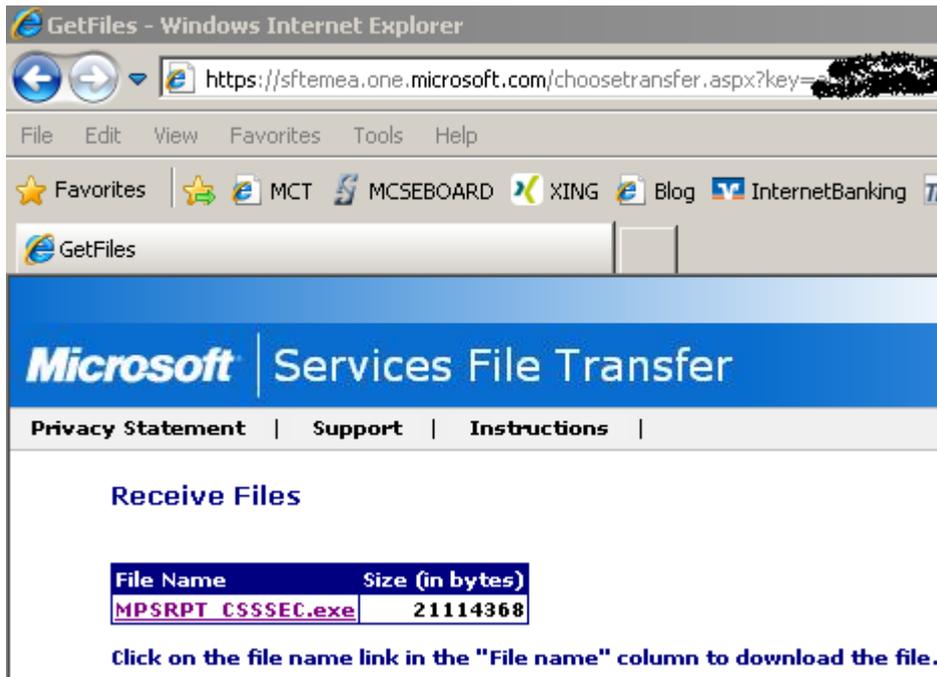
Auch eine manuelle Installation des FCS Updates hilft nicht:



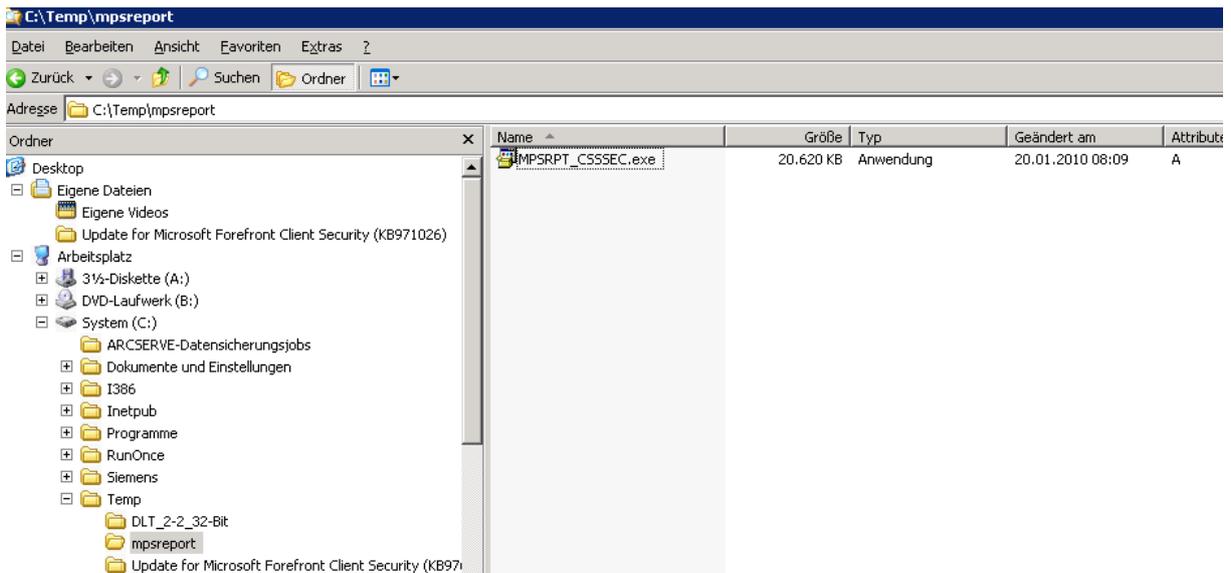
Nach dem telefonischen Erstkontakt mit Microsoft und der Problembeschreibung kam eine e-mail von dem Forefront Security Engineer zurueck, mit einem Link zum Download des MPSReport Tools.



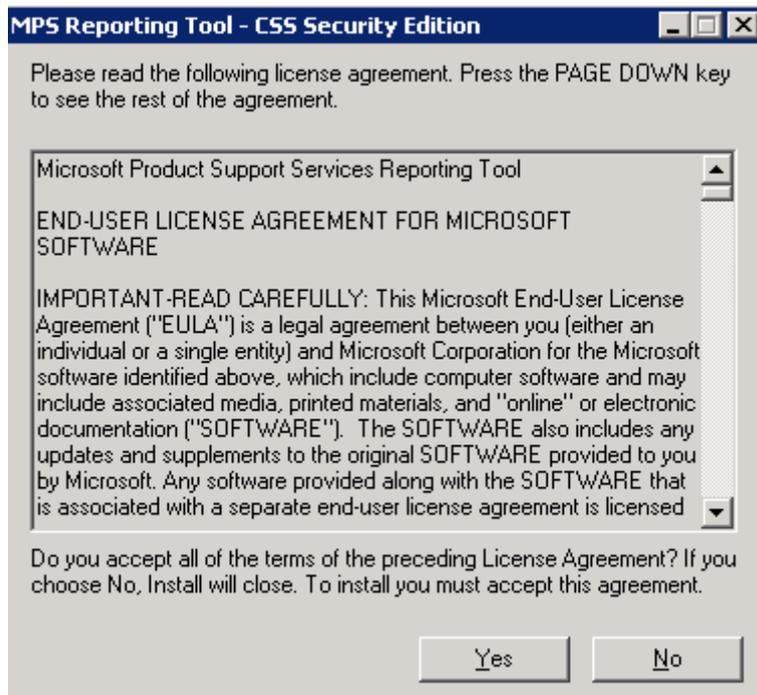
Download des Tools



Download complete



Programm Installation



Es geht los:

```
C:\> MPS Reporting Tool (CSS Security Edition) Version: 2010.01.13 (DumpMSInfo.cmd)
=====
MPSReports:      CSS Security Edition
Version:         2010.01.13
Build Date:      01/13/2010
Computername:
Current User:
Output Dir:      C:\WINDOWS\MPSreports\CSSSEC\Bin
Start Time:      20.01.2010  8:41:29,83
Microsoft Windows [Version 5.2.3790]
=====

Include the MSINF032 report? <defaults to Y in 15 seconds> [Y,N]?Y
20.01.2010  8:41:44,94 : Running MSINF032 Data Collection

*****
NOTE: MSINF032.EXE may take several minutes to complete.
      If this portion of the data collection hangs,
      please close this DOS window, then run MPSreports
      again and choose N (No) to the option to run MSINF032.
*****
20.01.2010  8:41:44,94 : MSINF032.EXE: Creating Winmsd (<.nfo>) Report
-
```

Es dauert etwas ☺

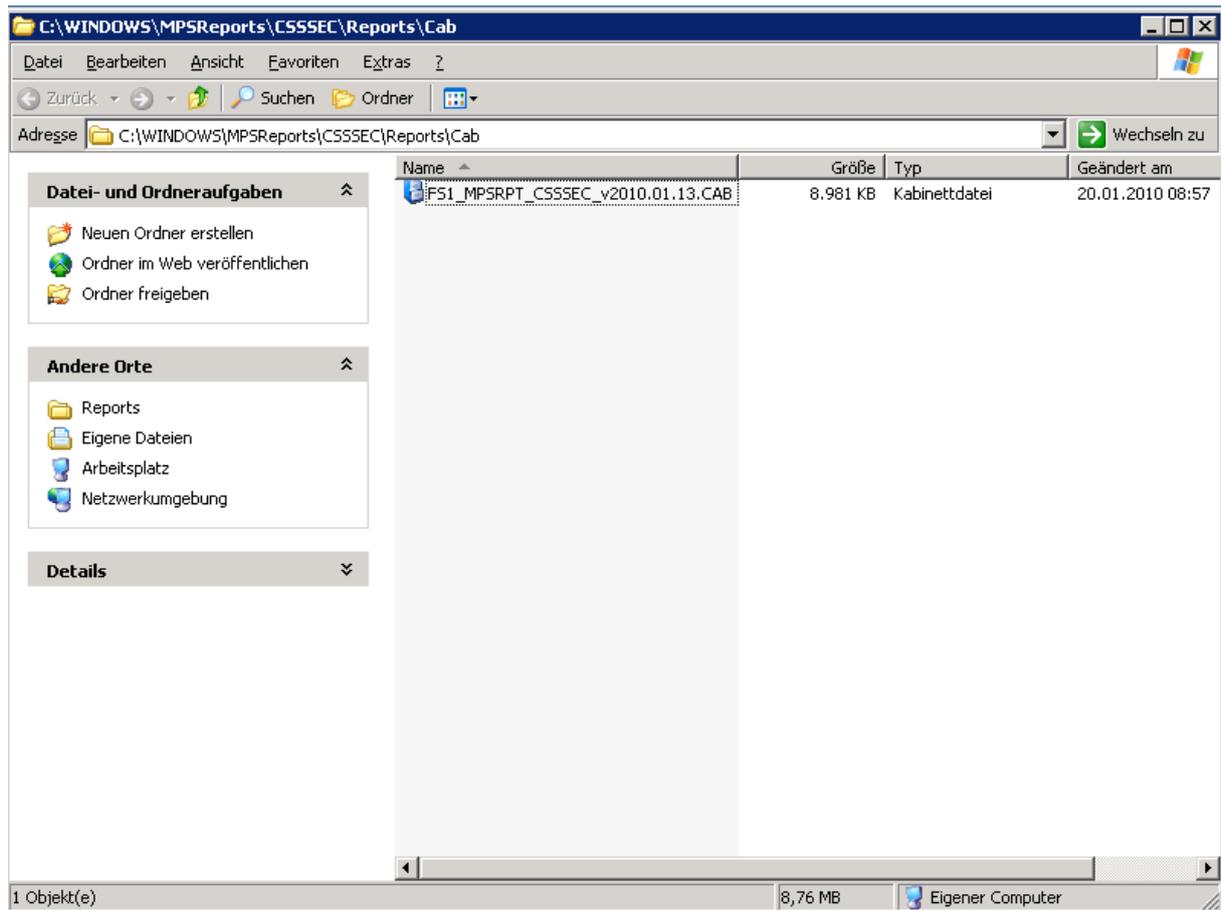
Daten ohne Ende. Ein Nacktscanner ist nichts dagegen ☺

```

MPS Reporting Tool (CSS Security Edition) Version: 2010.01.13 (AllPlatforms.CMD)
20.01.2010 8:46:27.11 : Saved: HKEY_Internet_Settings.txt
20.01.2010 8:46:27.11 : REG.EXE: Gathering Internet Explorer Keys from Registry
20.01.2010 8:46:28.00 : Saved: HKEY_Internet_Explorer.txt
20.01.2010 8:46:28.00 : Gathering Directory Tree: Temporary Internet Files
20.01.2010 8:46:28.02 : Saved: Dir_TempInternet.txt
20.01.2010 8:46:28.02 : PROXYCFG.EXE: Gathering WinHTTP Proxy Configuration
20.01.2010 8:46:30.81 : Saved: ProxyCFG_WinHTTP.txt
20.01.2010 8:46:30.81 : BITSADMIN.EXE: Gathering the BITSAdmin.txt log
Das System kann den angegebenen Pfad nicht finden.
20.01.2010 8:46:31.75 : Saved: BitsAdmin.txt
20.01.2010 8:46:31.75 : Gathering WPAD.dat Information
20.01.2010 8:46:33.17 : Saved: WPAD.DAT files for various profiles
20.01.2010 8:46:33.19 : Downloading AutoConfigURL
20.01.2010 8:46:33.42 : Saved: AutoConfigURL.txt
20.01.2010 8:46:33.42 : Gathering PACFile Information
20.01.2010 8:46:34.31 : Saved: PACFile files for various profiles
20.01.2010 8:46:34.31 : Gathering Winsock/LSP Information
20.01.2010 8:46:35.94 : Saved: Winsock.txt
20.01.2010 8:46:35.94 : Gathering Netsh NAP Information
20.01.2010 8:46:36.47 : Directory Listing of Catroot Folders
20.01.2010 8:46:36.47 : Saved: Dir_Catroot.txt
20.01.2010 8:46:36.47 : Directory Listing of Drivers Folder
20.01.2010 8:46:36.49 : Saved: Dir_Drivers.txt
20.01.2010 8:46:36.49 : Directory Listing of Internet Explorer Folder
20.01.2010 8:46:36.53 : Directory Listing of Downloaded Program Files Folder
20.01.2010 8:46:36.55 : Saved: Dir_InternetExplorer.txt
20.01.2010 8:46:36.55 : CSCSCRIPT.EXE ROIscan.vbs: Inventory of Installed Office / MSI Components
20.01.2010 8:46:41.05 : Saved: OfficeInventory.txt
20.01.2010 8:46:41.05 : Gathering Directory Tree: C:\WINDOWS\SoftwareDistribution
20.01.2010 8:46:42.53 : Gathering Directory Tree: C:\WINDOWS\System32\softwaredistribution
20.01.2010 8:46:42.60 : Saved: Dir_SoftwareDistribution.txt
20.01.2010 8:46:42.60 : Certutil and REG.EXE: Gathering System Certificates information
20.01.2010 8:46:44.88 : Saved: Certificates_Info.txt
20.01.2010 8:46:44.88 : REG.EXE: Gathering HKLM\SYSTEM\CurrentControlSet\Services information
20.01.2010 8:46:48.61 : REG.EXE: Gathering HKLM\SYSTEM\CurrentControlSet\Services Hive
20.01.2010 8:46:48.92 : Saved: Services_Key.txt and Services_Key.hiv
20.01.2010 8:46:48.92 : REG.EXE: Gathering HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
20.01.2010 8:46:48.94 : Saved: SessionManager_Key.txt
20.01.2010 8:46:48.94 : REG.EXE: Gathering HKLM\Software\Microsoft\OLE
20.01.2010 8:46:48.99 : Saved: HKLM_OLE_Key.txt
20.01.2010 8:46:48.99 : REG.EXE: Gathering WindowsUpdate info from Registry
20.01.2010 8:46:49.00 : Saved: HKLM_WindowsUpdate.txt
20.01.2010 8:46:49.02 : REG.EXE: Gathering HKLM HKCU HKU - WindowsUpdate Policy info from Registry
20.01.2010 8:46:49.06 : Saved: HK_Policies_WindowsUpdate.txt
20.01.2010 8:46:49.06 : REG.EXE: Gathering Current User Policy info from Registry
20.01.2010 8:46:49.08 : Saved: HKCU_Policies.txt
20.01.2010 8:46:49.08 : CHECKSYM.EXE: Saving module info for running processes
20.01.2010 8:46:58.64 : Saved: Process.txt and Process.csv
20.01.2010 8:46:58.64 : CHECKSYM.EXE: Gathering File Information for C:\WINDOWS\System32\*.DLL

```

Nach ca. 15 Minuten war der Output da



Das ist alles drin:

```

Administrator: Command Prompt
20.01.2010 08:59 <DIR> .
20.01.2010 08:59 <DIR> ..
20.01.2010 08:59 <DIR> ClientSetup
20.01.2010 08:49 118 FS1_Anonymous_Info.txt
20.01.2010 08:45 4.250 FS1_AUdcom.txt
20.01.2010 08:46 182 FS1_AutoConfigURL.txt
20.01.2010 08:44 303.063 FS1_Autoruns.txt
20.01.2010 08:46 2.084 FS1_BitsAdmin.txt
20.01.2010 08:49 374.790 FS1_CacIs_Client.txt
20.01.2010 08:46 59.349 FS1_Certificates_Info.txt
20.01.2010 08:45 414 FS1_ClassRegistration.txt
20.01.2010 08:44 1.836 FS1_clientDependDiag.log
10.12.2009 17:11 252.777 FS1_comsetup.log
20.01.2010 08:45 540 FS1_CSDVersion.txt
20.01.2010 08:57 3.625 FS1_Descriptors.txt
20.01.2010 08:45 1.354 FS1_DIFx.txt
20.01.2010 08:46 9.182 FS1_Dir_Catroot.txt
20.01.2010 08:46 10.004 FS1_Dir_Drivers.txt
20.01.2010 08:46 5.497 FS1_Dir_InternetExplorer.txt
20.01.2010 08:46 291.918 FS1_Dir_SoftwareDistribution.txt
20.01.2010 08:46 104 FS1_Dir_TempInternet.txt
20.01.2010 08:46 1.227 FS1_Diskquota.txt
20.01.2010 08:49 5.031 FS1_Dmdiag.txt
20.01.2010 08:45 2.339 FS1_Env.txt
20.01.2010 08:57 1.579.240 FS1_EUT_Application.csv
20.01.2010 08:57 1.857.948 FS1_EUT_Application.evt
20.01.2010 08:52 1.890.157 FS1_EUT_Application.txt
20.01.2010 08:57 88 FS1_EUT_Internet_Explorer.evt
20.01.2010 08:57 16.776.992 FS1_EUT_Security.evt
20.01.2010 08:55 25.052.813 FS1_EUT_Security.txt
20.01.2010 08:57 11.999.398 FS1_EUT_System.csv
20.01.2010 08:57 12.634.456 FS1_EUT_System.evt
20.01.2010 08:52 12.918.342 FS1_EUT_System.txt
20.01.2010 08:57 88 FS1_EUT_Windows_PowerShell.evt
20.01.2010 08:41 20.770 FS1_FCS_PATHS.LOG
20.01.2010 08:45 11.951 FS1_Fileversions.txt
20.01.2010 08:44 430 FS1_FilterManager.txt
20.01.2010 08:43 625 FS1_FSS_Regkeys.txt
20.01.2010 08:49 50.272 FS1_GPResult.txt
20.01.2010 08:44 899.245 FS1_Handle.txt
20.01.2010 08:44 860 FS1_hardware.log
31.07.2009 15:18 285.030 FS1_hcupdate.log
20.01.2010 08:46 282 FS1_HKCU_Policies.txt
20.01.2010 08:46 228.939 FS1_HKEY_Internet_Explorer.txt
20.01.2010 08:46 259.574 FS1_HKEY_Internet_Settings.txt
20.01.2010 08:45 3.922 FS1_HKLM_ClientSecurity.txt
20.01.2010 08:45 1.436.212 FS1_HKLM_Installer.txt
20.01.2010 08:45 5.853 FS1_HKLM_MOM.txt
20.01.2010 08:46 2.601 FS1_HKLM_OLE_Key.txt
20.01.2010 08:45 3.375 FS1_HKLM_Policies_ClientSecurity.txt
20.01.2010 08:45 5.387 FS1_HKLM_Setup.txt
20.01.2010 08:45 145.624 FS1_HKLM_Uninstall.txt
20.01.2010 08:45 352.479 FS1_HKLM_Updates.txt
20.01.2010 08:46 3.627 FS1_HKLM_WindowsUpdate.txt
20.01.2010 08:46 1.394 FS1_HK_Policies_WindowsUpdate.txt
18.04.2007 14:38 837 FS1_hosts.txt
20.01.2010 08:45 67.322 FS1_Hotfix.txt
10.12.2009 17:11 1.333.084 FS1_IIS6.LOG
20.01.2010 08:49 3.294 FS1_IISInfo.txt
20.01.2010 08:49 132 FS1_IISLogsLocation.txt
20.01.2010 08:57 44 FS1_Isainfo.txt
21.02.2003 20:40 226.636 FS1_Machine.config.txt
20.01.2010 08:49 7.968 FS1_mbsa2.txt
20.01.2010 08:44 596 FS1_MOMService.txt
20.01.2010 08:57 9.195.641 FS1_MPSRPT_CSSSEC_v2010.01.13.CAB
07.01.2010 12:32 2.646 FS1_mrt.log
20.01.2010 08:43 1.264.366 FS1_MSInfo32.nfo
20.01.2010 08:46 204 FS1_Netsh_NAP.txt
20.01.2010 08:57 12.247 FS1_Netstat.txt

```

Und noch viel mehr

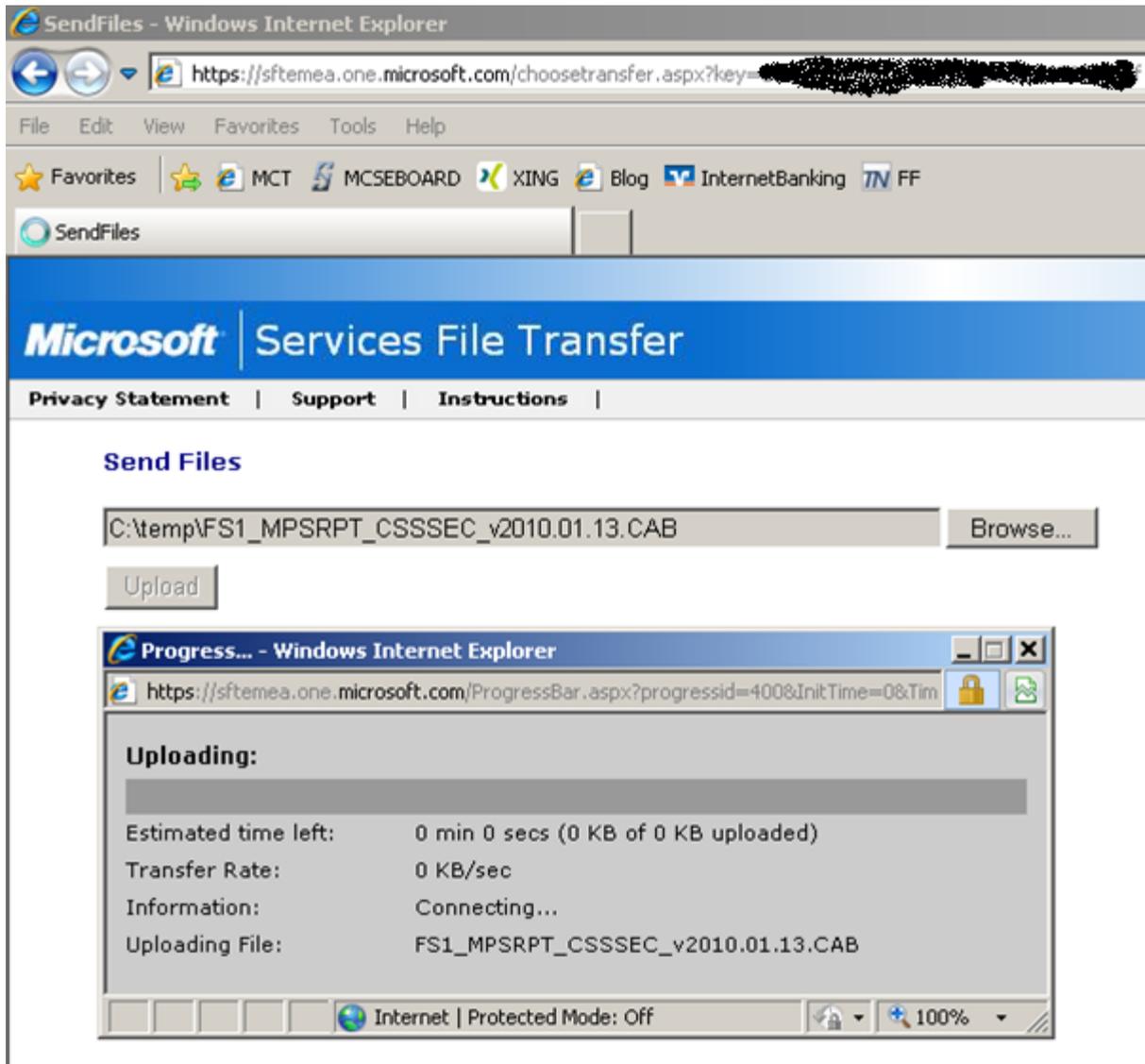
```

Administrator: Command Prompt
20.01.2010 08:45          67.322 FS1_Hotfix.txt
10.12.2009 17:11      1.333.084 FS1_IIS6.LOG
20.01.2010 08:49          3.294 FS1_IISInfo.txt
20.01.2010 08:49          132 FS1_IISLogsLocation.txt
20.01.2010 08:57          44 FS1_Isainfo.txt
21.02.2003 20:40      226.636 FS1_Machine.config.txt
20.01.2010 08:49          7.968 FS1_mbsa2.txt
20.01.2010 08:44          596 FS1_MOMService.txt
20.01.2010 08:57      9.195.641 FS1_MPSRPT_CSSSEC_v2010.01.13.CAB
07.01.2010 12:32          2.646 FS1_mrt.log
20.01.2010 08:43      1.264.366 FS1_MSInfo32.nfo
20.01.2010 08:46          204 FS1_Netsh_NAP.txt
20.01.2010 08:57          12.247 FS1_Netstat.txt
20.01.2010 08:45          9.131 FS1_NI.txt
20.01.2010 08:46      125.594 FS1_OfficeInventory.txt
20.01.2010 08:46          43 FS1_PACFile_Administrator.txt
20.01.2010 08:46          42 FS1_PACFile_DefaultUser.txt
20.01.2010 08:46          42 FS1_PACFile_LocalService.txt
20.01.2010 08:46          44 FS1_PACFile_NetworkService.txt
20.01.2010 08:46          38 FS1_PACFile_User.txt
20.01.2010 08:45          733 FS1_PID.txt
20.01.2010 08:47      1.227.637 FS1_Process.csv
20.01.2010 08:47      2.141.256 FS1_Process.txt
20.01.2010 08:46          494 FS1_ProxyCFG_WinHTTP.txt
20.01.2010 08:45          148 FS1_QFECheck.txt
20.01.2010 08:45      1.068.806 FS1_RegACLs.txt
20.01.2010 08:29      922.680 FS1_ReportingEvents.log
20.01.2010 08:45          16.281 FS1_SchedLgU.Txt
20.01.2010 08:57          5.522 FS1_ScheduledTasks.txt
20.01.2010 08:45      128.093 FS1_SC_Services_Output.txt
20.01.2010 08:44          38 FS1_SecurityCenter.log
20.01.2010 08:49          1.023 FS1_SensLogn.txt
20.01.2010 08:46      696.320 FS1_Services_Key.hiv
20.01.2010 08:46      546.256 FS1_Services_Key.txt
20.01.2010 08:46          1.889 FS1_SessionManager_Key.txt
13.01.2005 16:43      274.193 FS1_setupact.log
07.01.2010 12:25      818.543 FS1_Setupapi.log
13.01.2005 16:43      807.058 FS1_setuplog.txt
20.01.2010 08:45          19.845 FS1_SRUInfo.txt
20.08.2009 15:46      977.768 FS1_svcpack.log
20.01.2010 08:45          5.895 FS1_SvcRegistration.txt
20.01.2010 08:47      755.773 FS1_System32_DLL.csv
20.01.2010 08:47      1.405.295 FS1_System32_DLL.txt
20.01.2010 08:47      119.513 FS1_System32_EXE.csv
20.01.2010 08:47      228.372 FS1_System32_EXE.txt
10.12.2009 17:11      154.040 FS1_updspapi(SPx).log
20.01.2010 08:45          7.243 FS1_UserRights.txt
20.01.2010 08:45          10.183 FS1_WGADiag.txt
20.01.2010 08:39      1.115.137 FS1_Windowsupdate.log
20.01.2010 08:46          36.467 FS1_Winsock.txt
13.11.2009 14:07          6.182 FS1_wmsetup.log
13.11.2009 14:08          378 FS1_wmsetup10.log
20.01.2010 08:46          44 FS1_WPAD.DAT_Administrator.txt
20.01.2010 08:46          43 FS1_WPAD.DAT_DefaultUser.txt
20.01.2010 08:46          43 FS1_WPAD.DAT_LocalService.txt
20.01.2010 08:46          45 FS1_WPAD.DAT_NetworkService.txt
20.01.2010 08:46          39 FS1_WPAD.DAT_User.txt
20.01.2010 08:49          70 FS1_WSUS_BasicInfo.txt
20.01.2010 08:49          191 FS1_WWWRoot_Udirs.txt
20.01.2010 08:57          25.000 FS1_~PROGRESS.LOG
20.01.2010 08:59      <DIR> HotfixInstallLogs
20.01.2010 08:59      <DIR> IISLogFiles
20.01.2010 08:59      <DIR> MOM_LogFiles
20.01.2010 08:59      <DIR> SSA_Results
      113 File(s)      115.532.145 bytes
      7 Dir(s)      127.615.152.128 bytes free

C:\temp>

```

Upload des MPSReport Files



Finish not swedish

Upload - Windows Internet Explorer

https://sftemea.one.microsoft.com/Upload.uplx?progressid=400

File Edit View Favorites Tools Help

★ Favorites | MCT | MCSEBOARD | XING | Blog | InternetBanking | FF

Upload

Microsoft | Services File Transfer

[Privacy Statement](#) | [Support](#) | [Instructions](#) |

The file, FS1_MPSRPT_CSSSEC_v2010.01.13.CAB, was uploaded successfully.

To send another file click on the Send button.