Windows 7 und Windows XP im Netz weiterbetreiben (gilt nur für Maschinensteuerungen)

In der vorliegenden Anleitung wird beschrieben, auf welche Weise Sie PCs, die zwingenderweise noch mit Windows 7 oder älter weiterbetrieben werden müssen, sicherer konfigurieren können. Sollten Sie einzelne, unten beschriebene Schritte nicht befolgen können, so überspringen Sie sie. **Versuchen Sie aber trotzdem, möglichst viele der unten genannten Maßnahmen umzusetzen**. Langfristig wird so das Gesamtrisiko durch Malware reduziert.

Wichtiger Hinweis

Die vorliegende Anleitung kann eine Migration auf ein sicheres und supportetes System nicht ersetzen. Sie ist als Hilfsmittel für einen sonst nicht vermeidbaren Weiterbetrieb von inhärent unsicheren Systemen zu verstehen. Ein verantwortungsvolles Nutzerverhalten wird zwingend vorausgesetzt.

Der Verfasser, das ZIM und die HHU haften nicht für entstehende Schäden.

In besonderen Fällen kann es erforderlich sein, nicht mehr unterstützte Windows-Versionen (insbesondere Windows 7 und Windows XP) auch über das Supportende hinaus weiterzubetreiben. Durch richtige Einstellungen und **vor allem richtiges Nutzungsverhalten** lässt sich auch für diese Geräte nach Abwägung von Aufwand und Nutzen nach derzeitigem Stand (Januar 2020) ein *ausreichendes* Sicherheitsniveau erreichen.

Für **Windows 7** endete der Support am 14. Januar 2020. Danach liefert Microsoft nur noch kostenpflichtige Updates, die in Deutschland über software-express.de bezogen werden können. Die Kosten belaufen sich auf zur Zeit (25.12.2019) 61,53 Euro netto pro Gerät. Ein Rahmenvertrag wurde nicht geschlossen.
Sollte die mit Windows 7 betriebene Anlage Windows 10 nicht unterstützen, so ist es empfehlenswert zu prüfen, ob sie sich auf Windows 8.1 upgraden lässt. Der Support für Windows 8.1 endet erst im Januar 2023.

Für **Windows XP** endete der Support am 08. April 2014 (am 09. April 2019 ist auch der Support für Kassensysteme ausgelaufen, der durch einige Nutzer inoffiziell für Sicherheitsupdates von regulären Windows XP-Maschinen genutzt wurde).

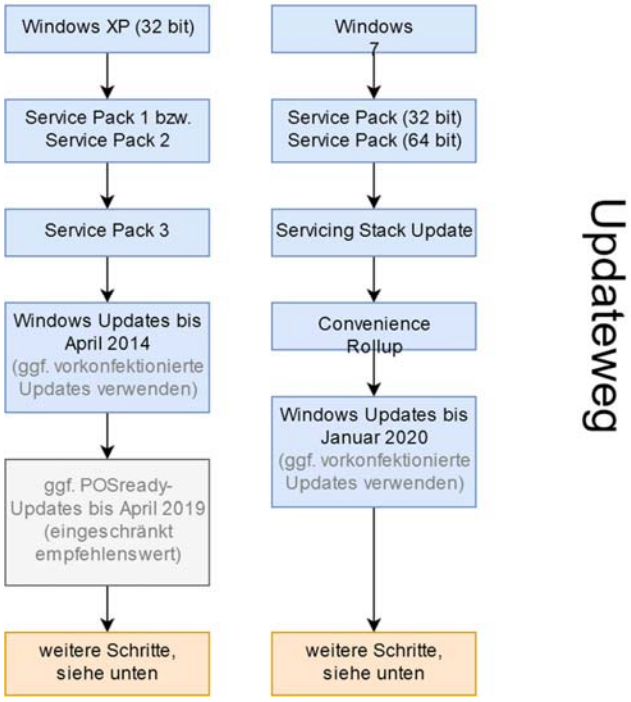
Das wichtigste Prinzip ist: nutzen Sie die anfällige Maschine so wenig wie möglich und konfigurieren Sie sie so sicher wie möglich!

Maßnahme A: Systemupdates

Es wird dringend empfohlen, dass die weiterzubetreibende Maschine voll durchgepatcht ist.

Es wird zwingend vorausgesetzt, dass die Maschine **hinter der Institutsfirewall betrieben** wird.

Hinweis! Wenn möglich, sind Windows-Updates über den offiziellen Microsoft Update-Katalog zu beziehen
Sollten Updates nicht verfügbar sein, kontaktieren Sie bitte das ZIM.



Maßnahme B: Richtige Software und Updates

1. Allgemein

Im nächsten Schritt muss die auf der betroffenen Maschine installierte Software gepflegt werden. Dazu gehört die Deinstallation unnötiger und das möglichst weitgehende Updaten notwendiger Software.

2. Browser

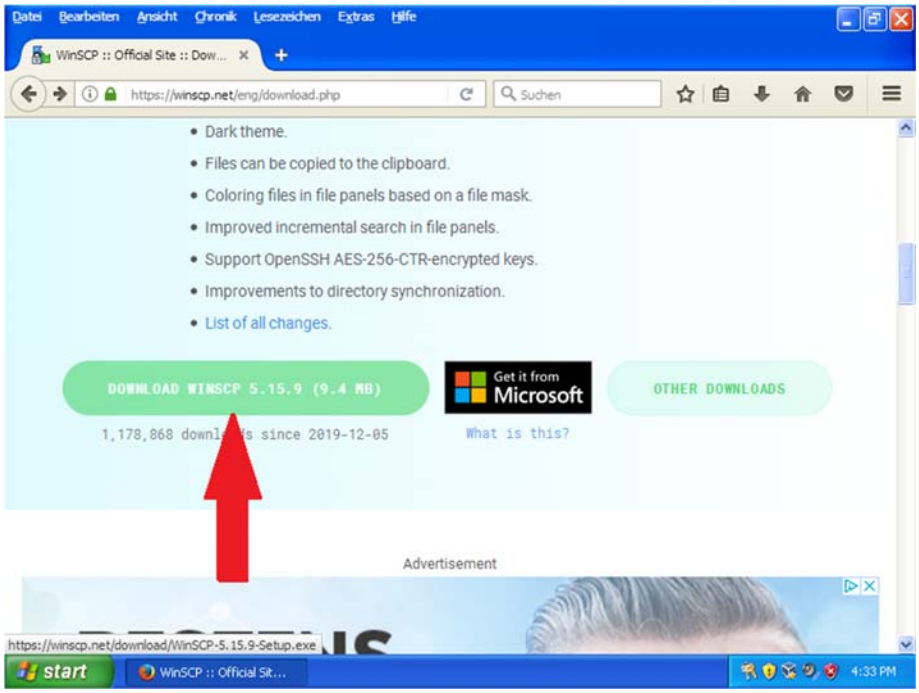
Sie sollten mit der betroffenen Maschine nicht im Internet browsen. Navigieren Sie lediglich zu den Seiten, die Sie erreichen müssen, um die Maschine upzudaten, sofern Sie die notwendige Software nicht z. B. mittels USB-Stick auf die Maschine kopieren können. Nutzen Sie die Maschine insbesondere nicht für Recherchetätigkeiten.

Windows XP: browsen Sie nicht im Internet! Nutzen Sie die neueste für Windows XP verfügbare (seit dem Jahr 2018 veraltete!) Version von Firefox: ftp.mozilla.org/pub/firefox/releases/52.9.0esr/win32/de/

Windows 7: hier werden die Sicherheitsupdates für Internet Explorer bald auslaufen. Installieren Sie bitte die neueste Version von Firefox: https://download.mozilla.org/?product=firefox-esr-latest&os=win

3. FTP-Client

Als FTP/SSH-Client empfehlen wir die Open Source Software WinSCP in der neuesten Version: https://winscp.net/eng/download.php



Maßnahme C: Windows sicherer konfigurieren

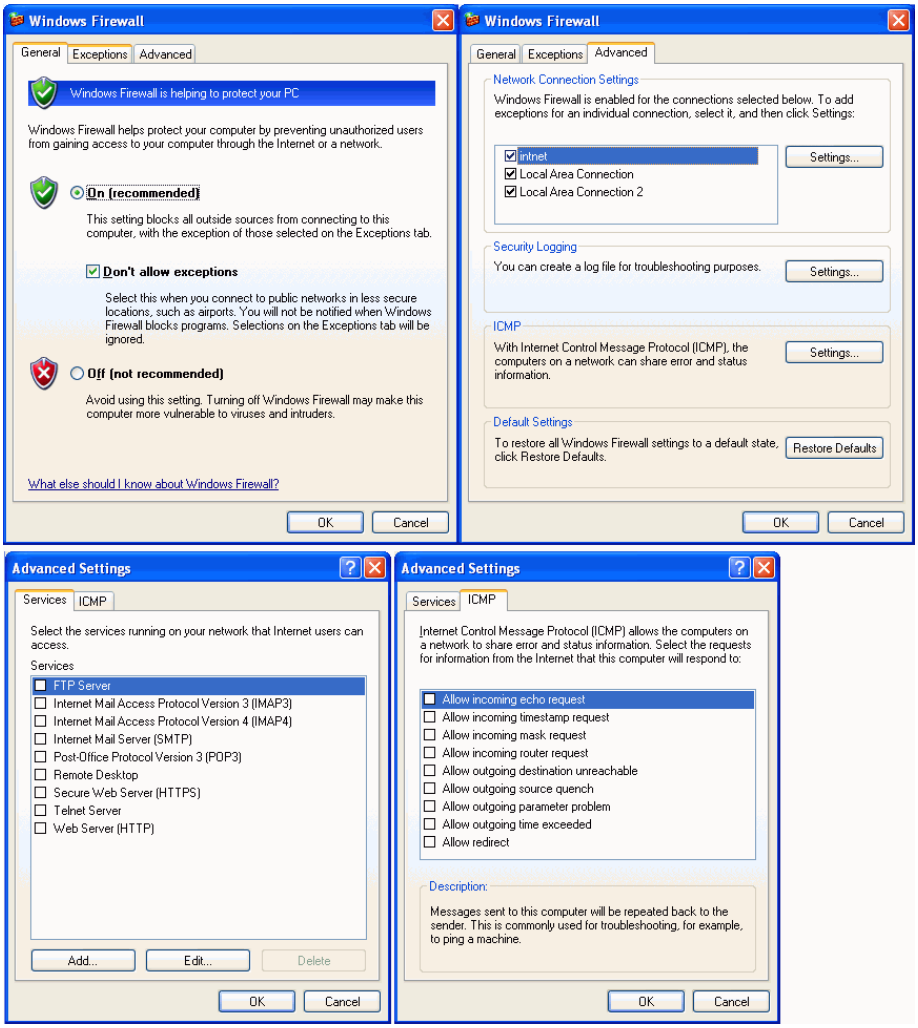
0. Kurzfassung:

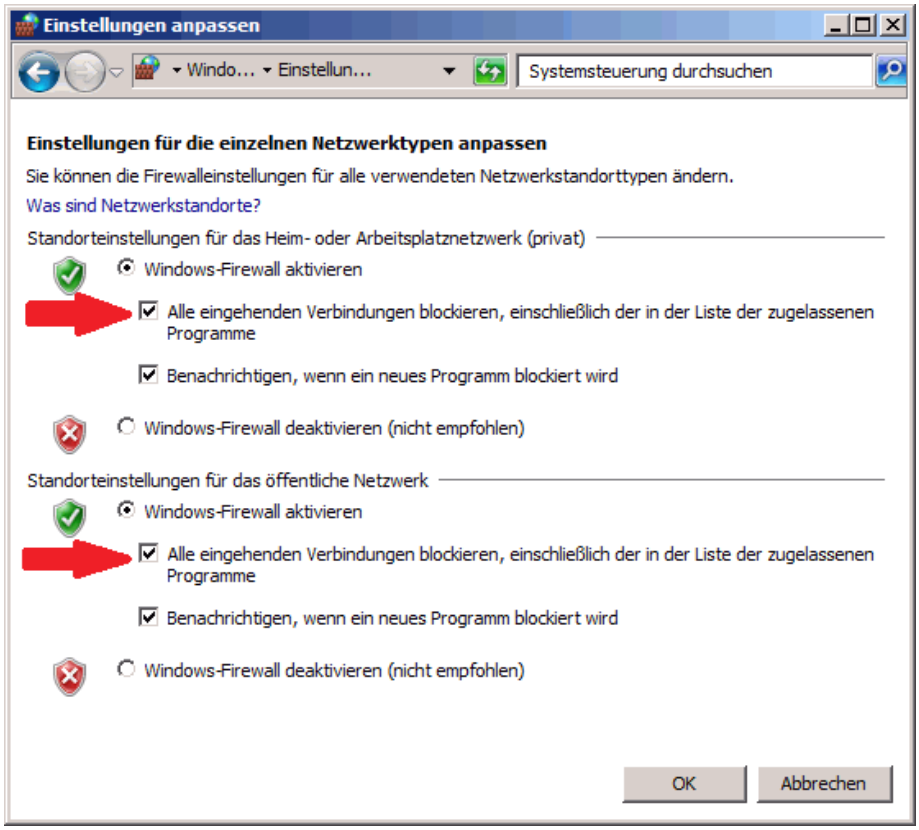
1. Firewall möglichst streng einstellen
2. Netzwerkadapter richtig konfigurieren
3. Unnötige Dienste abschalten
4. Dateifreigaben deaktivieren
5. Useraccounts abstufen

Versuchen Sie, möglichst viele der unten genannten Maßnahmen umzusetzen.

1. Firewall möglichst streng einstellen

Eingehende Verbindungen müssen ausnahmslos ausgeschaltet werden. Dies schließt auch vermeintlich sichere Umgebungen/IP-Adressbereiche wie das Institutsnetz mit ein, da auf diese Weise trotzdem Malware auf die Maschine gelangen kann.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel
Windows Firewall
General
Exceptions
Advanced
Network Connection Settings
Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:
intnet
Local Area Connection
Local Area Connection 2
Settings...
Security Logging
You can create a log file for troubleshooting purposes.
Settings...
ICMP
With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.
Settings...
Default Settings
To restore all Windows Firewall settings to a default state, click Restore Defaults.
Restore Defaults
OK
Cancel
Advanced Settings
Services
ICMP
Select the services running on your network that Internet users can access.
Services
FTP Server
Internet Mail Access Protocol Version 3 (IMAP3)
Internet Mail Access Protocol Version 4 (IMAP4)
Internet Mail Server (SMTP)
Post-Office Protocol Version 3 (POP3)
Remote Desktop
Secure Web Server (HTTPS)
Telnet Server
Web Server (HTTP)
Add...
Edit...
Delete
OK
Cancel
Advanced Settings
Services
ICMP
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:
Allow incoming echo request
Allow incoming timestamp request
Allow incoming mask request
Allow incoming router request
Allow outgoing destination unreachable
Allow outgoing source quench
Allow outgoing parameter problem
Allow outgoing time exceeded
Allow redirect
Description:
Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.
OK
Cancel

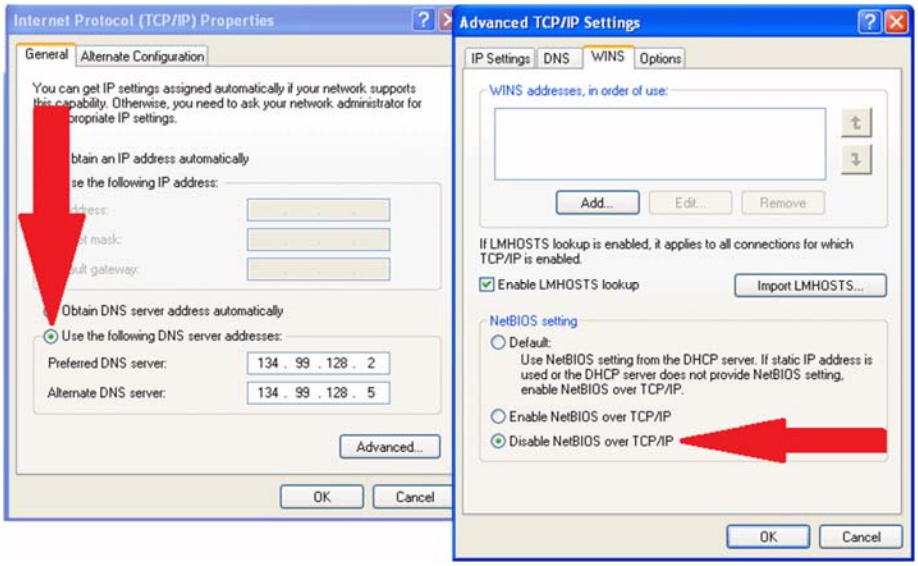


- Klicken Sie (unten links) auf *Start*
- Klicken Sie auf *Systemsteuerung*
- Klicken Sie **unter Windows XP** auf *Sicherheitscenter*
- Klicken Sie **unter Windows 7** auf *System und Sicherheit*
- Scrollen Sie ggf. herunter und klicken Sie auf *Windows Firewall*
- Klicken Sie **unter Windows 7** links auf *Windows-Firewall ein- oder ausschalten*
- Klicken Sie auf *Ein* bzw. *Aktivieren* und dann auf *Keine Ausnahmen zulassen* bzw. auf *Alle eingehenden Verbindungen blockieren*
- Klicken Sie **unter Windows XP** oben auf den rechten Reiter *Erweitert*
- Im weißen Kasten oben setzen Sie alle Häkchen
- Deaktivieren Sie für jede Netzwerkverbindung alle Dienste wie folgt:
    - Klicken Sie eine Verbindung an
    - Klicken Sie rechts neben dem weißen Kasten auf Einstellungen...
    - Deaktivieren Sie im neuen Fenster in beiden Reitern (unter Dienste und ICMP) alle Häkchen
    - Wiederholen Sie diese Schritte für jede Verbindung im oberen weißen Kasten
    - Klicken Sie auf OK
- Klicken Sie wieder auf OK und schließen Sie das Sicherheitscenter

2. Netzwerkadapter richtig konfigurieren

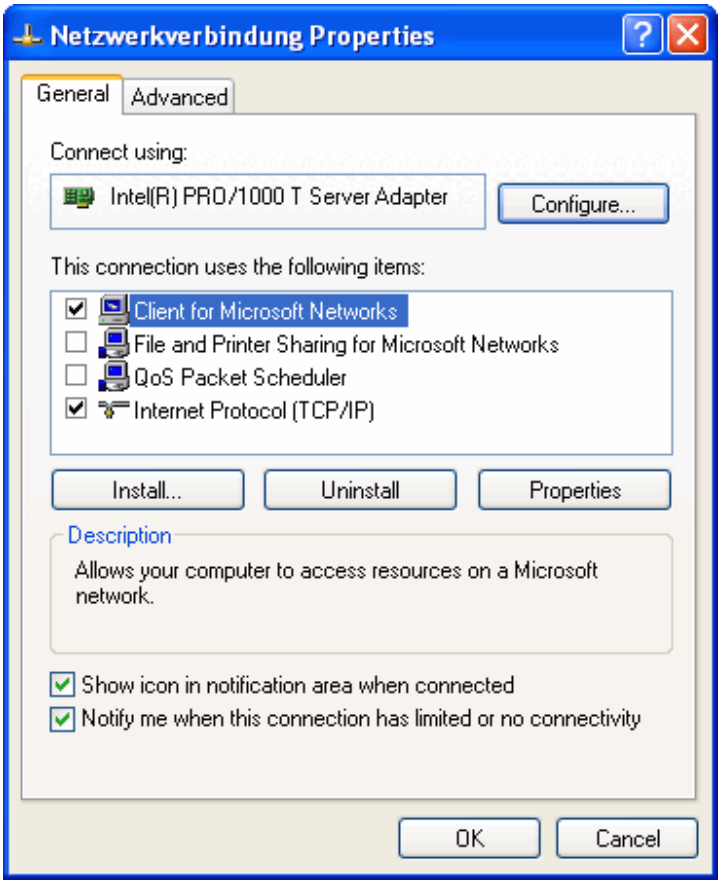
Leider ist es nicht ausreichend, nur die Firewall streng einzustellen. Windows baut im laufenden Betrieb automatisch Verbindungen mit anderen Geräten im Netzwerk auf – und über diese von innen her aufgebauten Verbindungen sind Angriffe auf Windows möglich.

- Klicken Sie (unten links) auf *Start*
- Klicken Sie auf *Systemsteuerung*
- Klicken Sie auf *Netzwerk- und Internetverbindungen* bzw. auf *Netzwerkverbindungen*
- Klicken Sie **unter Windows XP** ggf. noch Mal auf *Netzwerkverbindungen*
- Klicken Sie **unter Windows 7** auf *Netzwerk und Freigabecenter* und dann auf *Adaptereinstellungen ändern*
- Deaktivieren Sie für jede Netzwerkverbindung alle unnötigen Dienste (bis auf TCP/IP) und stellen Sie den DNS-Server der HHU wie folgt ein:
    - Jedes Symbol stellt eine Netzwerkverbindung dar
    - Klicken Sie mit der rechten Maustaste auf eine Internetverbindung und dann auf *Eigenschaften*
    - Klicken Sie auf *Internet Protocol (TCP/IP)* und dann unten rechts daneben auf *Eigenschaften*
    - Klicken Sie auf *Folgende DNS-Serveradressen verwenden* und geben Sie einen vertrauenswürdigen DNS-Server ein
        - An der HHU sind das *134.99.128.2* und *134.99.128.5*
    - Klicken Sie auf *Erweitert...*
    - Klicken Sie auf *WINS*
    - Klicken Sie ganz unten auf *NetBIOS über TCP/IP deaktivieren*



-
    - Klicken Sie zwei Mal auf *OK*

- Wählen Sie alle Häkchen bis auf *Internet Protocol (TCP/IP)* und *Client für Microsoft-Netzwerke* ab:



-
- Klicken Sie oben auf den rechten Reiter *Erweitert*
- Deaktivieren Sie das Häkchen bei *Gemeinsame Nutzung der Internetverbindung*
- Klicken Sie auf *OK*
- Wiederholen Sie diese Schritte für jede Internetverbindung

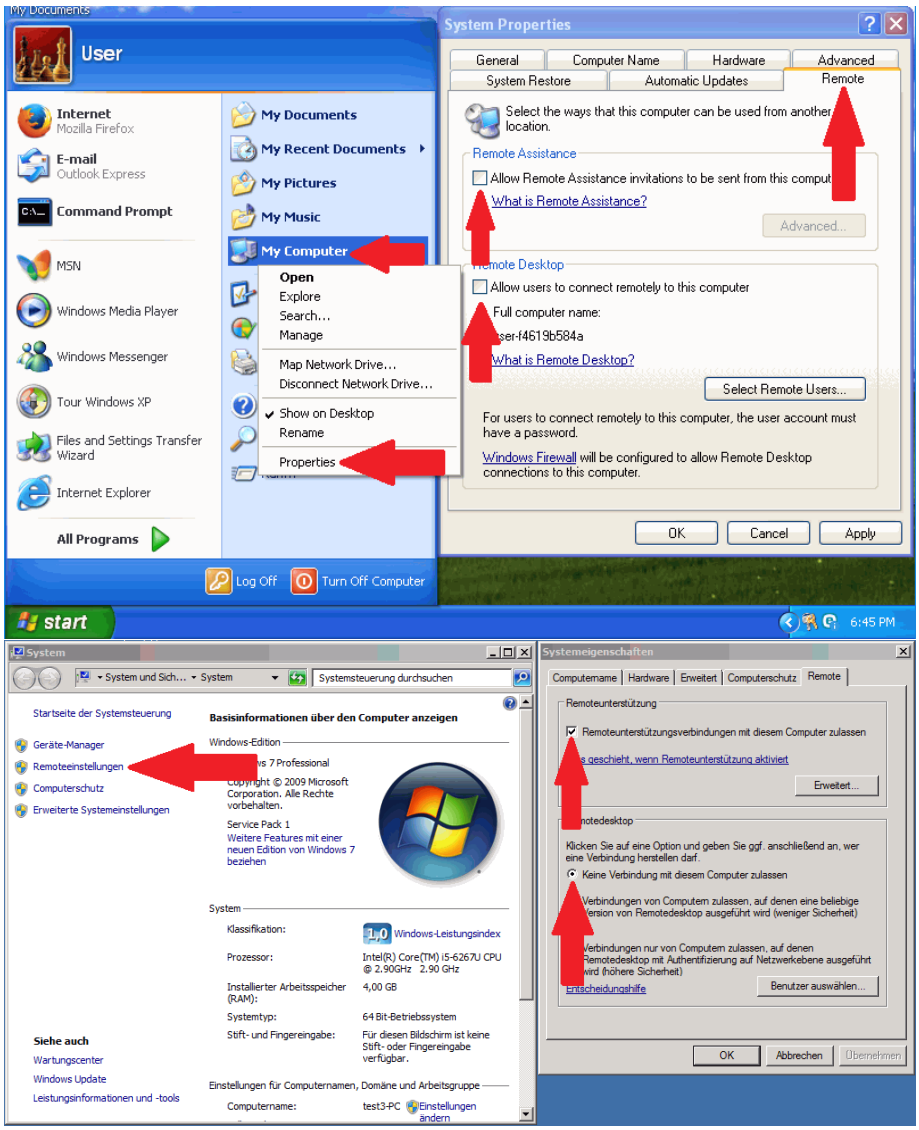
3. Unnötige Dienste abschalten

a. Remote Desktop deaktivieren

Zwar ist bei aktivierter Firewall das Risiko eines Angriffs über das Remote Desktop Protocol (RDP) gering, trotzdem empfiehlt es sich, diese Funktionalität bei veralteten Windows-Versionen abzuschalten.

- Klicken Sie (unten links) auf *Start*

- Klicken Sie *mit der* rechten Maustaste auf *Arbeitsplatz* bzw. *Computer*
- Klicken Sie auf auf *Eigenschaften*
- Klicken Sie oben auf den Reiter *Remote* bzw. oben links auf *Remoteeinstellungen*
- Deaktivieren Sie beide Häkchen bzw. setzen Sie die Option auf *Keine Verbindung mit diesem Computer zulassen*



b. Sonstige Dienste

Systemweit können zur Sicherheit noch weitere Dienste deaktiviert werden. Dafür gibt es zwei Methoden:

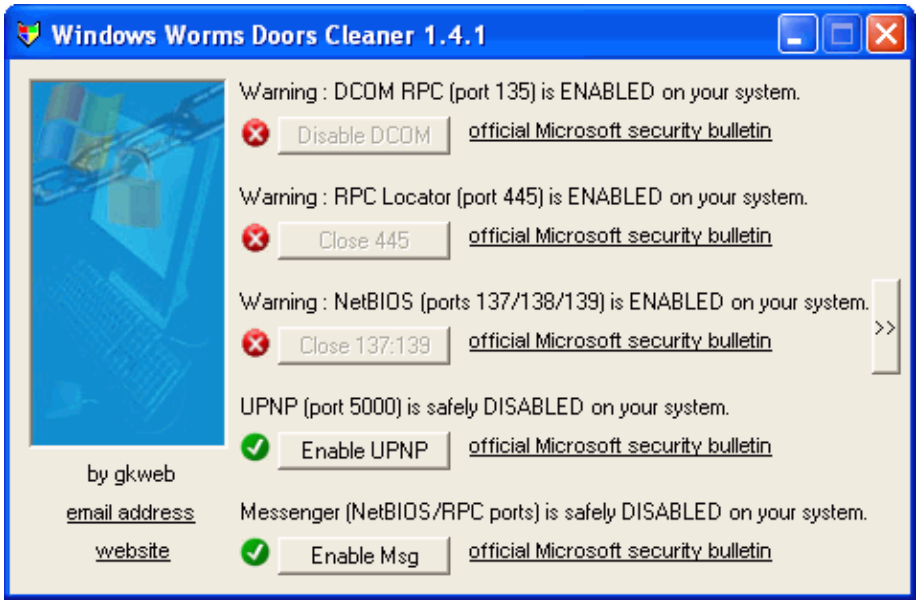
Automatische Methode (nur Windows XP)

Sie können die Freeware *WWDC.exe* (Windows Worms Door Cleaner) von ***Guillaume Kaddouch*** ***(gkweb76*** ***©2004)*** nutzen, um nicht unbedingt notwendige Netzwerkdienste in Windows abzuschalten.

Lizenzhinweis: das Tool WWDC.exe wird auf verschiedenen Seiten im Internet als Freeware verteilt, aber vom Entwickler gkweb76 nicht mehr gepflegt. Sie sollten das Tool nicht verändern und ohne Namensnennung (attribution) nicht weiterverbreiten.

Download: wwdc.exe (50 kb) (SHA-256: df40f41072aeb634e639b7666104e424fc2a7a6ed758f43e239cf0a06aa3b2d0; md5: 999f6e5c8d5c81f48afbdab7f8777323)

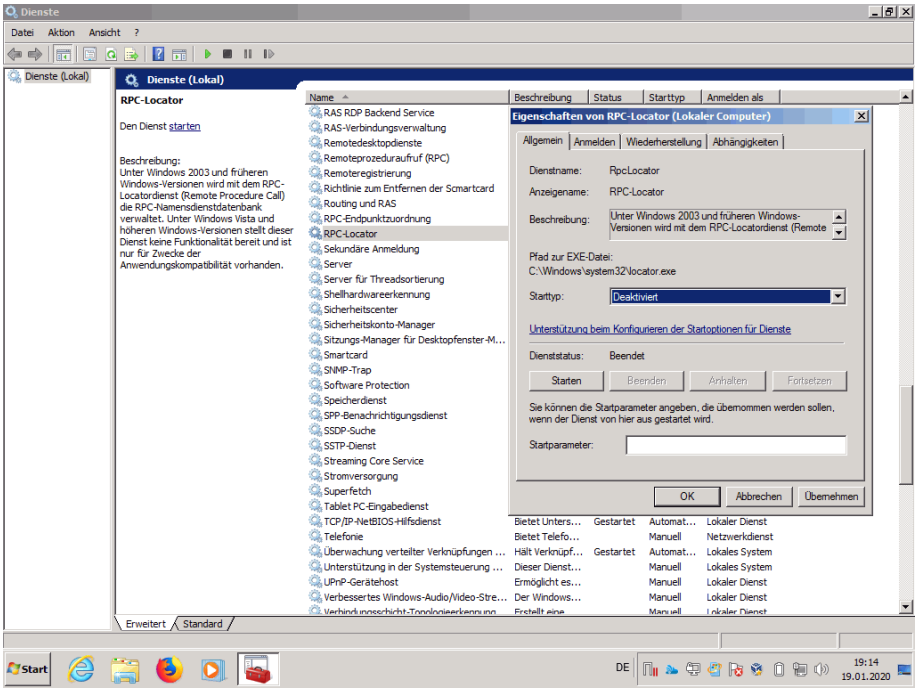
- Laden Sie das Programm herunter und starten Sie es
- Im Bestätigungsfenster bestätigen Sie den Start des Programms mit *Ausführen*
- Im nächsten Fenster bestätigen Sie das Schließen des Ports 135 für DCOM RPC mit *Ja/Yes*
- Klicken Sie auf die rot markierten Knöpfe *Close* und bestätigen Sie ggf. mehrfach mit *Ja/Yes*
- Klicken Sie auf *OK* und starten Sie die Maschine neu



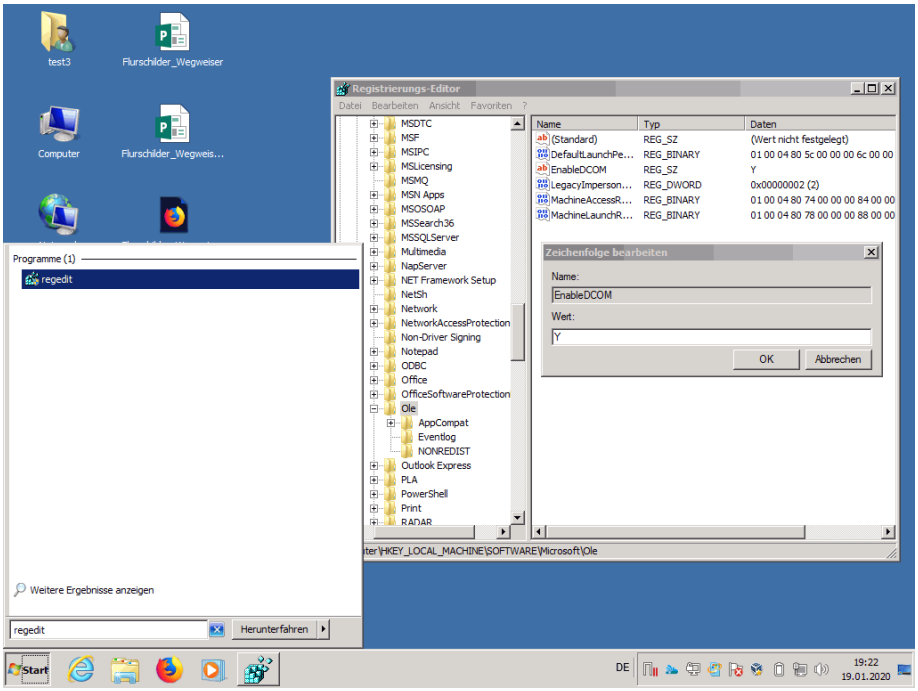
Manuelle Methode

- *RCP-Locator* wie folgt:
  - Klicken Sie (unten links) auf *Start*
  - Klicken Sie **unter Windows XP** auf *Ausführen...*
  - Geben Sie *services.msc* ein und klicken Sie auf *OK*
  - Scrollen Sie im neuen Fenster bis *Remote Procedure Call (RCP)* ***Locator*** herunter

- Klicken Sie mit der rechten Maustaste auf *Remote Procedure Call (RCP) Locator* und dann auf *Eigenschaften*
- Klicken Sie auf das Dropdownmenü neben *Starttyp* und stellen Sie sicher, dass dort *Deaktiviert* eingestellt ist
- Lassen Sie *Remote Procedure Call (RCP)* auf *Automatisch* stehen (verwechseln Sie beide Dienste nicht)
- Klicken Sie auf *OK* und schließen Sie das Fenster



- *DCOM* wie folgt:
  - Klicken Sie (unten links) auf *Start*
  - Klicken Sie **unter Windows XP** auf *Ausführen...*
  - Geben Sie *regedit* ein und klicken Sie auf *OK*
  - Klappen Sie in der linken Fensterhälfte den Pfad *HKEY_LOCAL_MACHINE\Software\Microsoft\OLE* auf
  - Klicken Sie doppelt auf *EnableDCOM*, geben Sie im neuen Fenster *N* ein und klicken Sie auf *OK*
  - Scrollen Sie nach oben und klappen Sie *Software* mit einem Klick auf das Minuszeichen zu
  - Öffnen Sie nun *System\CurrentControlSet\Services\NetBT\Parameters*
  - Klicken Sie mit der rechten Maustaste ins freie Feld, bewegen Sie die Maus auf *Neu* und klicken Sie auf DWORD-Wert
  - Geben Sie SMBDeviceEnabled ein und drücken Sie die Eingabetaste
  - Schließen Sie das Fenster und starten Sie die Maschine neu

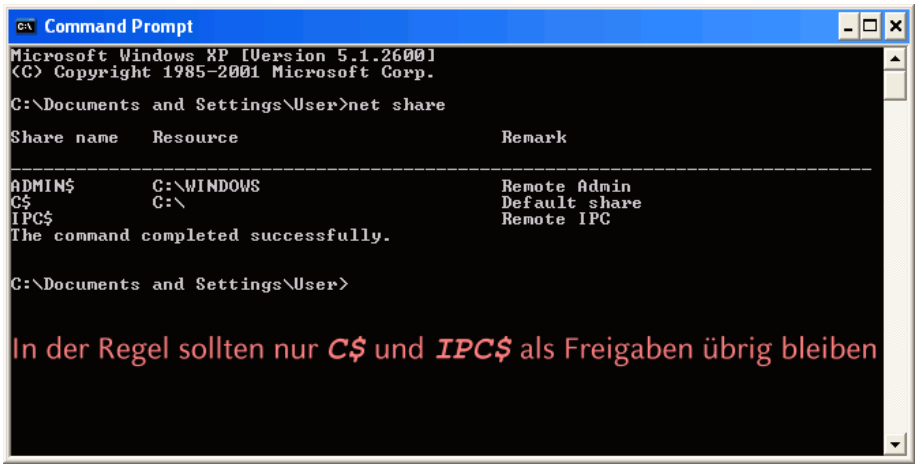


4. Dateifreigaben deaktivieren

Dateifreigaben (shares) sind ein mögliches Einfallstor für Malware. Problematisch, dass auch über eine ausgehende Verbindung Malware auf die Maschine gelangen kann. Da Windows XP besonders verwundbar ist, müssen diese ausgeschaltet werden. Über den Befehl *net share* in der Kommandozeile kann man anzeigen lassen, welche Dateifreigaben aktiv sind.

- Klicken Sie (unten links) auf *Start*
- Klicken Sie **unter Windows XP** auf *Ausführen...*
- Geben Sie *cmd* ein und klicken Sie auf *OK*
- Geben Sie im schwarzen Fenster *net share* ein und drücken Sie die Eingabetaste
    - In der nun erscheinenden Tabelle sehen Sie die freigegebenen Ordner/Dateien
    - Merken oder notieren Sie sich alle Freigaben, die nicht *ADMIN$*, *C$* oder *IPC$* heißen
        - Im untenstehenden Bild ist die Freigabe mit dem Namen *ExampleFldr* nicht gewollt
        - Wir merken uns den Pfad *C:\ExampleFldr*

-
  -
    - Wir gehen zu dem Ordner, klicken auf ihn mit der rechten Maustaste und dann auf *Freigabe und Sicherheit ...*
    - Wir deaktivieren den Haken neben *Diesen Ordner im Netzwerk freigeben*
  - Navigieren Sie zum dem Ort, an dem jeder einzelne freigegebene Ordner liegt
  - Deaktivieren Sie jede einzelne Freigabe über Rechtsklick, *Freigabe und Sicherheit ...*



5. Useraccounts abstufen

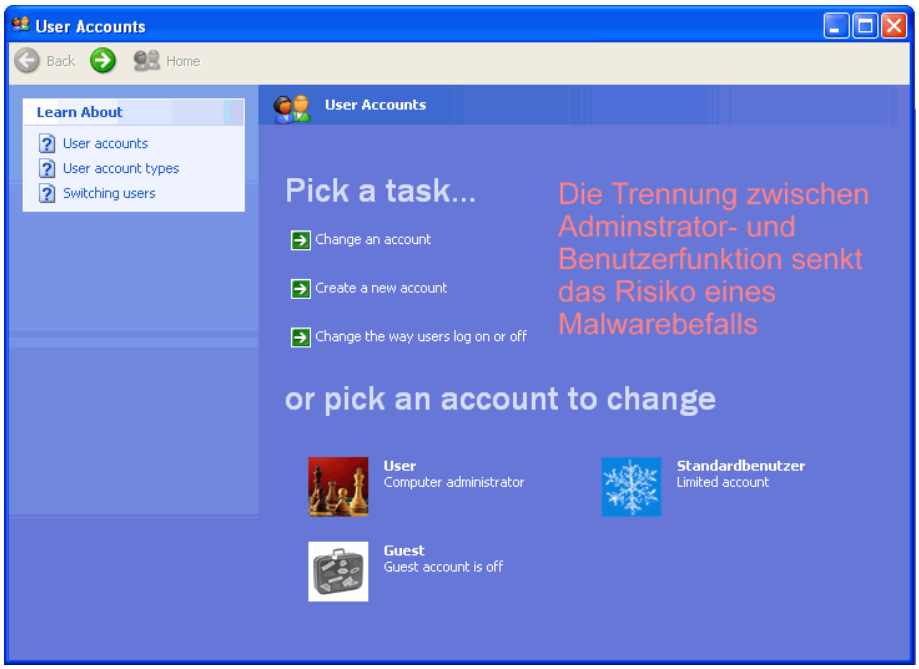
Zuletzt sollte sichergestellt werden, dass es eine Trennung zwischen Administratoraccount (für die Konfiguration der Maschine) und Benutzeraccount (für den eigentlichen alltäglichen Betrieb) gibt, sofern die für die Maschine betriebene Software auch ohne administrative Privilegien funktioniert.

a. Passwort für Administratoraccount festlegen:

- Klicken Sie (unten links) auf *Start*
- Klicken Sie auf *Systemsteuerung*
- Klicken Sie auf *Benutzerkonten*
- Klicken Sie **unter Windows XP** auf Ihren Benutzernamen
- Klicken Sie auf *Passwort erstellen*
- Geben Sie insgesamt zwei Mal ein sicheres Passwort ein

b. Eingeschränktes Benutzerkonto erstellen:

- Klicken Sie (unten links) auf *Start*
- Klicken Sie auf *Systemsteuerung*
- Klicken Sie auf *Benutzerkonten*
- Klicken Sie **unter Windows 7** auf *Benutzerkonten* und dann auf *Anderes Konto verwalten*
- Klicken Sie auf *Neues Konto erstellen*
- Erfinden Sie einen Benutzernamen, geben Sie ihn ein und klicken Sie ein Mal auf *Weiter*
- Wichtig: im nächsten Fenster klicken Sie oben auf *Eingeschränkt*
- Klicken Sie dann auf *Konto erstellen*
- Klicken Sie den neu angelegten Benutzer an
- Klicken Sie auf *Passwort erstellen*
- Geben Sie insgesamt zwei Mal ein sicheres Passwort ein – dieses muss sich zwingend vom Administratorpasswort unterscheiden.



Wichtig ist, dass Sie für die alltägliche Arbeit mit der Maschine ausschließlich eingeschränkte Benutzerkonten verwenden.

6. Hinweis zu Virenscannern (nur bedingt empfehlenswert)

Besonders auf Maschinen, die nicht zum Surfen benutzt werden sollen, ist die Installation eines Virenscanners generell nicht empfehlenswert. Virenscanner führen häufig zu Kompatibilitätsproblemen und verlangsamen prinzipbedingt durch sie geschützte Systeme. Sollten Sie sich dennoch aufgrund der Arbeitsweise mit der betroffenen Maschine dafür entscheiden, einen Virenscanner einzusetzen, gelten die untenstehenden Empfehlungen.

a. Windows XP

Leider stellt Microsoft für Security Essentials (MSE) unter Windows XP keine Signaturupdates mehr bereit. Auch über die auslaufende Sophos-Lizenz der HHU lässt sich keine unter Windows XP funktionierende Version mehr beziehen. Diesem Grund müsszen Sie, falls Sie einen Virenschutz nutzen möchten, auf andere Hersteller zurückgreifen. Uns bekannte, mit Windows XP kompatible Virenscanner aus dem europäischen Raum sind (unter anderem):

- ESET NOD32 Version 9 - kostenpflichtig, ab ca. 30 Euro jährlich, Bildungsrabatt ab fünf Geräten möglich; *Steuerungen ausgehender Verbindungen unter Windows XP erfolgreich getestet*
- AVAST und AVG - kostenpflichtig, ab ca. 34 Euro jährlich, Bildungsrabatt unter Umständen möglich
- G Data Antivirus 25.1.0.12 - kostenpflichtig, ab ca. 34 Euro jährlich, Bildungsrabatt ab fünf Geräten wahrscheinlich möglich

Beachten Sie, dass die o.g. Hersteller zwar auch kostenlose Versionen für Heimanwender anbieten, diese aber vermutlich nicht an der HHU eingesetzt werden dürfen, auch wenn sie technisch funktionieren.

b. Windows 7

Da Microsoft zur Zeit (noch) Signaturupdates für Microsoft Security Essentials unter Windows 7 bereitstellt und gleichzeitig die Campuslizenz für Sophos Antivirus ausläuft, empfiehlt es sich dringend, MSE unter Windows 7 zu installieren:

https://www.microsoft.com/de-DE/download/details.aspx?id=5201

Zur Zeit (Stand Februar 2020) empfiehlt es sich nicht, unter Windows 7, 8 oder 10 einen anderen Virenscanner als Microsoft Security Essentials bzw. Windows Defender zu nutzen. Sollten Sie verdächtige Dateien handhaben und überprüfen wollen, empfiehlt sich ein Vorabscan mithilfe von Diensten wie Virustotal.