Handbuch für Türsteher

Version 3.0.0 (Mai 2018)

excubits.com
Einfach. Sicher. Excubits.

Impressum:

Urheberrecht:	Excubits
Web:	https://excubits.com
Kontakt:	info@excubits.com
Version:	3.0.0
Status:	Veröffentlicht

Inhaltsverzeichnis

Was ist Türsteher? ... 1
Systemanforderungen ... 2
Installation ... 2
Automatische Installation ... 2
Automatische Installation manuell starten ... 3
Deinstallation ... 3
Allgemeine Konfigurationshinweise ... 3
Türsteher aktivieren und deaktivieren ... 4
Protokolldatei aktivieren und deaktivieren ... 5
Hashing aktivieren und deaktivieren ... 5
Kommandozeilen-Prüfung aktivieren und deaktivieren ... 5
Whitelist konfigurieren ... 5
Wildcards richtig nutzen ... 7
Prioritätsregeln ... 7
Verwendung von Hashwerten ... 8
Blacklist konfigurieren ... 8
Blacklist Beispiel 1: Sie wollen ein bestimmtes Verzeichnis verbieten ... 8
Blacklist Beispiel 2: Es ist eine Sicherheitslücke bekannt geworden ... 9
Empfehlungen für die [BLACKLIST] ... 10
Leise Regeln (Silent Rules) ... 10
Parentchecking: Bedingte Regeln für Eltern-Prozesse ... 11
Beispiele für die Parent-Regeln in der [WHITELIST] ... 11
Beispiele für die Parent-Regeln in der [BLACKLIST] ... 12
CMD-Check/ Kommandozeilen-Prüfung ... 12
Kommandozeilen-Whitelist konfigurieren ... 13
Kommandozeilen-Blacklist konfigurieren ... 14
Ende der Konfiguration ... 14
Türsteher für den ersten Start vorbereiten / Simulationsmodus ... 14
Installationsmodus ... 15
Ereignismeldungen ... 16
Hilfsprogramme (Tools) ... 16
Anwendung für den Tray-Bereich ... 16
Unterschiedliche Farben für unterschiedliche Modi ... 17
Warnmeldungen der Tray-Anwendung abschalten ... 17

Bei Alarm E-Mail an den Administrator 18
Steuerung im laufenden Betrieb 18
Technischer Hintergrund 18
Generelle Empfehlungen 19
Zeichenerklärung / Sonderzeichen 20
Stichwortverzeichnis 21

Was ist Türsteher?

Türsteher ist eine Sicherheitssoftware für Windows-Computer. Türsteher blockiert unbekannte oder ausführbare Schadsoftware. Zum Beispiel Computer-Viren, -Würmer, Verschlüsselungstrojaner oder Ähnliches. Dabei ist es egal, ob die schädliche Software von Netzlaufwerken, USB-Sticks, externen Festplatten, CD-/DVD-ROMs oder E-Mail-Anhängen kommen. Auch neu entdeckte Sicherheitslücken, für die es noch keine Updates gibt, kann Türsteher deutlich entschärfen.

Türsteher funktioniert nach dem Ausschlussprinzip: Alle bekannten Programme und Funktionen laufen wie gewünscht und gewohnt. Alle unbekannten und möglicherweise gefährlichen Programme blockiert Türsteher. Die Liste der bekannten Programme kann jederzeit erweitert werden.

Neueste Software-Architektur

Türsteher läuft als sogenannter Treiber im Kern des Betriebssystems. Dadurch kann unsere Software unbekannte oder bösartige Programmdateien viel früher blockieren als herkömmliche Virenscanner. Einmal konfiguriert kann Türsteher ein System ohne weitere Aktualisierungen vor neuen, unbekannten Schadprogrammen schützen.

Zusätzliche Programmtools für Profis

Über Elternbasierte Regeln können Sie festlegen, welche Anwendungen ein Programm starten darf und welche nicht. Diese Funktion ist vor allem deswegen sehr sinnvoll, da Cyber-Kriminelle über Webbrowser oder Office heimlich schädliche Programme starten können. Dies können Sie mit Türsteher nun wirksam verhindern.

Mit dem Kommandozeilen-Scanning können Sie außerdem festlegen, mit welchen Kommandozeilen-Parametern ein Programm gestartet werden darf und mit welchen nicht. Auf diese Weise können Sie Interpreter wie Powershell, JScript, Java, Python und weitere zusätzlich absichern.

Hinweis

Bitte nehmen Sie sich für die Installation und Konfiguration von Türsteher etwas Zeit. Denn Türsteher lässt sich nur dann optimal und sicher nutzen, wenn Sie die Funktionsweise verstanden zu haben.

Lesen Sie sich diese Anleitung aufmerksam durch und halten Sie sich exakt an die Empfehlungen und Beschreibungen, um Abstürze oder ein blockierendes System zu vermeiden.

Systemanforderungen

Türsteher läuft unter den folgenden Versionen von Windows:

Version	32-bit/64-bit
Windows XP	Auf Anfrage, nur für Firmenkunden
Windows Vista	Auf Anfrage, nur für Firmenkunden
Windows 7 (inkl. Windows Server)	ja / ja
Windows 8 (inkl. 8.1, Server, Core)	ja / ja
Windows 10 (inkl. Server, Core)	ja / ja

Zum Ausführen von Türsteher benötigen Sie mindestens 8 MB freien Speicher auf der Festplatte. Beachten Sie, dass Türsteher eine Protokolldatei anlegt, in der die Dateipfade und Dateinamen blockierter Programmdateien gespeichert werden. Abhängig von der Anzahl der protokollierten Einträge kann diese Protokolldatei auch mehrere Megabytes groß werden. Es sollte also ausreichend Speicherplatz für die Protokolldatei verfügbar sein.

Installation

Um Türsteher installieren zu können, benötigen Sie administrativen Zugriff auf den Rechner. Für den laufenden Betrieb von Türsteher sind nach der Installation keine Administratoren-Rechte nötig. Zum An- bzw. Abschalten und für die Deinstallation des Treibers werden ebenfalls Administratoren-Rechte benötigt.

Automatische Installation

Das Installationsprogramm kann den Treiber und die mitgelieferten Tools automatisch konfigurieren und starten. Klicken Sie doppelt auf die Installations-Anwendung. Folgen Sie im Anschluss einfach den Dialogen des Installationsprogramms.

Das Installationsprogramm installiert den Treiber und legt eine Basiskonfiguration an. Im folgenden Kapitel finden Sie eine detaillierte Beschreibung der Konfigurationsdatei und wie man sie anpasst. Das Installationsprogramm hat Ihnen einige Schritte bereits abgenommen. So finden Sie die `türsteher.ini` Datei in Ihrem Systemverzeichnis (meist `C:\Windows\`), zudem wurde die Logdatei angelegt und der Treiber vollautomatisch im System registriert.

Unter `C:\Programme\` bzw. `C:\Programme (x86)\` finden Sie den Ordner Excubits. Klicken Sie sich bis in den Ordner Türsteher durch. Darin finden Sie nun diese Anleitung (Handbuch), Steuerungsskripte und Anwendungen (`./Tools`), die

Ihnen bei der Installation helfen und Sie beim späteren Betrieb mit Türsteher unterstützen können.

Automatische Installation manuell starten

Sie können die automatische Installation auch manuell ausführen, indem Sie die Installations-Anwendung erst entpacken, zum Beispiel mit Win-RAR oder 7zip in einen Ordner mit dem Namen Excubits. Nun empfehlen wir Ihnen diesen Ordner in das Verzeichnis `C:\Programme (x86)\` oder `C:\Programme\` zu kopieren. Gehen Sie nun in den Ordner Türsteher und klicken Sie das Programm `Install.exe` doppelt an. Das Programm installiert nun den Treiber und die mitgelieferten Tools so, als hätten Sie die Installation über das Installationspaket durchgeführt.

Deinstallation

Sie können den Treiber und die Tools jederzeit mit dem Deinstallationsprogramm wieder vom Rechner entfernen. Führen Sie dazu einfach das Programm mit dem Namen `Uninstall.exe` aus, welches sich im Installationspaket von Türsteher befindet. Dieses Programm löscht den Treiber, die Tray-Anwendung, die Log- und Konfigurationsdatei und kann Türsteher vom System entfernen.

Allgemeine Konfigurationshinweise

Türsteher implementiert ein striktes Regelsystem, bei dem man präzise angeben muss, welche Dateien oder Pfade erlaubt bzw. verboten sind. Dateien und Pfade, die nicht in der Konfiguration angegeben wurden, werden von Türsteher später ohne Rückfrage blockiert. Das kann im schlimmsten Fall dazu führen, dass das Betriebssystem nicht mehr korrekt oder überhaupt nicht mehr startet. Daher ist es sehr wichtig, die Liste mit Vorsicht zu konfigurieren. Prüfen Sie die von Ihnen angegebenen Pfade und Dateinamen am besten stets über den Explorer, um sicherzustellen, dass die korrekte Schreibweise gewählt wurde.

Konfiguration im Unicode-Format

Die Konfiguration von Türsteher befindet sich ausschließlich in der Datei `tuersteher.ini`. Es handelt sich um eine Datei im Unicode-Format, die man mit jedem gängigen Texteditor öffnen kann (z. B. mit Notepad, Notepad++). Sie können auch Schriftzeichen aus anderen Sprachen nutzen, wie beispielsweise:

- Галдёж
- مْرَحَبًا
- הלו

Groß- und Kleinschreibung

Türsteher unterscheidet nicht zwischen Groß- und Kleinschreibung. Sie können die Regeln für Dateinamen und Dateipfade also vollständig in Großbuchstaben, in Klein- und Großbuchstaben oder nur in Kleinbuchstaben angeben.

Platzhaltersymbole / Wildcards

Daneben unterstützt Türsteher sog. Platzhaltersymbole (engl. wildcards). Mit diesen können Sie Regeln verallgemeinern. So können Sie beispielsweise mit `*.scr` definieren, dass sämtliche Dateien mit der Dateiendung `.scr` blockiert werden sollen. Als Symbole erkennt Türsteher den **Stern** `*` für eine beliebige Anzahl von Zeichnen und das **Fragezeichen** `?` für exakt ein beliebiges Zeichen.

Konfigurationsdatei `tuersteher.ini`

Um Türsteher zu konfigurieren und zu aktivieren, gehen Sie nun in die Konfigurationsdatei `tuersteher.ini`. Dies können Sie über das entsprechende Verzeichnis tun oder über die Trayanwendung unten rechts. Nun sollte sich der Texteditor (normalerweise Notepad) mit folgendem Inhalt öffnen:

```
[#LETHAL]
[LOGGING]
[SHA256]
[#CMDCHECK]
[WHITELIST]
C:\Windows\*
C:\Program Files\*
C:\Program Files (x86)\*
C:\ProgramData\Microsoft\*
7FBFAB17FE55578159F482A3C9741F02EF5C15C939F4BF1C7B164FAA0AB6DDA3
[BLACKLIST]
C:\Windows\System32\msiexec.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files (x86)\Internet Explorer\iexplore.exe
[CMDWHITE-LIST]
!*explorer.exe>*wscript.exe*C:\Firmenskripte\*
*>*
[CMDBLACKLIST]
*explorer.exe>*wscript.exe*
[EOF]
```

Neustart nach jeder Änderung der Konfiguration

Jede Änderung in der Konfigurationsdatei erfordert einen Neustart von Türsteher. Nur so können Änderungen übernommen werden.

Türsteher aktivieren und deaktivieren

Das Zeichen `#` (auch Hashtag genannt) bedeutet ausgeschaltet, ohne das Hashtag ist die entsprechende Komponente angeschaltet:

`[#LETHAL]` = ausgeschaltet

[LOGGING] = angeschaltet
[SHA256] = angeschaltet
[#CMDCHECK] = ausgeschaltet

Bei der Erstinstallation sollte Türsteher immer erst einmal inaktiv geschaltet sein, also [#LETHAL]. So können Sie die Einstellungen testen, ohne dass falsche Konfigurationen Probleme bereiten. Sobald Sie die Konfiguration fertiggestellt und getestet haben, können Sie Türsteher aktiv schalten [LETHAL]. Jetzt werden unbekannte und gefährliche Programme blockiert.

Protokolldatei aktivieren und deaktivieren

Das Zeichen # bedeutet ausgeschaltet, ohne das Hashtag ist die entsprechende Komponente angeschaltet:

[LOGGING] = angeschaltet
[#LOGGING] = ausgeschaltet

Wir empfehlen die Protokollierung stets aktiv zu schalten. Türsteher schreibt dann jedes Ereignis in die Logdatei (C:\Windows\tuersteher.log). Versucht zum Beispiel ein Programm zu starten, das nicht auf der Whitelist steht, blockiert Türsteher den Start des Programms und schreibt dieses Ereignis in die Logdatei. Sie können diese Datei auch bequem über die Trayanwendung einsehen. Klicken Sie dazu auf Logdatei öffnen.

Hashing aktivieren und deaktivieren

Wenn Sie Hashwerte von Dateien als Referenz verwenden wollen, aktivieren Sie [SHA256]. Wollen Sie die Hashfunktion von Türsteher nicht verwenden, deaktivieren Sie diese Funktion: [#SHA256].

Lesen Sie im Kapitel **„Verwendung von Hashwerten"** mehr über den Umgang mit Hashwerten.

Kommandozeilen-Prüfung aktivieren und deaktivieren

Soll Türsteher zusätzlich die Kommandozeilen-Regelprüfung anwenden, muss die Zeile [CMDCHECK] angegeben werden. Möchten Sie die Kommandozeilen-Regelprüfung nicht nutzen, ist [#CMDCHECK] anzugeben.

Lesen Sie im Kapitel **„CMD-Check/ Kommandozeilen-Prüfung"** mehr über den Umgang mit der Kommandozeilen-Prüfung.

Whitelist konfigurieren

```
[WHITELIST]
C:\Windows\*
C:\Program Files\*
C:\Program Files (x86)\*
C:\ProgramData\*
```

Unterhalb des Eintrags [WHITELIST] definieren Sie alle Pfade, von denen aus Programmcode gestartet werden darf. Hier sollten Sie mindestens die Dateipfade hinterlegen, die für den Betrieb von Windows und den von Ihnen installierten Programmen zwingend notwendig sind, d. h. insbesondere alle vom Betriebssystem Windows benötigten Pfade (oder Dateien). Durch die automatische Installation sind die wichtigsten Pfade bereits eingetragen.

Ab Windows 7 sind dies in der Regel die folgenden Pfade:

```
C:\Windows\*
C:\Program Files\*
C:\ProgramData\Microsoft\*
```

Wenn Sie eine 64-bit Version von Windows nutzen, finden Sie zusätzlich noch den Pfad für installierte 32-bit Programme unter:

```
C:\Program Files (x86)\*
```

Achten Sie darauf, **jede Pfadangabe** mit dem Symbol * zu beenden. Das Sternsymbol dient hier als Platzhalter (wildcard) und gibt sämtliche Dateien und Unterverzeichnisse in diesen Ordnern frei. Alternativ können Sie auch jede Datei einzeln aufführen, dies ist jedoch aufwändig und nur im Hochsicherheitsbereich sinnvoll.

Verzeichnisse von Computerherstellern

Ggf. hat der Hersteller Ihres Computers noch weitere Verzeichnisse für Treiber angelegt, die sich häufig unterhalb des Hauptlaufwerks befinden (meist unter C:\). Bei Rechnern der Hersteller DELL, ACER und ASUS heißen diese Verzeichnisse beispielsweise oft:

- C:\DELL*
- C:\ASUS*
- C:\DRIVERS*
- C:\Intel*
- C:\AMD*
- C:\OEM*

Weitere vertrauenswürdige Programme freigeben

Wenn Sie zusätzliche Programme, wie Gimp, Veracrypt oder Notepad++ in anderen Verzeichnissen installiert haben, müssen Sie diese ebenfalls in der Whitelist freigeben. Die Einträge könnten dann beispielsweise wie folgt lauten:

```
D:\PortableApps\VeraCrypt\*
D:\PortableApps\Gimp\*
```

Neben Pfadangaben können Sie auch einzelne Programmdateien in die Whitelist eintragen. Hierzu schreiben Sie den kompletten Pfad mit Angabe des Dateinamens und seiner Erweiterung in eine Zeile. So können Sie beispielsweise bestimmte Programmdateien zulassen, ohne den gesamten Pfad und dessen Inhalte zu erlauben. Befinden sich beispielsweise im Ordner unter F:\Sandbox\

mehrere DLLs und EXE-Dateien, Sie möchten allerdings nur eine bestimmte Anwendung mit dem Namen `TestA.exe` zulassen, so fügen Sie in die Whitelist folgende Regel ein:

```
F:\Sandbox\TestA.exe
```

Wildcards richtig nutzen

Türsteher unterstützt sog. Wildcards (Platzhaltersymbole). Mit diesen können Sie individuelle Regeln definieren. Zum Beispiel: Sie wollen sämtliche `.exe` Dateien im Verzeichnis `F:\Sandbox` zulassen. Oder Sie wollen Dateien, die mit A beginnen und `.exe` abschließen zulassen. Oder Sie wollen Programmdateien, von einem beliebigen Laufwerk, die mit hallo beginnen und mit `.exe` abschließen freigeben:

```
F:\Sandbox\*.exe
A*.exe
?:\hallo*.exe
```

Das Sternsymbol steht dabei für ein oder mehrere beliebige Zeichen, das Fragezeichen steht für genau ein Zeichen.

Prioritätsregeln

Türsteher kann auch sog. Prioritätsregeln verarbeiten. Mit einem Ausrufezeichen `!` können Sie einer Regel Vorrang geben, sie hat dann eine höhere Priorität.

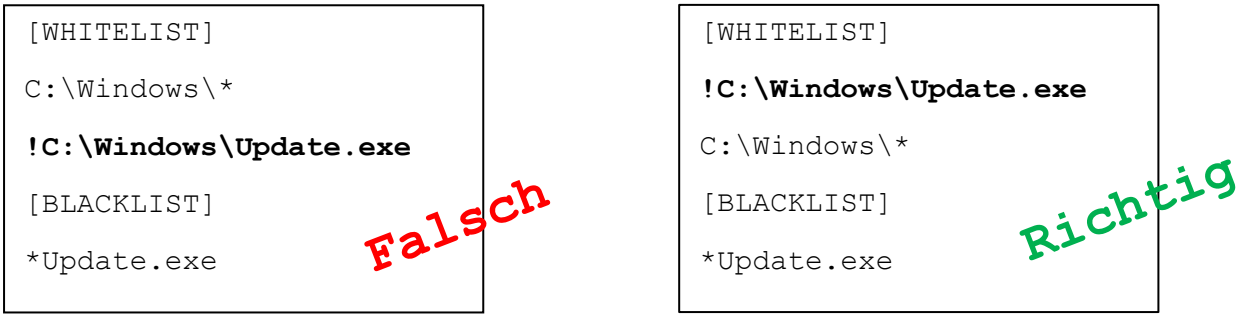
Wir empfehlen beispielsweise den Pfad `C:\Windows\Temp\*` in die Blacklist aufzunehmen. Alle Programme, die in diesem Verzeichnis sind, können nun nicht mehr gestartet werden. Es kann aber vorkommen, dass bestimmte Updateprogramme ihre Prozesse genau in diesen Ordnern ausführen möchten. Auch wir wollen, dass Updates eingespielt werden können. Mit einer Prioritätsregel kann man dieses Problem lösen. Dazu geben wir in der [`WHITELIST`] das gewünschte Programm mit einem Ausrufezeichen eine höhere Priorität. Die Regel in der Whitelist überstimmt nun die Regel in der Blacklist. Nehmen wir an, dass das gewünschte Update `AVUpdater.exe` heißt. Dann lauten die Regeln folgendermaßen:

```
[WHITELIST]
!C:\Windows\Temp\AVUpdater.exe
[BLACKLIST]
C:\Windows\Temp\*
```

Prioritätsregeln funktionieren in allen Regel-Bereichen für Türsteher: In der White- und Blacklist und bei den Kommandozeilen-Regeln (`CMDCHECK`).

Hinweis!

Regeln mit einer höheren Priorität müssen der Reihenfolge nach als erstes stehen. Beispiel:



Verwendung von Hashwerten

Türsteher kann auch `SHA-256` Hashwerte mit der Whitelist abgleichen. D. h. anstatt einer Pfadregel kann auch schlicht der Hashwert der freizugebenden (Whitelist) oder der zu blockierenden (Blacklist) Datei angegeben werden. Die Angabe des Dateipfades oder Dateinamens ist dann nicht notwendig. Bitte beachten Sie, dass die Pflege solcher Hashlisten zeitaufwändig ist. Bei Updates und Patches müssen die Hashwerte neu generiert werden.

Generell empfehlen wir, die Verwendung von Hashwerten nur für die Verzeichnisse zu nutzen, die potenziell durch Veränderung gefährdet sind. Zum Beispiel Netzlaufwerke, die über keinen speziellen Berechtigungsschutz verfügen und von Anwendern geändert werden können. Hier könnten Anwendungsprogramme z. B. mit einem Virus infiziert oder durch Schadprogramme ersetzt werden. Auf solchen Laufwerken sollten dann Hashwerte genutzt werden.

Wir bieten für die optimale Konfiguration Schulungen und Beratung an.

Blacklist konfigurieren

```
[BLACKLIST]
C:\Windows\System32\msiexec.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files (x86)\Internet Explorer\iexplore.exe
```

Unterhalb des Eintrags [`BLACKLIST`] definieren Sie alle Pfade, von denen **kein Programmcode** gestartet werden darf. Programme, die auf dieser Liste stehen werden automatisch blockiert.

Blacklist Beispiel 1: Sie wollen ein bestimmtes Verzeichnis verbieten

In der Whitelist haben Sie das Windows-Verzeichnis über `C:\Windows\*` freigegeben. Die Whitelist-Regel erlaubt nun, dass alle Programme in diesem Verzeichnis gestartet werden können, auch in allen Unterverzeichnissen. Nun möchten Sie aber ein bestimmtes Verzeichnis blockieren, weil Sie es für unsicher halten. Beispielsweise das Verzeichnis `C:\Windows\Fonts\*`. Um nun dieses

Verzeichnis und alle Programme darin zu blockieren, müssen Sie es in die Blacklist aufnehmen:

```
[WHITELIST]
C:\Windows\*
[BLACKLIST]
C:\Windows\Fonts\*
```

Sie können einzelne Anwendungen oder auch ganze Verzeichnisse blockieren. Es ist auch möglich, den Hashwert einer zu blockierenden Datei anzugeben.

Blacklist Beispiel 2: Es ist eine Sicherheitslücke bekannt geworden

Angenommen, im Microsoft Browser Internet Explorer wurde eine Sicherheitslücke entdeckt und es gibt noch kein Update für diese Sicherheitslücke. Mit Türsteher können Sie nun über die Blacklist verhindern, dass Kriminelle diese Lücke ausnutzen können. Sie können nun einfach folgende Regel definieren:

```
[WHITELIST]
C:\Windows\*
[BLACKLIST]
C:\Windows\Program Files\Internet Explorer\*
```

Wenn Sie eine 64-bit Version von Microsoft Windows verwenden, fügen Sie noch eine zusätzliche Regel ein:

```
[WHITELIST]
C:\Windows\*
[BLACKLIST]
C:\Windows\Program Files\Internet Explorer\*
C:\Windows\Program Files (x86)\Internet Explorer\*
```

Auf diese Weise wird der Internet Explorer und all seine Komponenten durch Türsteher blockiert. Der Internet Explorer kann nicht mehr gestartet werden und damit besteht das Risiko einer unbeabsichtigten Infektion nicht mehr. Sobald die Sicherheitslücke geschlossen wurde und Sie den Browser wieder freigeben möchten, können Sie die Regel einfach wieder entfernen.

Hinweis!

Statt eines ganzen Verzeichnisses kann es in manchen Fällen auch zweckmäßig sein, nur einzelne Programmdateien (wie z. B. DLLs zu Plug-ins) zu deaktivieren. Insbesondere dann, wenn diese wegen einer Sicherheitslücke gefährdet sind. Häufig ist es nämlich so, dass bestimmte Bibliotheken oder Plug-ins für Angriffe verwundbar sind. Cyber-Kriminelle nutzen die Lücken dann aus, um Ihren Rechner mit weiterem Schadcode zu infizieren. Wenn Sie die verwundbaren Plug-ins/Bibliotheken über die Blacklist blockieren, können diese nicht mehr genutzt werden und Angreifer können Sie auch nicht für einen Angriff ausnutzen. Nachdem eine Programmaktualisierung für die verwundbaren Komponenten

vorhanden ist, kann diese eingespielt und die Regel aus der Blacklist entfernt werden.

Vorsicht bei der Verwendung von Blacklist-Regeln

Bitte beachten Sie, dass das Deaktivieren von Programmdateien manchmal dazu führt, dass bestimmte Programme nicht mehr korrekt funktionieren. Das Ausschalten bestimmter Dateien (insbesondere von DLLs und Treibern) sollte mit größter Vorsicht erfolgen. Wir empfehlen ausdrücklich die Stabilität der Systeme über Referenz- und Testsysteme vorab zu verifizieren, bevor Regeln der Blacklist auf Produktiv-Systeme gespielt werden.

Empfehlungen für die [BLACKLIST]

Wir haben für unsere Kunden eine Blacklistempfehlung zusammengestellt. Die aufgelisteten Anwendungen und Pfade werden häufig dazu genutzt, Schadcode auf Rechnern zu installieren und stellen damit ein potenzielles Risiko dar. Wenn Sie diese Anwendungen nicht zwingend für den täglichen Betrieb benötigen, setzen Sie sie auf die Blacklist. Für die Liste besteht kein Anspruch auf Vollständigkeit, Nutzung auf eigene Gefahr. Bei Rückfragen stehen wir unseren Kunden gerne zur Verfügung. Eine aktuelle Version der Blacklist finden Sie unter: https://excubits.com/content/files/blacklist.txt

Leise Regeln (Silent Rules)

Da Türsteher jedes von der Konfiguration abweichende Ereignis in die Logdatei schreibt, kann dies in manchen Situationen stören. Zum Beispiel, wenn Sie Systemkomponenten des Betriebssystems bewusst blockieren möchten, Sie dies aber systembedingt nicht deaktivieren können. Angenommen Sie möchten das Programm `notepad.exe` dauerhaft verbieten, aber nicht bei jedem Versuch es zu starten eine Meldung in die Logdatei schreiben. Mit Silent Rules, den sog. leisen Regeln, verhindern Sie dies. Die Leisen Regeln werden durch das Dollarzeichen **`$`** am Anfang der Regelzeile definiert:

```
[BLACKLIST]
$*notepad.exe
```

Diese beispielhafte Regel besagt, dass `notepad.exe` blockiert werden soll und dass kein Eintrag in die Logdatei geschrieben werden soll. Falls Notepad startet, wird dies von Türsteher blockiert, ohne einen Eintrag in die Logdatei zu schreiben.

Hinweis!

Leise Regeln können nur in den Blacklist-Bereichen [`BLACKLIST`] und [`CMDBLACKLIST`] angewendet werden.

Parentchecking: Bedingte Regeln für Eltern-Prozesse

Türsteher unterstützt in der [WHITELIST] und [BLACKLIST] auch bedingte Regeln für Eltern-Prozesse. Es gibt Programme, die nach dem Start des Hauptprogramms je nach Bedarf Unterprogramme starten. Wir nennen das Hauptprogramm den Vaterprozess, die nachfolgenden Unterprogramme Kindsprozesse. Dass Vaterprozesse Unterprogramme, also Kindsprozesse, starten, ist bei Programmen wie dem Explorer notwendig und sinnvoll. Doch Hacker nutzen diese Möglichkeit aus, um eigene schädliche Programme zu starten und Computer zu infizieren. Sie verschicken beispielsweise Word- oder PDF-Dateien mit schädlichen Programmen „im Gepäck", die dann von Word oder dem PDF-Reader gestartet werden. Um diese Art des Angriffs zu verhindern, haben wir Parentchecking entwickelt.

Beim Parentchecking gleicht Türsteher vor Ausführung des Vaterprozesses ab, welche Kindsprozesse dieser starten möchte. Ist der jeweilige Vaterprozess in der Whitelist, darf auch der Kindsprozess starten, andernfalls wird er blockiert. So kann man beispielsweise definieren, dass Word oder ein PDF-Reader keine Prozesse, Shellcodes, Laufzeitbibliotheken oder Treiberdateien (`.dll, .sys, .ocx, .drv, .cpl`) ausführen dürfen. Selbst Shellkommandos lassen sich einschränken und typische Exploit-Commandlets per Regel deaktivieren.

Die Regeln für das Parentchecking haben dabei folgendes allgemeines Format:

```
Pfad/Dateiname Vater>Pfad/Dateiname Kind
```

Bitte beachten Sie, dass der Pfad/Dateiname durch das Symbol **>** getrennt ist und dazwischen **kein** Leerzeichen stehen darf. Türsteher unterstützt auch hier die Wildcards (Platzhaltersymbole * und ?) auch alle Unicode-Zeichen, wie:

```
C:\مُرَحَبا\rалдёж\x.exe>C:\Windows\*.dll
```

Hinweis!

Wenn man Parent-Regeln und normale Regeln in Türsteher gleichzeitig verwenden möchte, muss man die korrekte Reihenfolge beachten: Denn die erste treffende Regel greift! Setzen Sie die wichtigste Regel an die erste Stelle, alle weiteren folgend.

Beispiele für die Parent-Regeln in der [WHITELIST]

Parent-Regeln für die Whitelist könnten folgendermaßen aussehen:

```
!*MicrosoftEdge.exe>*MicrosoftEdge.exe
!*microsoftedgecp.exe>*microsoftedgecp.exe
```

Diese beiden Regeln besagen, dass der Microsoft Edge Browser nur sich selbst und den sogenannten Microsoft Edge Content Process starten darf. Mit einer Blacklist-Regel sollten Sie dann einschränken, dass Edge selbst keine anderen Prozesse starten darf.

Die folgenden drei Regeln erlauben Microsoft Word nur Prozesse aus Systemordnern zu starten:

```
*\Office1*\WINWORD*.EXE>?:\Windows\*
*\Office1*\WINWORD*.EXE>?:\Program Files\*
*\Office1*\WINWORD*.EXE>?:\Program Files (86)\*
```

Mit diesen folgenden zwei Regeln wird das benutzerspezifische Programm Thonny für den Anwenderordner `C:\Users\Escubits\...` erlaubt:

```
!C:\Users\Excubits\AppData\Local\Programs\Thonny\*>C:\Users\Excubits
\AppData\Local\Programs\Thonny\*
!C:\Users\Excubits\AppData\Local\Programs\Thonny\*>C:\Users\Excubits
\.thonny\*
```

Beispiele für die Parent-Regeln in der [BLACKLIST]

Parent-Regeln für die Blacklist könnten wie folgt aussehen:

```
[BLACKLIST]
*iexplore.exe>*cmd.exe
*iexplore.exe>*powershell.exe
*chrome.exe>*bitsadmin.exe
*firefox.exe>cmd.exe
*flash*>cmd.exe
*flash*>powershell.exe
*flash*>*script*.exe
*flash*>*bitsadmin.exe
*flash*>C:\Users\*
```

Die ersten vier Regeln zeigen Anwendungen, die in der Praxis sehr häufig bei Angriffen auf Browser ausgenutzt werden. Die erste Regel gibt zum Beispiel an, dass der Internet Explorer keine `cmd.exe`-Shell starten darf. Die zweite Regel gibt an, dass der Internet Explorer den Interpreter `powershell.exe` nicht ausführen darf. Die dritte Regel gibt an, dass der Chrome Browser die Anwendung `bitsadmin.exe` nicht starten darf. Die vierte Regel hindert Firefox daran, den Kommandozeilen-Interpreter (`cmd.exe`) zu starten. Die letzten Regeln verhindern, dass das sehr häufig für Angriffe ausgenutzte Adobe Flash Plug-in sicherheitskritische Systemtools starten kann.

Programme können vielfach auch diverse Laufzeitbibliotheken laden. Angreifer können das Nachladen bestimmter DLLs ausnutzen, um schädlichen Code auf dem Rechner zu starten. Wenn Sie verhindern wollen, dass Anwendungen DLLs aus Benutzerverzeichnissen laden können, nutzen Sie folgende Regel für die Blacklist:

```
C:\Windows\*.exe>C:\Users\*.dll
```

CMD-Check/ Kommandozeilen-Prüfung

Mit der Kommandozeilen-Regelprüfung können Sie angeben, mit welcher Kommandozeile bestimmte Anwendungen gestartet werden dürfen und mit welchen nicht. Dies ist besonders zum Blockieren oder Freischalten von sog.

Skript-Interpretern hilfreich, denn die vom jeweiligen Interpreter geladenen Skripte werden über Kommandozeilen-Parameter übergeben. Ruft man beispielsweise eine JS-Datei mit dem Explorer auf, wird der Pfad und Dateiname an den Skript-Interpreter (`wscript.exe`) weitergereicht. Mit CMD-Check können Sie bestimmen, welche Pfade und Dateien an den Skript-Interpreter weitergereicht werden dürfen und welche nicht. Wir empfehlen, nur die eigenen Skripte zu erlauben und alle anderen strikt zu blockieren. Dies sichert Ihre IT und hilft insbesondere VB, JS und JAVA-Anwendungen sicherer auszuführen als bisher.

Kommandozeilen-Whitelist konfigurieren

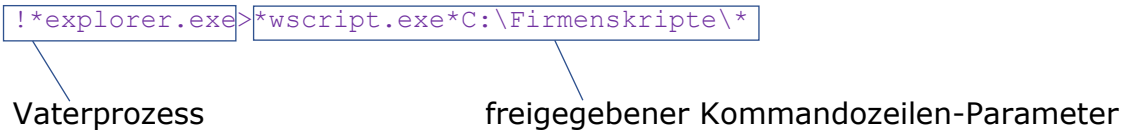
Im Bereich der Kommandozeilen-Whitelist konfigurieren Sie die Kommandozeilen, die Sie freigeben möchten. Wollen Sie die Kommandozeilen-Regelprüfung aktivieren, müssen Sie sie mit [`CMDCHECK`] aktivieren und zwingend die [`CMDWHITELIST`] konfigurieren.

Beispiel für Kommandozeilen-Whitelist

```
[CMDWHITELIST]
!*explorer.exe>*wscript.exe*C:\Firmenskripte\*
*>*

[CMDBLACKLIST]
*>*wscript.exe*
```

Das Ausrufezeichen zu Beginn der Kommandozeilen-Whitelist definiert eine Prioritätsregel. Sie ist notwendig, da in der Kommandozeilen-Blacklist eine strenge Regel alle Skripte des `wscript.exe`-Interpreters verbietet. Das Programm `wscript.exe` darf nach der Regel nur Skripte aus dem Verzeichnis `C:\Firmenskripte\*` öffnen. Und das auch nur über den Windows Explorer. Nur in dieser Kombination kann man nun `wscript.exe` starten. Microsoft Word oder der Internet Explorer können `wscript.exe` nicht ausführen. Selbst dann nicht, um Skripte aus dem Verzeichnis `C:\Firmenscripte\*` zu starten.



Der Eintrag vor `>` definiert den Vaterprozess. Der Eintrag nach `>` definiert den freigegebenen Kommandozeilen-Parameter.

Kommandozeilen-Regeln können teilweise sehr komplex werden. Wir unterstützen und beraten unsere Kunden gerne bei der Erstellung solcher Regeln.

Kommandozeilen-Blacklist konfigurieren

Im Bereich der Kommandozeilen-Blacklist konfigurieren Sie die Kommandozeilen, die Sie blockieren möchten. Wollen Sie diese Funktion aktivieren, müssen Sie dies mittels der Zeile [CMDCHECK] tun. Anschließend **müssen Sie** auch die [CMDBLACKLIST] konfigurieren.

Beispiel für eine CMDCHECK-Regel:

```
[CMDBLACKLIST]
*>*wscript.exe*
```

Im gezeigten Beispiel wurde eine Regel definiert, die wscript.exe für sämtliche Aufrufe blockiert. Der erste * definiert jeden möglichen Prozess. *wscript.exe* definiert den Kommandozeilen-Parameter. Sämtliche Kombinationen von wscript.exe und Kommandos an diesen Prozess werden nun blockiert. Mit dieser Regel können Sie sicherstellen, dass kein Vaterprozess wscript.exe mit irgendeinem Kommandozeilen-Parameter starten kann.

Das gezeigte Beispiel kann insbesondere vor Kryptolockern schützen, die in letzter Zeit vermehrt als JS-Skripte per E-Mail versandt werden.

Hinweis!

Da im Bereich kleiner- und mittelständiger Betriebe häufig Skripte ausgeführt werden müssen, kann der Skriptinghost nicht einfach auf die Blacklist gesetzt werden. Hier können Kommandozeilen-White- und -Blacklists für mehr Sicherheit sorgen, indem genau definiert wird, welche Skriptdateien ausgeführt werden können. So sollten insbesondere Skripte aus temporären Ordern oder von externen Datenträgern standardmäßig auf die Blacklist gesetzt werden. Denn Cyberkriminelle nutzen diesen Weg häufig für Angriffe.

Ende der Konfiguration

Die Konfigurationsdatei muss stets mit folgender Zeile beendet werden:

[EOF]

Hinweis!

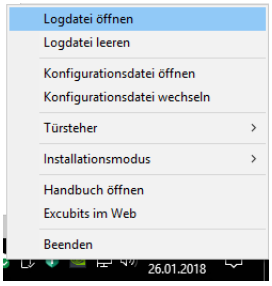
Bitte beachten Sie, dass Türsteher die Konfigurationsdatei nicht akzeptiert und den Treiber nicht lädt, wenn diese nicht mit [EOF] abgeschlossen wird.

Türsteher für den ersten Start vorbereiten / Simulationsmodus

Wenn Sie Türsteher nach Ihren Vorstellungen angepasst und konfiguriert haben, können Sie den ersten Start vorbereiten. Am besten Sie nutzen dazu den **Simulationsmodus**, denn damit können Sie leicht prüfen, wie sich Türsteher im

echten Betrieb verhalten wird. Gleichzeitig verhindern Sie, dass Ihr System abstürzt oder schwere Probleme entstehen, wenn Sie vielleicht eine Regel vergessen haben. Für den Simulationsmodus schalten Sie das Logging ein und den lethalen Modus aus:

`[#LETHAL]` = (Zeile mit Hashtag bedeutet ausgeschaltet)
`[LOGGING]` = (Zeile ohne Hashtag bedeutet angeschaltet)



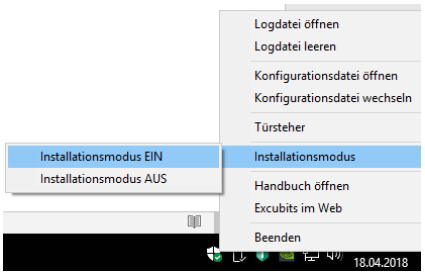
Haben Sie den Simulationsmodus aktiviert, können Sie den Rechner neu starten. Nach dem Neustart schreibt Türsteher nun jedes von der Konfiguration abweichende Verhalten in die Logdatei, jedoch im Simulationsmoduls noch **ohne es zu blockieren**. Haben Sie alles korrekt konfiguriert, sollten keine Meldungen in der Logdatei (`tuersteher.log`) auftauchen. Prüfen Sie nun im Simulationsmodus ausgiebig das Verhalten von Türsteher und Ihren Anwendungen. Denken Sie an den Neustart von Türsteher, damit alle Änderungen übernommen werden. Diese Arbeitsschritte sollten Sie nun so lange durchführen, bis Türsteher keine Einträge in die Logdatei schreibt.

Sobald Sie mit den gesetzten Regeln zufrieden sind, können Sie den Simulations-modus ausschalten. Setzen Sie dafür folgende Zeile in der Konfigurationsdatei:

`[LETHAL]` = angeschaltet

Nun müssen Sie Türsteher nur noch neu starten, damit die Änderungen in der Konfigurationsdatei übernommen werden. Türsteher ist nun voll aktiv. Programmdateien außerhalb der zugelassenen Pfade können nicht mehr gestartet werden, da diese von Türsteher blockiert werden. Sollten Sie das Logging aktiviert haben, schreibt Türsteher jedes Ereignis in die Logdatei.

Installationsmodus



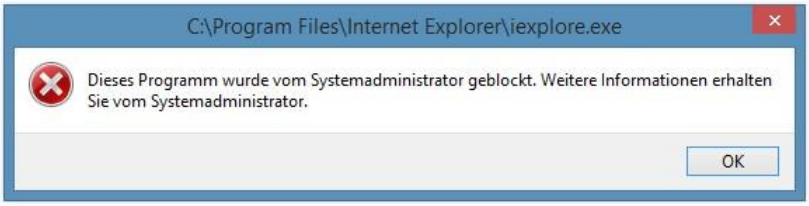
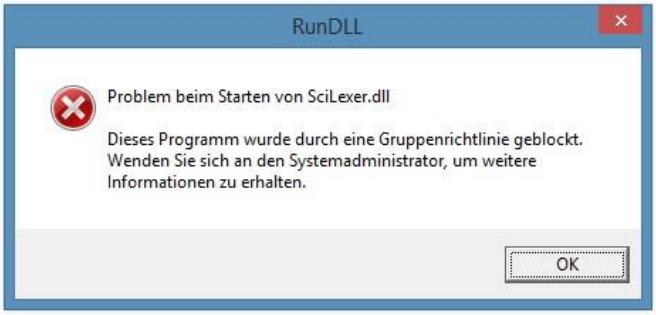
Sie wollen ein Windows-Update einspielen oder ein neues Programm auf `C:\` installieren? Nutzen Sie dazu den Installationsmodus. Windows kann für das Update alle Verzeichnisse nutzen und auch während der Computer hochfährt, kann das Windows-Update Änderungen am System vornehmen.

Vergessen Sie nicht, den Installationsmodus nach der Installation wieder zu deaktivieren.

Hinweis!

Im Installations-Modus schützt Türsteher nicht, es können sämtliche ausführbaren Programme ausgeführt werden. Die Tray-Anwendung zeigt dann jede halbe Stunde eine Warnmeldung an. Diese erinnert Sie, dass Türsteher noch im Installationsmodus ist.

Ereignismeldungen

Meldung	Bedeutung
	Diese Meldung wird angezeigt, wenn beispielsweise der Internet Explorer auf der Blacklist von Türsteher steht und von Türsteher blockiert wurde.
	Wenn eine Anwendung versucht, eine DLL aus einem nicht freigegebenen Ordner auszuführen, sehen Sie z. B. diese Meldung.

Hilfsprogramme (Tools)

Türsteher läuft vollständig unabhängig im Kern des Betriebssystems und benötigt keine Anwendung zur Steuerung. Für eine leichtere Konfiguration und für den Betrieb von Türsteher werden zwei Hilfsprogramme mitgeliefert. Die Anwendungen sind optional und müssen weder installiert noch benutzt werden, Türsteher funktioniert auch ohne diese Tools.

Anwendung für den Tray-Bereich

Die Türsteher Tray (`TuersteherTray.exe`) finden Sie nach der Installation im Tray-Bereich der Windows Taskleiste, unten rechts. Sie erkennen Türsteher an einem T-Symbol in unterschiedlichen Farben:

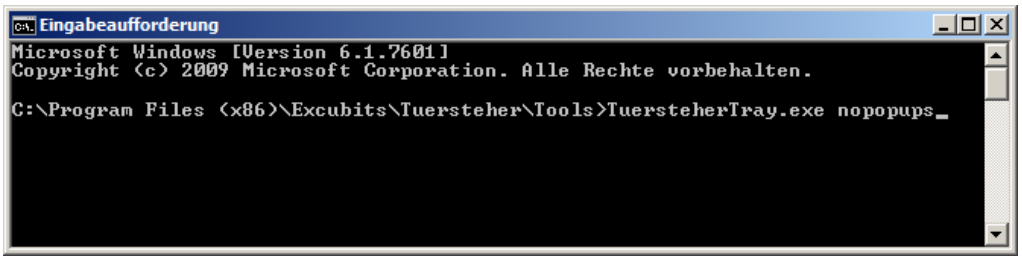
Die aktive Tray-Anwendung prüft, ob sich die Türsteher-Logdatei verändert.

Unterschiedliche Farben für unterschiedliche Modi

Zeichen	Bedeutung
	Ist Türsteher aktiv und es wurden keine Gefahren erkannt, ist das T-Symbol grün.
	Wenn Türsteher eine ausführbare Datei blockiert, färbt sich das Symbol rot. Zudem zeigt die Anwendung in einer Sprechblase an, welche Datei(en) blockiert wurde(n) und schreibt diese Information auch in das Windows Event-Log.
	Wurde Türsteher in den Installations-Modus geschaltet, färbt sich das T-Symbol gelb.
	Ist Türsteher nicht aktiv, so ist das T-Symbol grau. Die Tray-Anwendung zeigt dann jede halbe Stunde eine Warnmeldung an. Diese weist Sie darauf hin, dass Türsteher nicht aktiv ist und kein Schutz besteht.
	Befindet sich Türsteher im Simulationsmodus, ist das Icon blau. Im Simulationsmodus schützt Türsteher nicht, es können sämtliche ausführbaren Programme gestartet werden.

Warnmeldungen der Tray-Anwendung abschalten

Wenn Sie keine Warnmeldungen der Tray-Anwendung angezeigt bekommen möchten, können Sie die Anwendung mit der Kommandozeilen-Option `nopopups` starten, dann werden alle sog. Tooltips unterdrückt. Dazu müssen Sie die Tray-Anwendung wie folgt starten: `TuersteherTray.exe nopopups`.

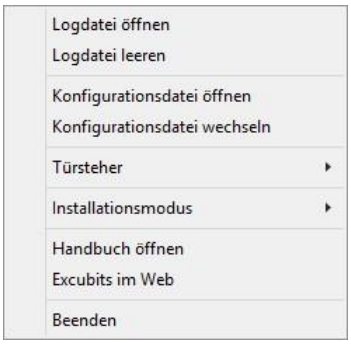


Bei Alarm E-Mail an den Administrator

Daneben besteht die Möglichkeit eigene Anwendungen für Türsteher zu entwickeln. So kann zur Alarmierung auch eine E-Mail an den Administrator oder IT-Sicherheitsbeauftragten gesendet werden, SMS-Meldungen sind ebenfalls machbar. Neben dem Windows-eigenen EventLog können auch andere zentrale Logging-Dienste wie z.B. SNMP Traps versandt werden.

Gerne programmiert Excubits UG die für Sie passende Lösung. Bei Interesse schreiben Sie uns, wir machen Ihnen gerne ein individuelles Angebot.

Steuerung im laufenden Betrieb



Durch einen Klick auf das T-Symbol kann ein Menü geöffnet werden. Dieses bietet die Möglichkeit, die Logdatei zu öffnen oder zu leeren, die Datei mit den Regeln zu öffnen oder zu tauschen, den Treiber zu starten oder zu stoppen sowie die Tray-Anwendung zu beenden. Zudem können Sie auch jederzeit dieses Handbuch öffnen und unsere Webseite besuchen.

Hinweis!

Um den Treiber zu starten oder zu stoppen, werden stets Administratorrechte benötigt.

Technischer Hintergrund

Türsteher implementiert technisch gesehen einen sog. Minifilter (Treiber), der vollständig autark im Kern des Betriebssystems läuft. Dadurch arbeitet Türsteher an zentraler Stelle, sozusagen im Herzen des Betriebssystems. Über definierte Regeln bestimmen Sie als Anwender, wann Türsteher aktiv wird und auszuführenden Programmcode blockiert. Da Türsteher im Kern des Betriebssystems arbeitet, kann er sehr früh eingreifen und von typischen Schadprogrammen nicht ohne Weiteres umgangen werden. Ein Schadprogramm müsste erst selbst in den Kern von Windows gelangen oder Türsteher mittels System- oder Administrator-Rechten deaktivieren. Beides ist normalerweise nicht möglich und erfordert vom Angreifer sehr viel Fachwissen und/oder schwere Sicherheitslücken im Betriebssystem.

Schutz durch Whitelisting

Türsteher erkennt sämtliche Programme, die mit dem Betriebssystemlader in den Arbeitsspeicher geladen werden sollen, dies sind die bekannten EXE-Dateien, aber auch Bildschirmschoner (SRC), Laufzeitbibliotheken (DLLs), Treiber (SYS, DRV) oder Plug-ins (OCX, DLL). Dabei spielt die Dateiendung aber keine Rolle, selbst wenn sich eine ausführbare Programmdatei beispielsweise mit der Dateiendung `.jpg` als Bild tarnt, erkennt Türsteher die ausführbare Programm-

datei und kann diese blockieren. Türsteher verhindert so, dass versehentlich angeklickte bösartige Programmdateien von USB-Sticks, externen Festplatten, Netzlaufwerken, CD-/DVD-ROMs oder E-Mail-Anhängen ausgeführt werden können. Schadprogramme, die durch Sicherheitslücken auf Ihren PC gelangen können, werden von Türsteher ebenso blockiert, wie unbeabsichtigt heruntergeladene Programme aus dem Internet. Das von Türsteher implementierte Whitelisting-Schutzsystem schützt Ihren PC damit proaktiv vor Viren, Würmern, Ransomware, Crypto-Lockern u. v. w.

Schutz ohne ständige Rückfragen

Türsteher arbeitet autark und ist nicht von Entscheidungen des Anwenders abhängig. Türsteher fragt den Anwender niemals nach einer sicherheitsrelevanten Entscheidung, sondern entscheidet selbst. Entgegen vielen anderen Sicherheitsprodukten, wie Anti-Viren-Scannern oder Desktop-Firewalls belästigt Türsteher den Anwender nicht oder nötigt ihm gar eine Entscheidung ab. In der Folge entscheidet Türsteher immer richtig und blockiert Programmdateien.

Schutz zum frühestmöglichen Zeitpunkt

Der Treiber von Türsteher startet zu einem sehr frühen Zeitpunkt des Bootvorgangs und ist damit in der Lage Ihr System bereits während des Hochfahrens des Betriebssystems zu schützen. Sie können dadurch genau bestimmen, mit welchen Treibern Ihr Windows starten darf.

Generelle Empfehlungen

Türsteher kann Sie vor jeglichen ausführbaren Dateien schützen. Normalerweise bräuchten Sie dadurch keine weiteren Schutzsysteme. Doch benutzen leider nicht alle Windows-Anwender Türsteher. Deswegen ist es im Interesse der Allgemeinheit, zusätzlich zu Türsteher ein Antivirusprogramm und eine Firewall zu nutzen. So können Sie verhindern, dass gefährliche Programme, die bei Ihnen durch Türsteher nicht gestartet werden können, (versehentlich) an andere Menschen verteilt werden.

System und Programme immer aktuell halten

Sie sollten zudem stets sämtliche Aktualisierungen und Service Packs für Ihr Betriebssystem sowie alle installierten Programme einspielen. Dies gilt insbesondere für alle mit dem Internet genutzten Anwendungen wie Browser, Plug-ins (z. B. Flash, PDF-Plug-ins, Java, .NET oder Silverlight) etc.

Administratorenrechte nicht dauerhaft benutzen

Der Rechner sollte nicht dauerhaft mit Administrator-Benutzerrechten genutzt werden. Für den alltäglichen Betrieb ist es ratsam, ein Benutzerkonto mit Standard-Benutzerrechten oder eingeschränkten Benutzerrechten anzulegen und mit diesem Benutzerkonto zu arbeiten. Nach Möglichkeit sollten Sie einen Browser verwenden, der über Sandbox-Technologie verfügt. Dadurch reduzieren Sie die Gefahr, dass Sicherheitslücken ausgenutzt werden können. Google

Chrome und die aktuelle Version des Internet Explorers haben eine integrierte Sandbox-Technologie.

Online-Glossar für IT-Sicherheitsinteressierte

Wenn Sie mehr über Angriffsmethoden, Begrifflichkeiten und Definitionen im Bereich IT-Sicherheit wissen möchten, empfehlen wir unser Online-Glossar:

https://excubits.com/content/de/glossar.html

Zeichenerklärung / Sonderzeichen

Sonderzeichen	Stichwort	Bedeutung
#	Deaktivieren	ausgeschaltet
?	Platzhaltersymbol / Wildcard	Zeichen für exakt ein beliebiges Zeichen
*	Platzhaltersymbol / Wildcard	Zeichen für beliebige Anzahl von Zeichnen
!	Prioritätsregeln	Regeln mit Ausrufezeichen **(!)** haben Vorrang gegenüber anderen Regeln.
$	Silent Rules	Regeln mit Dollarzeichen **($)** am Anfang erzeugen keine Logeinträge, obwohl Türsteher diese Dateien blockiert.
>	Parentchecking	Trennzeichen zwischen Vater- und Kindsprozess beim Parentchecking. Kein Leerzeichen dazwischen: `C:\مُرَحَبا\галдёж\x.exe>C:\Windows\*.dll`

Stichwortverzeichnis

Aktivieren und deaktivieren 4, 5
Änderungen übernehmen 4, 15
Blacklist 7, 8, 9, 10, 12, 13, 14
CMD-Check 13
Deinstallation 2, 3
Eltern-Prozesse 11
Ereignismeldungen 16
Hashing 5, 8
Installationsmodus 15
Kommandozeilen 1, 5, 7, 12, 13, 14
Konfigurationsdatei 2, 3, 4, 14, 15
Leise Regeln 10
Logdatei 2, 5, 10, 15, 16, 18
Neustart 4, 15
Parentchecking 11
Parent-Regeln 11, 12
Prioritätsregeln 7
Sicherheitslücke 9
Silent Rules 10
Simulationsmodus 14, 15
Systemanforderungen 2
Tray-Anwendung 3, 15, 16, 17, 18
Tray-Bereich 16
Unicode 3, 11
Warnmeldungen 17
Whitelist 5, 6, 7, 8, 11, 13
Wildcard 4, 6, 7, 11
Windows-Update 15
Zeichenerklärung / Sonderzeichen 20