FAQ

c't-Notfall-Windows 2024

Unser Bausatz in c't 2/2024 erstellt ein Notfallsystem, das vom USB-Stick startet. Durch externe Einflussfaktoren, etwa nicht erreichbare Server, übergriffige Sicherheitssoftware und schlicht durch die Vielzahl möglicher Optionen und Erweiterungen aktueller Windows-Versionen gelingt das nicht auf jedem PC im ersten Anlauf. Die wichtigsten Hinweise und Kniffe aus mehreren Wochen Support haben wir hier zusammengestellt.

Von Peter Siering

Bluescreens bei allen Virenscannern

Bei mir stoppt das Notfall-Windows mit einem Bluescreen, egal welchen Virenscanner ich starte. Was läuft falsch?

Wir haben eine „Selbstverständlichkeit“ in den Artikeln leider nicht thematisiert: Wir lassen bei den Tests die Scanner im Wesentlichen auf die in einem PC vorhandenen Partitionen los und schaltet den Scan auf den Laufwerken des Notfallsystems aus (B:, X:, Y:). Die Scanner scheinen es nicht zu vertragen, wenn sie auf die Laufwerke des Notfallsystems losgelassen werden und das führt im Extremfall wohl auch zu Bluescreens.

In jedem Fall aber liefern sie Fehlalarme wegen einiger Werkzeuge im Notfallsystem. Insofern: Bitte die Scanner nicht auf die genannten Laufwerke loslassen. Hintergrund zu den Fehlalarmen: Im Notfallsystem stecken Werkzeuge, die im Ernstfall sehr nützlich sein können, die aber Virenscanner alarmieren lassen. Das liegt unter anderem daran, dass Kriminelle einige dieser Werkzeuge für Angriffe missbrauchen. Wir untersuchen sämtliche Dateien jedes Jahr akribisch und veröffentlichen Fehlalarme nebst Erklärungen auf der Projektseite (siehe ct.de/ydfz).

Notfallsystem nach Bauen testen

Kann ich vor dem Beschreiben eines USB-Sticks das erzeugte Notfallsystem ausprobieren?

Um sicherzustellen, dass beim Bau des Notfallsystems ein lauffähiges Exemplar entstanden ist, starten Sie die ISO-Datei aus dem Unterverzeichnis Output in einer Virtualisierungsumgebung. Es genügt, wenn Sie die ISO-Datei dort als Bootmedium einbinden. Wenn die Menüs belebt sind und das System grundsätzlich bedienbar ist, hat der eigentliche Bauvorgang geklappt. Berücksichtigen Sie bitte, dass manche der enthaltenen Programme nur dann korrekt funktionieren, wenn Sie das System von einem USB-Stick oder anderen beschreibbaren Medien starten.

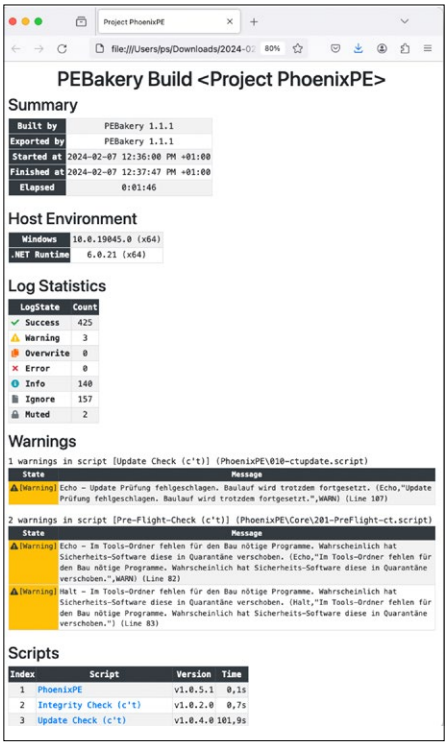
Alle Bauversuche brechen ab

Ich habe mehrere Anläufe genommen, um das Notfallsystem zu bauen, scheitere aber immer wieder an Fehlermeldungen. Was kann ich versuchen?

Das kommt sehr darauf an, was schiefläuft. Lesen Sie die Fehlermeldungen, die der Bausatz in der Regel anzeigt. Nehmen Sie die Meldung ernst, etwa wenn die von einem weiterhin aktiven Virenschutzprogramm spricht oder andere Anomalien des Bau-PCs bekrittelt. Der Bausatz prüft wichtige Voraussetzungen, die nach unseren Support-Erfahrungen kritisch sind und einen erfolgreichen Baulauf verhindern werden.

Es lohnt sich, einen Blick in die Log-Dateien zu werfen: Die im Browser angezeigte Variante lädt zwar zäh, erlaubt aber mit einem Klick direkt an die Stelle zu springen, an der Warnungen oder Fehler auftraten. Halten Sie zu Beginn des Logs Ausschau nach rot oder orange gefärbten Zeilen. Klicken Sie auf diese verlinkten Zeilen. Wenn Sie dann ein wenig hochrollen, sehen Sie die letzten Befehle, die vor dem eigentlichen Fehler ausgeführt wurden. In vielen Fällen sind das fehlgeschlagene Downloads. Wie die Artikel empfehlen, genügt es, mit zeitlichem Abstand den Baulauf erneut zu starten.

War es keine temporäre Störung aufseiten der Download-Quelle, sondern etwa ein Update, durch das sich die Download-URL verändert hat, warten Sie einfach einen Tag: Wir beobachten automatisiert die vom Bausatz frequentierten Quellen und korrigieren die Skripte zeit-



Die von PEBakery erstellten Logs sind in der HTML-Variante besonders praktisch: Sie laden je nach Größe zwar etwas zäh, erlauben es im Browser aber, direkt zu Fehlerstellen zu springen. Halten Sie Ausschau nach zu Beginn gelb oder rot dargestellten Warnungen oder Fehlern. Ein Klick auf [Warning] oder [Error] genügt dann.

nah durch ein Update. Erfahrene Nutzer können auch selbst die Skripte bearbeiten und die URL anpassen. Die angesteuerte URL findet sich in den Logs.

Häufig ist aber auch Sicherheitssoftware für Download-Probleme verantwortlich. Proxys, die Downloads auf Schadsoftware untersuchen, stecken in vielen Sicherheitspaketen und geben sich nur selten zu erkennen. Prüfen Sie unbedingt, ob solche Software auf Ihrem PC aktiv ist; schauen Sie in dessen Protokolle, um eventuelle Interventionen zu erkennen. Im Zweifel hilft vorübergehendes Deaktivieren. Auch ein Werbefilter wie Pi-hole könnte je nach verwendeten Filterlisten Downloads behindern. Entsprechend gilt: Schauen Sie auch in dessen Protokolle.

Sollte PEBakery selbst mit einem Fehler (Stacktrace) aussteigen, ohne ein Log zu schreiben, hat es in den meisten Fällen geholfen, ein anderes Laufwerk für das Bauverzeichnis auszuwählen. Auch haben wir vereinzelt von PCs gehört, bei denen ein Windows-Updatestau den Bau behinderte; im Zweifelsfall ist es stets eine gute Idee, einen Windows-PC vor einem Bauversuch neu starten zu lassen, damit er eventuell halbfertige Updates verarbeitet. Letztlich bleibt immer auch eine Mail an uns, am besten an ctnotwin24@ct.de, gern mit Log-Dateien und Screenshots der Fehler.

USB-Sticks starten nicht

Das Bauen und Überspielen des Notfallsystems hat anscheinend tadellos geklappt, aber es startet nicht von meinem USB-Stick oder bricht währenddessen ab. Was kann ich tun?

Bei hartnäckigen Problemen empfehlen wir, das Bauergebnis sicherheitshalber zu prüfen, wie in „Notfallsystem nach Bauen testen“ beschrieben. Häufige Ursache für Startprobleme sind USB-Sticks von zweifelhafter Qualität oder bereits stark beanspruchte Exemplare. Probieren Sie unbedingt einen anderen Stick, idealerweise anderer Provenienz. Wir hören auch immer wieder davon, dass es auch auf die verwendeten USB-Ports eines PCs ankommt, an einem geht es, an einem anderen nicht. Gelegentlich spielt auch die Art der Datenträgereinbindung eine Rolle: manche PCs unterscheiden zwischen USB-Floppy und -Harddisk – probieren Sie beides aus. Weitere Tipps finden Sie in unserer USB-Boot-FAQ (via ct.de/ydfz).

Integritätsprüfung fehlgeschlagen

Bei mir startet der Bauprozess nicht. Stets erhalte ich den Hinweis, die Integritätsprüfung sei fehlgeschlagen. Ich habe die md5-Summen mehrfach überprüft.

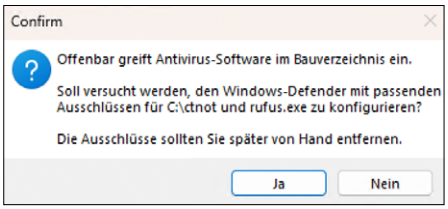
Wenn die initiale Integritätsprüfung fehlschlägt, liegt das daran, dass sie Dateien oder Verzeichnisse im Bauverzeichnis findet, die sie nicht erwartet. Die Prüfung ist uns leider etwas zu pingelig geraten. Entschuldigen Sie bitte, dass wir das nicht besser dokumentiert haben.

Im Bauverzeichnis c:\ctnot (oder ähnlich) sollten nur *.iso-Dateien und ctnotwin24*.zip-Archive liegen und auch keine Unterverzeichnisse angelegt sein. Wenn Sie dann das ctnotwin24.zip dort entpacken, wird die Integritätsprüfung nichts zu meckern haben und der Baulauf beginnen.

Ist die Prüfung einmal für den entpackten Bausatz erfolgreich, findet keine weitere statt. Sie können sie abschalten, indem Sie in PEBakery links im Baum das Skript „Integrity Check (c't)“ anklicken und rechts den Haken vor „Integritätsprüfung überspringen“ setzen oder nach dem Entpacken die Datei „md5“ im Hauptverzeichnis des Bauordners löschen.

Virenscanner abgeschaltet, aber Abbruch

Ich habe, wie empfohlen, meinem Virenscanner verboten, das Bauverzeichnis zu überwachen, trotzdem bricht der Bauprozess mit der Meldung ab „Could not create testfile (Echo,„Could not create testfile“,WARN)“. Was läuft falsch?



Der Bausatz prüft, ob Sicherheitssoftware aktiv ist, und kann Ausnahmen nur für den Windows-Defender setzen. Nehmen Sie solche Meldungen unbedingt ernst, besonders wenn sie noch nach dem Setzen von Ausnahmen weiter auftreten.

Wenn diese Meldung erscheint, ist im Bauverzeichnis weiterhin Schutzsoftware aktiv. Der Bausatz schreibt eine Eicar-Testdatei, die per Konvention von Virenschutzsoftware erkannt wird. Die genannte Meldung tritt nur dann auf. Wenn es partout nicht gelingt, dem Schutz eine Ausnahmeregel für den Bau beizubiegen, hilft es vielleicht, die Software vorübergehend anzuhalten. Hinweise zum Setzen von Ausnahmen entnehmen Sie bitte der Dokumentation der eingesetzten Schutzsoftware. Wir kennen nicht alle dieser Programme (dafür gibt es zu viele) und können daher nicht mit Bedientipps aushelfen.

ISO-Datei als Laufwerk bereitstellen

Alle Tipps im Artikel zum Einbinden der heruntergeladenen ISO-Datei als Laufwerk scheitern. Was kann ich tun?

Sie können eine ISO-Datei auch aus der Powershell heraus als Laufwerk einbinden. Rufen Sie dazu den folgenden Befehl angepasst an den Pfad und Namen Ihrer ISO-Datei auf:

```
Mount-DiskImage -imagepath ↵
↳ "C:\mein.iso" | Get-Volume
```

Wenn Sie das Laufwerk später wieder loswerden wollen, hilft der folgende Befehl:

```
DisMount-DiskImage  ↵
↳ -imagepath "C:\mein.iso"
```

PEBakery wird nicht gefunden

Ich habe die Anleitung befolgt, alles heruntergeladen und entpackt. Nach dem Aufruf von PEBakeryLauncher.exe habe ich die .NET-Runtime wie empfohlen installieren lassen. Jetzt findet PEBakeryLauncher.exe aber PEBakery.exe nicht. Was mache ich falsch?

Vermutlich haben Sie das Zip-Archiv unseres Bausatzes mit ungeeigneten Mitteln entpackt. Wir hören das häufiger von Lesern, die Dateimanager zum Entpacken von Zip-Archiven einsetzen. Ver-

wenden Sie idealerweise die Windows-Bordmittel zum Entpacken: Öffnen Sie das Zip-Archiv also mit dem Explorer, markieren Sie die enthaltenen Dateien und kopieren Sie diese über die Zwischenablage in das zum Bauen erstellte Verzeichnis, etwa c:\ctnot. Unsere Integritätsprüfung (siehe Frage weiter oben) läuft leider zu spät an, um solche Entpackfehler erkennen und davor warnen zu können.

Programmupdates

Wenn ich das Notfallsystem boote und darin Programme starte, weisen die von sich aus auf verfügbare Updates hin. Folge ich den Updateangeboten, erfolgen zwar Downloads, aber die Programme sind spätestens nach einem Reboot wieder auf dem alten Stand. Was kann ich tun?

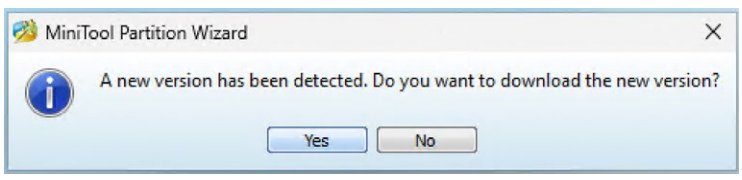
Am besten tun Sie gar nichts und ignorieren diese Hinweise auf Updates – mit einer Ausnahme: Die eingebauten Virenscanner aktualisieren sich beim Starten regelmäßig. Diese Updates funktionieren, bleiben aber ebenfalls nicht über einen Neustart hin erhalten.

Wir aktualisieren den Bausatz mit Updates für neue Programmversionen, soweit das zum Bauen kritisch ist (etwa bei Programmanbietern, die stets nur die aktuelle Version unter einer geänderten URL zum Download anbieten). Sollten uns Probleme mit bestimmten Programmversionen bekannt werden, gibt es nötigenfalls auch Updates.

Dass sich programminterne Updates nicht dauerhaft festsetzen, hat mehrere Gründe: So finden die Programme keine reguläre Installation vor, liegen in anderen Pfaden und sind auch nicht mit allen Beigaben im Notfallsystem vorhanden. Deswegen schlagen Updates fehl.

Obendrein kommen Teile des Notfallsystems und auch viele Programme und Komponenten aus einer zur Laufzeit nicht veränderlichen WIM-Datei. Das lässt Windows-Schädlinge scheitern, das Notfallsystem zu manipulieren. Es verhindert aber auch die Programmupdates.

Dass Updates fehlschlagen, hat sogar Vorteile: Die Versionen, die der Bausatz bezieht, sind getestet. Es gibt Programme, bei denen die Version kritisch ist, zum Beispiel bei Autoruns: Neuere Versionen zerstören unter Umständen die Registry der Windows-Installation des mit dem Notfallsystem behandelten PCs. Unterm Strich also ein Grund, es im Notfallsystem mit den Updates ausnahmsweise nicht so genau zu nehmen.



Ins Notfallsystem eingebaute Programme lassen sich nicht aktualisieren, auch wenn sie es gern anbieten. Das ist technisch nicht möglich und in vielen Fällen wegen nicht erfüllter Abhängigkeiten oder sogar technischen Problemen mitunter sogar gefährlich.

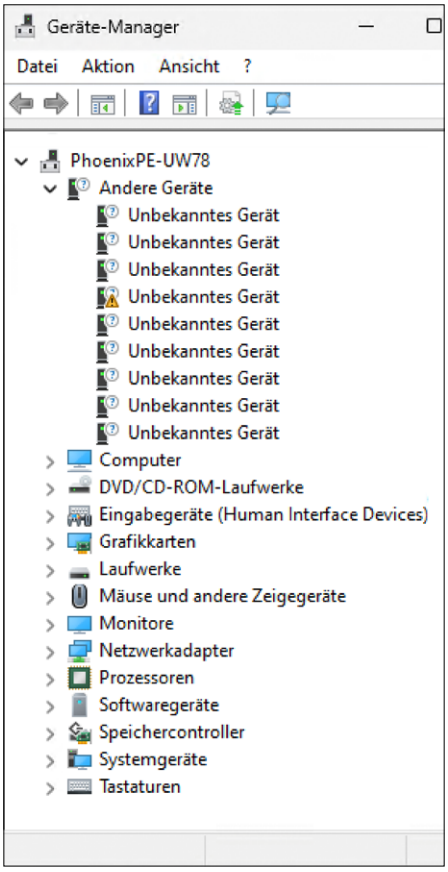
Treiber fehlen

Nach dem Bauen und Starten des Notfallsystems fehlen im Gerätemanager offensichtlich Treiber, obwohl ich die Treiber meines PCs exportiert und eingebaut habe. Was habe ich falsch gemacht?

Das ist in folgenden Grenzen normal: Das Notfallsystem beziehungsweise das als Basis verwendete Windows PE bringen nur einen begrenzten Satz von Treibern mit. Unser Bausatz beziehungsweise PhoenixPE reichern diesen Satz mit Treibern an, die im verarbeiteten Windows-ISO-Image enthalten sind. Dabei handelt es sich ausschließlich um Treiber, die Microsoft über die Installationsmedien verteilt und dafür signiert hat. Einige wenige Treiber ergänzt der Bausatz aus anderen Quellen.

Mitnichten integriert der Bausatz alle aus Windows-Installationsmedien extrahierbaren Treiber, weil das ein zu großes Notfallsystem-Image erzeugen würde, das auf PCs mit wenig Hauptspeicher nicht mehr liefe. Obendrein benötigt ein Notfallsystem auch nicht Treiber für jedes Gerät. Wenn also alle Funktionen gegeben sind, ergibt es wenig Sinn, weitere Treiber einzubauen.

Funktionieren hingegen einzelne, elementare Geräte wie Tastatur und Mauspad



Dass das Notfallsystem nicht sämtliche Geräte mit passenden Treibern versorgt, ist normal, solange alle elementaren Geräte versorgt sind, sollte man hier keinen Ehrgeiz an den Tag legen.

im Notfallsystem nicht, lassen sich die Treiber des zum Bauen verwendeten PCs einbauen; die Artikel in c't 2/2024 haben das erklärt. Die Prozedur erfasst allerdings ausdrücklich nur Treiber, die eben nicht von Microsoft selbst stammen. Sie ist also ungeeignet, um weitere Treiber von Microsoft selbst aus Windows herauszukratzen.

Im Notfallsystem fehlende Treiber, die ein frisch installiertes Windows ohne zusätzliche Updates bereits enthält, lassen sich nur durch Anpassen des Bausatzes integrieren. Tipps für fehlende Treiber nehmen wir gern entgegen. Alternativ könnten Sie auch schauen, ob es vom Hersteller des Geräts oder Chips, etwa Intel oder Realtek geeignete Treiber gibt. Die würde die automatisierte Treiberintegration erfassen und man kann sie oft auch im laufenden Notfallsystem nachladen, wenn eine dauerhafte Integration nicht gefragt ist. *(ps@ct.de)*

Projektseite, Downloads, Artikel:
ct.de/ydfz