c’t-Notfall-Windows 2020

Handgriffe zum Bauen unseres Notfallsystems auf Windows-Basis

Das c't-Notfall-Windows startet vom USB-Stick. Es hilft, nicht mehr lauffähige, beschädigte oder von Schädlingen heimgesuchte Windows-Installationen aufzurichten. Wir haben die Ausstattung aktualisiert und ergänzt. Den neuen Bausatz stellen wir zum Download bereit.

Von Stephan Bäcker und Peter Siering

Die technische Basis für das c't-Notfall-Windows bildet Windows PE, also Microsofts Minimal-Windows, das unter anderem für das Einrichten von Windows und die Systemwiederherstellung bemüht wird. Durch Tricks mausert sich das abgespeckte System zu einem vom USB-Stick startenden vollwertigen Rettungssystem. Windows-Nutzer finden sich in einer bekannten Umgebung wieder: Explorer als Dateimanager, Firefox als Browser, Notepad, Gerätemanager et cetera. Dateisystem- und Netzwerkzugriffe laufen in der Original-Implementierung. Das Notfallsystem benutzt reguläre Windows-Treiber und erreicht so höchstmögliche Kompatibilität, etwa auch für den Zugriff auf Bitlocker-verschlüsselte Daten.

Die Ausstattung geht aber deutlich über ein reguläres Windows hinaus: Der Bausatz ergänzt Programme zur Schädlingssuche (Avira PC Cleaner, Eset Online Scanner und Kaspersky Virus Removable Tool), Software zur Datenrettung, Helfer für die Hardwarediagnose und Werkzeuge, mit denen sich vergessene Passwörter zurücksetzen lassen. Dateivergleicher, Fernwartung, Hex-Editor, Imaging- und Klon-Tools sowie diverse Viewer runden den Funktionsumfang ab. Tipps für den Umgang mit dem System und seinen Beigaben finden Sie im Ordner „c't-Artikel" auf dem Desktop des fertigen Notfallsystems. Die PDF-Dateien enthalten die in Details überarbeiteten Anleitungen der Vorjahresfassung.

Dieser Artikel konzentriert sich auf Hinweise zum Bauen des Notfallsystems und Neuerungen. Die folgenden Artikel widmen sich detailliert dem Kopieren von Windows-Installationen zur Diagnose und als Sicherung sowie der Datenrettung. Wenn Sie das System bauen, schauen Sie unbedingt auch auf der Projektseite vorbei, die Sie über ct.de/yhft finden. Hier veröffentlichen wir ergänzende Hinweise, eventuelle Updates, und Sie finden dort auch ein Forum für den Austausch mit anderen Nutzern zum Bausatz selbst.

Credits

Was wir als c't-Notfall-Windows hier veröffentlichen, ist nicht allein auf unserem Mist gewachsen. Der Bausatz wird von ChrisR und einer regen Community im Forum theoven.org entwickelt. Die Gemeinde finanziert sich weitgehend selbst und ist auf Spenden angewiesen. Wir frieren alljährlich eine Version ein, spitzen sie auf eine aus unserer Sicht essenzielle Auswahl zu und sorgen für rund ein Jahr dafür, dass der Bausatz funktionstüchtig bleibt. Im Forum zum Bausatz leisten wir, aber auch einige besonders engagierte Leser, Hilfe zu eventuellen Problemen. An dieser Stelle herzlichen Dank dafür!

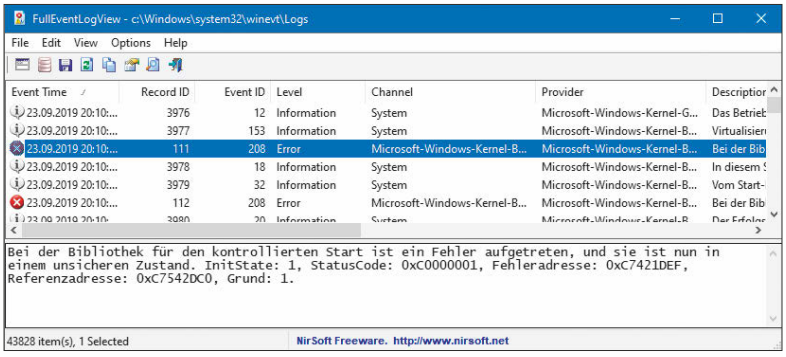
Im vergangenen Jahr hatten wir das Programm ausgetauscht, das den Bausatz verarbeitet. Ursprünglich sind die auf Windows PE aufbauenden Systeme mithilfe des Programmes Winbuilder entstanden – letztlich einer Skript-Engine und -Sammlung, die die Einzelteile zusammenbaut. Das Programm hat allerdings technische Mängel und so kam das von Hajin Jang als Alternative entwickelte PE-Bakery gerade recht. Das hat den Bau deutlich stabilisiert und der Umbau von ChrisR auf Wimlib die Laufzeit drastisch reduziert. Das aktuelle Notfall-Windows nutzt die gleiche PEBakery-Version wie schon ihr Vorläufer. Das Basisprojekt ist Win10XPE, das ChrisR am 20.7.2019 veröffentlicht hat.

Neuerungen

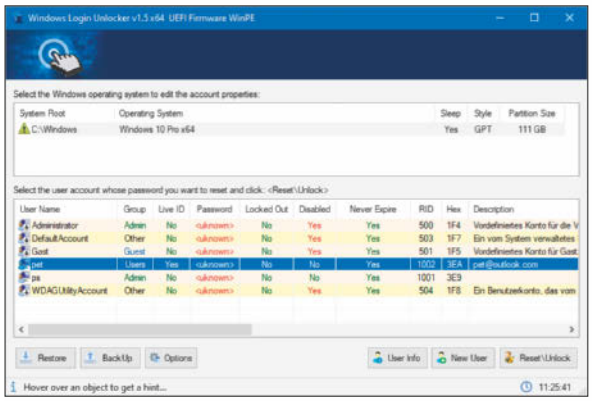
Der aktuelle Bausatz ist robuster, weil er unter anderem frühzeitig eventuelle Interventionen von Sicherheitssoftware erkennt. Die gefährdet ansonsten nämlich den Bauerfolg. Ansonsten bringt er eine aktualisierte Grundausstattung mit und kann jetzt Windows 10 in der 1903er-Ausgabe als Basis nutzen. Neu an Bord ist ein Event-Viewer, um Ereignisprotokolle anzusehen, und eine zusätzliche Software, um sich Zugang zu einem Windows-Benutzerkonto zu verschaffen, das an ein Microsoft-Konto gekoppelt ist.

FullEventLogView finden Sie unter „Analyse" im Startmenü. Um die Ereignisse einer brachliegenden Windows-Installation einzusehen, wählen Sie im File-Menü „Choose Data Source" aus. Wählen Sie im ersten Feld des Dialogs „Load events from external folder with log files". Fangen Sie dann im Feld „External event log folder" an, Laufwerk und Pfad Ihrer Windows-Installation einzugeben. Das Programm hilft während der Eingabe mit Vorschlägen. Der vollständige Pfad lautet bei einer typischen Installation „c:\windows\system32\winevt\logs". Die übrige Bedienung ist weitgehend intuitiv möglich.

Zur Bedienung des „Windows Login Unlocker" gibt es wenig zu sagen, dafür



Neu an Bord ist ein Werkzeug zum Anzeigen von Ereignisprotokollen brachliegender Windows-Installationen.



Der Windows Login Unlocker bringt sogar das Kunststück fertig, Microsoft-Konten wieder zugänglich zu machen, wenn jede Hoffnung auf eine Passwortwiederherstellung erloschen ist.

mehr zu seinen Fähigkeiten und zur Herkunft: Er kann Windows-Konten aufsperren, die mit einem Microsoft-Konto verknüpft sind. An dieser Aufgabe scheitert das bewährte und im Notfall-Windows schon enthaltene „ntpwedit". Den Login Unlocker sollte man allerdings vorerst nur in solchen Notfällen einsetzen. Die Software stammt aus einem russischen Forum, die Weiterentwicklung wurde aufgekündigt. Wir haben dem Programm auf die Finger gesehen und nichts Bedenkliches entdeckt.

Seiteneffekte muss man aber in Kauf nehmen: Wenn man damit ein per Microsoft-Konto gesichertes Benutzerkonto aufsperrt, wandelt das Programm dieses Profil in ein lokales ohne Passwort um. Das heißt, die Verbindung zu dem Online-Konto geht verloren. Wie auch bei ntpwedit lassen sich anschließend mit NTFS-Hilfe verschlüsselte Dateien (EFS) nicht mehr lesen.

Bautipps

Wie gehabt brauchen Sie zum Bauen des Notfallsystems außer dem Bausatz die Originaldateien von Windows 10 in einer speziellen Form (also WIM und nicht als ESD-Datei). Am einfachsten sind sie in Form der Eval-Versionen zum Download zu bekommen. Auch wenn der Download je nach Internet-Anbindung einen Moment dauern mag, spart man sich danach viel Bastelei. Sämtliche nötigen Downloads finden Sie über ct.de/yhft. Die wesentlichen Bedienschritte fast der Kasten auf Seite 19 zusammen. Tun Sie sich aber den Gefallen zunächst hier weiterzulesen, um für den Fall gewappnet zu sein, dass der Minimalsatz von Bedienschritten nicht genügen sollte – auf den Bausatz wirken Faktoren ein, die sich nicht immer zu 100 Prozent kontrollieren lassen.

Das Bauen geht auf einem PC mit einer SSD deutlich schneller. Das Laufwerk braucht ungefähr 10 GByte freien Platz, um die Downloads aufzunehmen und temporäre Dateien zu erstellen. Besondere Anforderungen an die RAM-Ausstattung stellt der Bausatz nicht – vier GByte genügen. Während des Bauvorgangs werden weitere Programme heruntergeladen und aus den Komponenten entpackt. Das ruft immer wieder Sicherheitssoftware auf den Plan, die solche Vorgänge für verdächtig hält oder einzelne Programme als besonders gefährlich einstuft. Wir haben den Bausatz aber akribisch geprüft und gehen davon aus, dass er schädlingsfrei ist. Ein paar Alarme sind jedoch denkbar, Details finden Sie bei Bedarf auf der Projektseite unter ct.de/yhft. Um den Bausatz störungsfrei zu bauen, empfiehlt die Anleitung deshalb das Einrichten von Ausnahmen für das Bauverzeichnis und das Programm zum Bespielen von USB-Sticks.

Beim Bauen kann es vorkommen, dass einzelne Server nicht erreichbar sind, die der Bauprozess ansteuert. Steckt der Prozess augenscheinlich fest, sollten Sie ihn über die Stop-Funktion beenden und nicht über den Taskmanager abwürgen. So ist sichergestellt, dass ein neuer Klick auf den Build-Knopf den Prozess wieder sauber starten kann. Spätestens nach einigen Stunden sollten sich Download-Probleme von selbst erledigen. Sollten Server dauerhaft nicht erreichbar sein oder sich an der heruntergeladenen Software Änderungen ergeben haben, werden wir passende Updates bereitstellen und Hinweise auf der Projektseite veröffentlichen.

Das Bauverzeichnis ist für den einmaligen Gebrauch gedacht: Wenn Sie nach einer 64-Bit-Version auch die 32-Bit-Version bauen möchten, sollten Sie neu entpacken und beginnen. Das zahlt sich auch bei anhaltenden anderen Fehlern aus.

Diagnosehilfen

Am Ende eines Baulaufs oder auch im Fehlerfall zeigt PEBakery ein Fenster an, das den Export von Protokollen erlaubt. In hartnäckigen Fällen können Sie uns solche Protokolle gern per Mail an ctnotwin20@ct.de zuschicken. Exportieren Sie bitte das Build-Log in HTML-Form. Diese Form lässt sich am besten sichten. Das vorausgewählte Build-Log ist das nützliche Protokoll, das System-Log nur in Ausnahmefällen. Auf der Projektseite finden Sie zum Vergleich Log-Dateien für erfolgreiche Bauläufe für die x86- und x64-Version und die aktuelle Eval-Version von Windows 10. Die Läufe stammen von einem älteren Core i3 mit 4 GByte RAM und SSD. Die Laufzeiten der einzelnen Skripte sollten aktuelle Systeme heute noch unterbieten.

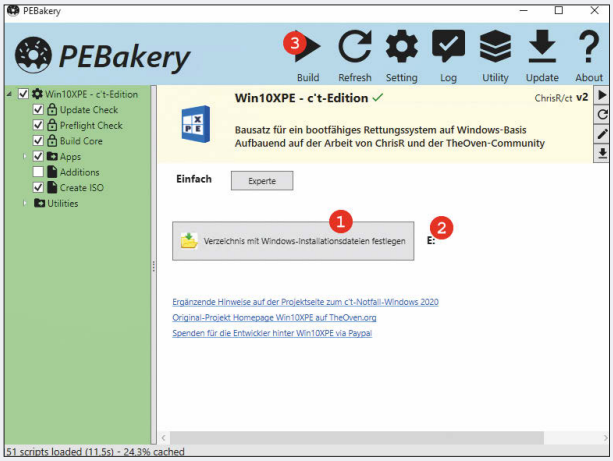
Je länger die Veröffentlichung des Bausatzes zurückliegt, desto wahrscheinlich ist es, dass Sie beim Benutzen des Notfallsystems Hinweise einzelner Programme auf verfügbare Updates erhalten. Diese Updates gelingen in der Regel nur im Bausatz und nicht im erstellten Notfall-Medium. Da es sich dabei oft um Minor-Updates handelt, ergibt es aus unserer Sicht keinen Sinn, den Bausatz ständig zu aktualisieren. Sollten sich aus Ihrer Sicht tatsächlich interessante Neuerungen durch ein solches Update ergeben, prüfen wir gern, ob wir ein Update erstellen können. Vorab sei aber gesagt: Es geht nicht in jedem Fall, manches Programm lässt sich in neuer Version nicht integrieren, weil es andere technische Anforderungen stellt, etwa eine .NET-Umgebung voraussetzt (die auch dieses Mal nicht Teil des Notfallsystems ist).

Apropos nicht umsetzbare Wünsche: Auch diese Fassung des c't-Notfall-Windows spricht nicht mit SMB-Servern, die nur Version 1 des Protokolls anbieten. Wir haben uns entschlossen, keine weitere Zeit in eine Lösung dieses Problems zu stecken. Verglichen mit dem Funktionsumfang des Original-Bausatzes von theoven.org werden Sie auch einige Programme vermissen, die dort enthalten sind. Die Community schnürt dort durchaus Pakete mit Software, die jenseits der Grenze liegen, was wir in Absprache mit den Herstellern zum Download bereitstellen können. In Grenzen sollte es indes möglich sein, sogenannte „Member XPE App Plugins" auch in unseren Bausatz einzubinden. Bleibt noch: Viel Erfolg beim Bauen! *(ps@ct.de)* c't

Downloads, Projektseite, Forum:
ct.de/yhft

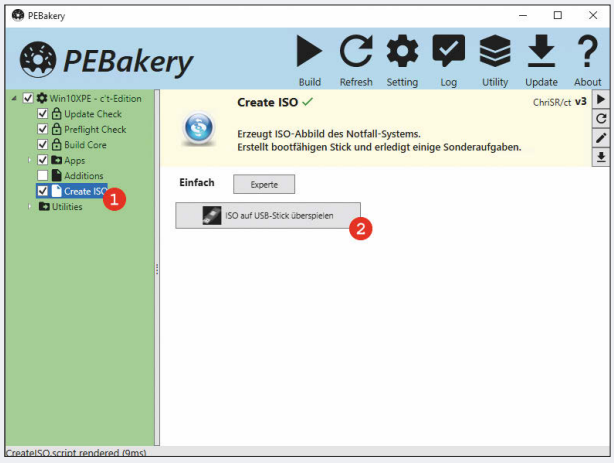
Der Weg zum bootfähigen USB-Stick

1. Lesen Sie den ganzen Artikel vorher durch.
2. Laden Sie das ZIP-Archiv (ungefähr 250 MByte) mit dem Bausatz herunter (siehe ct.de/yhft).
3. Laden Sie eine ISO-Datei mit einer Eval-Version von Windows 10 herunter (zwischen 3 und 4 GByte). Empfehlungen für geeignete Versionen finden Sie auf der Projektseite (siehe ct.de/yhft). Sie haben die Wahl zwischen 32- und 64-Bit-Versionen; meist passt 64 Bit.
4. Erstellen Sie ein Verzeichnis, in dem der Bauvorgang vonstatten gehen soll, zum Beispiel c:\ctnot.
5. Definieren Sie in in Ihrem Virenscanner eine Ausnahme für dieses Verzeichnis. Erstellen Sie zusätzlich eine Ausnahme für den Prozess „rufus-3.7p.exe“.
6. Entpacken Sie das ZIP-Archiv in diesem Verzeichnis.
7. Binden Sie per Doppelklick die ISO-Datei als virtuelles Laufwerk ein (unter Windows 7 brauchen Sie dafür unter Umständen zusätzliche Software, die Sie ebenfalls via ct.de/yhft finden).
8. Starten Sie in c:\ctnot PEBakeryLauncher.exe.
9. Windows Defender SmartScreen wird eine Warnung anzeigen, da das Programm heruntergeladen ist, obwohl es signiert ist. Führen Sie es trotzdem aus.
10. Folgen Sie gegebenenfalls den Hinweisen zur Installation einer aktuellen .NET-Umgebung; falls die nötig war, müssen Sie PEBakeryLauncher.exe anschließend noch einmal starten.
11. Bestätigen Sie die Benutzerkontensteuerung.
12. Drücken Sie den Knopf „Verzeichnis mit Windows-Installationsdateien“ auswählen und wählen Sie das Laufwerk, das Sie unter 7. eingebunden haben. Vorsicht: C: ist vorausgewählt; Sie müssen das andere Laufwerk (etwa D:) auswählen. Das ausgewählte Laufwerk erscheint hinter dem Knopf.
13. Betätigen Sie den Build-Knopf und haben Sie etwas Geduld. Auf einem PC mit SSD dauert das Bauen rund 10 Minuten. Es werden dabei einige Dateien aus dem Internet heruntergeladen.

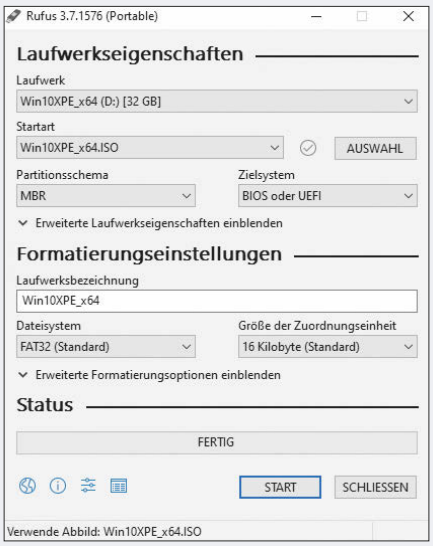


Wenn alle Dateien bereitliegen und das ISO als Laufwerk eingebunden ist, genügen zwei Klicks (1+3) und der Bauvorgang startet. Der Bausatz zeigt das ausgewählte Laufwerk an (2).

14. PEBakery zeigt nur kurz eine Erfolgsmeldung an und öffnet ein Fenster zum Export von Log-Dateien. Steht der Fehlerzähler auf 0, hat der Bau geklappt.
15. Um das Notfallsystem auf einen USB-Stick zu überspielen, klicken Sie im Projektbaum links „Create ISO“ an und betätigen Sie dann den Knopf „ISO auf USB-Stick überspielen“.
16. Es startet das Programm Rufus zum Beschreiben eines Sticks. Stecken Sie jetzt den Stick an. Achten Sie darauf, dass sein Laufwerk in Rufus vorausgewählt ist und Drücken Sie dann auf „START“.
17. Das war es. Beenden Sie PEBakery.
18. Tipps zum Booten vom USB-Stick finden Sie auf der Projektseite (siehe ct.de/yhft).



Zum Beschreiben eines USB-Sticks müssen Sie auf die Seite des „Create-ISO“-Skripts wechseln.



Rufus überträgt die Dateien aus dem erzeugten ISO auf einen USB-Stick. Achten Sie unbedingt darauf, dass das richtige Laufwerk selektiert ist. Alle Dateien werden gelöscht.