Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan Bund ISB

Melde- und Analysestelle Informationssicherung MELANI

GovCERT.ch

Anleitung zur Entfernung von Schadsoftware

MELANI / GovCERT.ch

Version:	v1.01
Autor:	MELANI / GovCERT.ch
Getestet auf:	Windows 7 Home Premium SP1 Deutsch (64 Bit)

[1] http://creativecommons.org/licenses/by-nd/3.0/

Einleitung

Diese Anleitung soll Ihnen dabei helfen, eine Infektion Ihres Computers mit Schadsoftware (sogenannter *Malware*) zu identifizieren und zu bereinigen. Diese Anleitung wurde von der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) verfasst und auf einem Windows 7 getestet. Grundsätzlich sollte die Anleitung jedoch mit jeder Version von Windows (Windows XP[2], Windows Vista, Windows 8) verwendbar sein.

Vermutlich lesen Sie dieses Dokument, weil Sie durch Ihren Internet Service Provider (ISP) auf eine Infektion Ihres Computers aufmerksam gemacht wurden oder weil Sie vermuten, Ihr Computer sei mit Schadsoftware infiziert. Diese Anleitung wird Sie Schritt für Schritt durch die Anwendung von *Norton Power Eraser* führen, um Ihren Computer nach Schadsoftware zu scannen und diese zu entfernen.

***** Wichtig! *****

Diese Anleitung wurde mit grosser Sorgfalt verfasst. Dennoch ist es möglich, dass die in dieser Anleitung beschrieben Werkzeuge nicht in der Lage sind, alle Schadsoftware zu erkennen. Grundsätzlich empfiehlt MELANI bei einer Infektion des Computers diesen neu aufzusetzen (Neuinstallation des Betriebssystems) um mögliche Rückstände der Schadsoftware zu eliminieren. Für die Funktionalität und Verwendung der in dieser Anleitung genannten Tools übernimmt MELANI keine Verantwortung. MELANI lehnt jegliche Haftung für Schäden ab, welche aus dem Einsatz dieser Anleitung oder einem der darin beschriebenen Werkzeuge entstehen.

Wenn Sie Opfer einer kriminellen Handlung geworden sind und diese strafrechtlich untersuchen respektive verfolgen lassen möchten, empfehlen wir Ihnen, eine Anzeige bei Ihrer lokalen Kantonspolizeidienststelle zu erstatten. Versuchen Sie in diesem Falle nicht, die Schadsoftware zu entfernen, da Ihr Computer möglicherweise für die Spurensicherung benötigt wird. Wir empfehlen, den Computer bis zu diesem Zeitpunkt nicht mehr zu verwenden.

[2] Die Unterstützung von Windows XP durch Microsoft endet am 8. April 2014. Wir empfehlen Benutzer von Windows XP auf eine aktuelle Version von Windows umzusteigen.
https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet

Anleitung

In dieser Anleitung wird die Entfernung von Schadsoftware mittels des von Symantec gratis bereitgestellten *Norton Power Eraser* beschrieben. Es existieren noch andere kommerzielle sowie auch gratis erhältliche Entfernungstools („Cleaner“). Sie finden eine Liste von solchen Werkzeugen am Ende dieses Dokumentes.

Herunterladen des Norton Power Eraser

Als erstes muss *Norton Power Eraser* heruntergeladen werden. Dazu benötigen Sie eine aktive Internet Verbindung. Die Software kann unter folgender URL heruntergeladen werden:

https://security.symantec.com/nbrt/npe.aspx

Öffnen Sie die oben erwähnte URL in Ihrem Webbrowser. Daraufhin öffnet sich die Webseite von Norton Power Eraser:

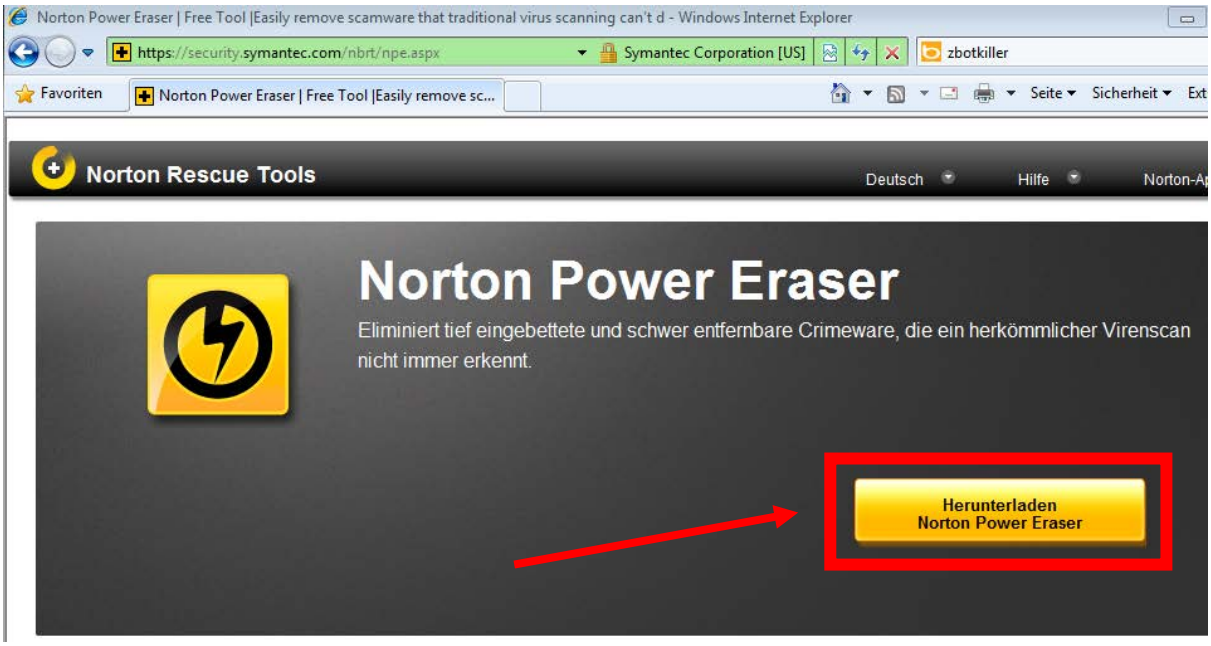

Abbildung 1 - Webseite Norton Power Eraser

Durch einen Klick auf die entsprechende Schaltfläche (oben ***rot*** markiert) kann der Download gestartet werden.

Nun öffnet sich ein neuer Dialog (*Dateidownload*).

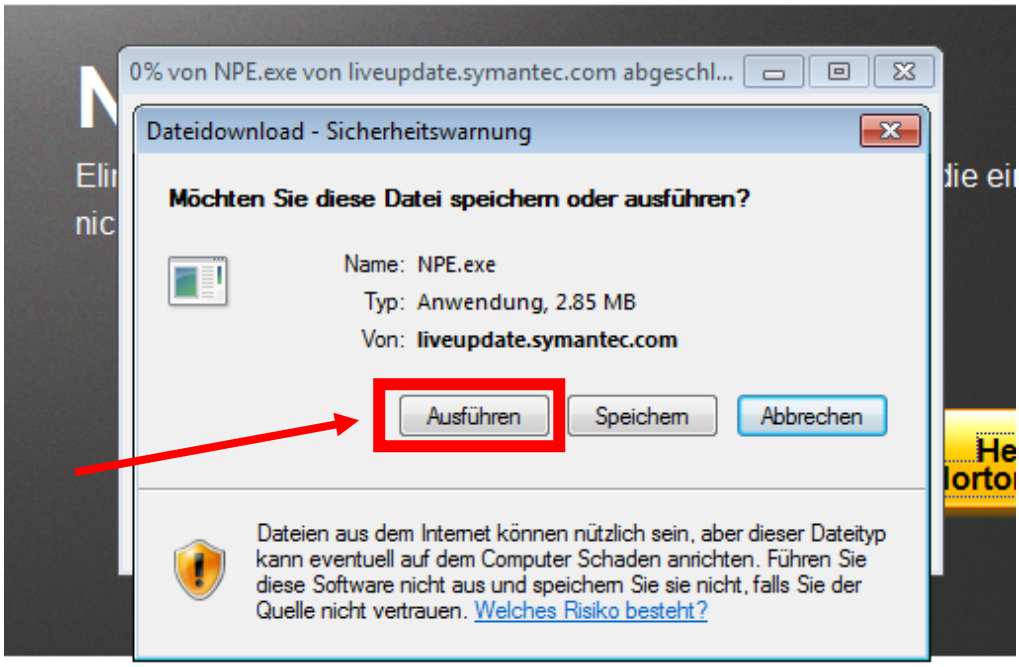

Abbildung 2 - Starten Sie den Dateidownload durch einen Klick auf die Schaltfläche "Ausführen"

Wählen Sie hier bitte die Option „*Ausführen*“ durch Klicken auf die entsprechende Schaltfläche (oben ***rot*** markiert) aus. Der Download benötigt üblicherweise nur wenige Sekunden. Sobald dieser abgeschlossen ist, wird *Norton Power Eraser* gestartet. Bei neueren Versionen von Windows erscheint an dieser Stelle üblicherweise noch ein Dialog der Benutzerkontensteuerung:

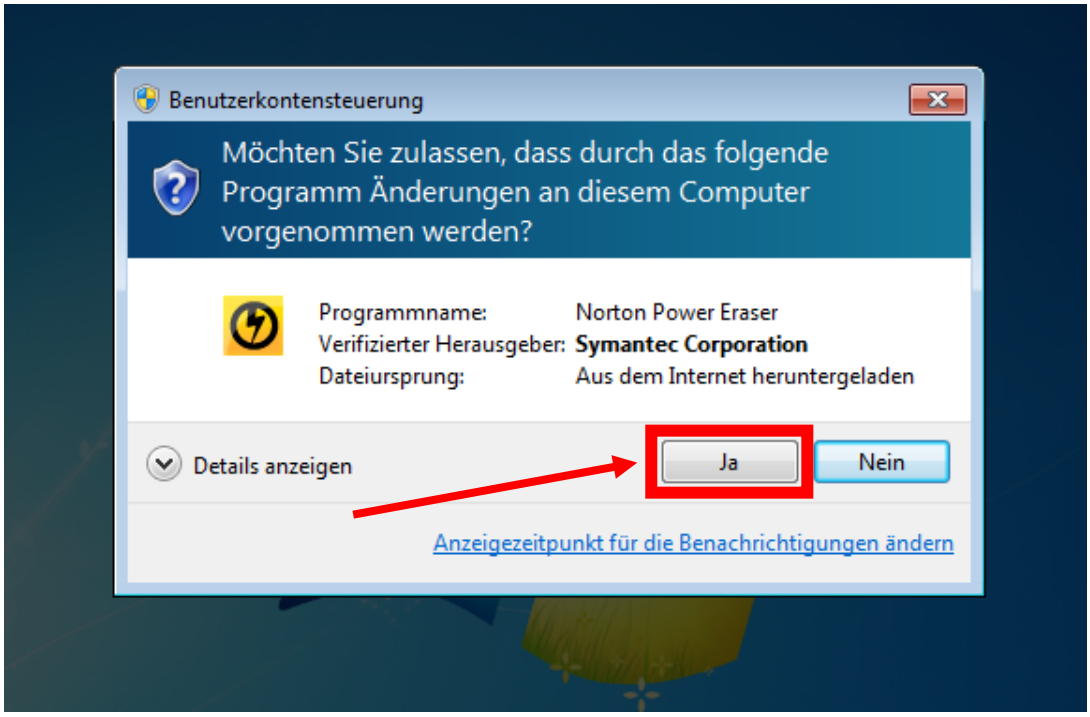

Abbildung 3 - Benutzerkontensteuerung: Starten Sie Norton Power Eraser durch einen Klick auf die Schaltfläche "Ja"

Der Dialog der Benutzerkontensteuerung kann mit einem Klick auf die Schaltfläche „*Ja*“ (oben ***rot*** markiert) beantwortet werden, wonach sich die Software startet.

Bevor die Software verwendet werden kann, muss die Endbenutzerlizenzvereinbarung akzeptiert werden:

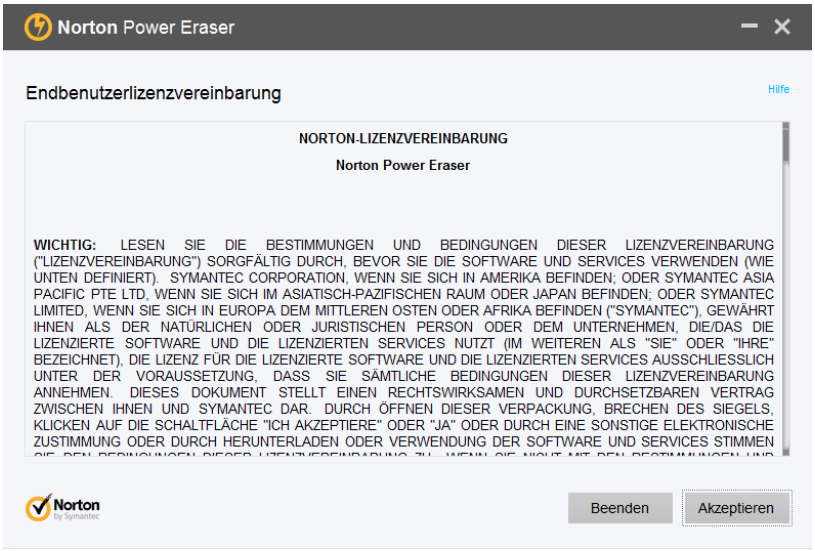

Abbildung 4 - Die Endbenutzervereinbarung muss akzeptiert werden, damit die Software verwendet werden kann

Nach dem Akzeptieren der Endbenutzerlizenzvereinbarung erscheint der Startbildschirm von Norton Power Eraser:

Abbildung 5 - Startbildschirm, klicken Sie auf "Scan auf Risiken", um den Scan zu starten

Klicken Sie auf die Schaltfläche *„Scan auf Risiken“* (oben ***rot*** markiert) um Ihren Computer nach Malware zu scannen.

Der Scan wird beim nächsten Neustart automatisch durchgeführt, weshalb Sie Ihren Computer nun neustarten sollten:

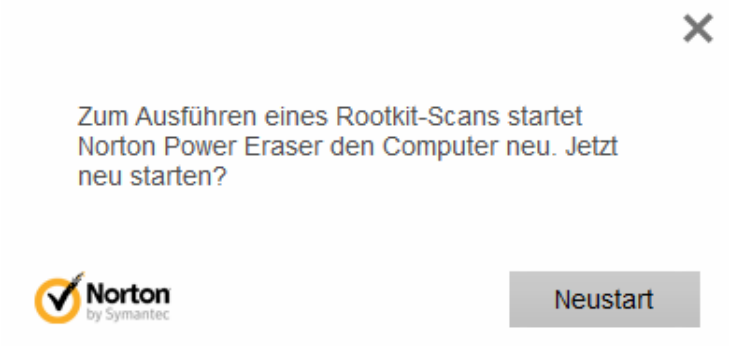

Abbildung 6 - Starten Sie Ihren Computer neu, um den Scan zu starten

Nach dem Neustart Ihres Computer sucht die Software automatisch nach Schadsoftware auf Ihrem Computer. Während dem Scan erscheint ein entsprechender Dialog auf dem Bildschirm:

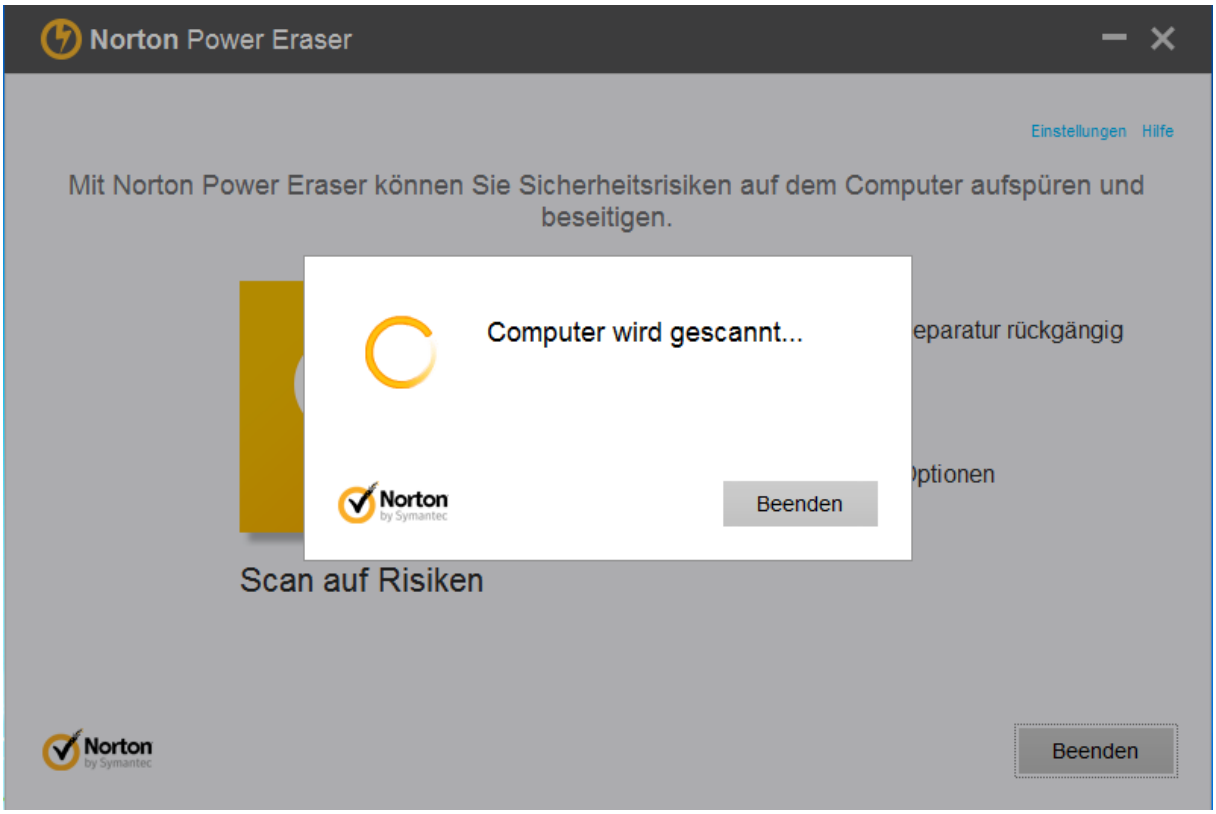

Abbildung 7 - Bitte warten Sie, während die Software ihren Computer auf Schadsoftware scannt

Je nach Computer kann der Scan mehrere Minuten dauern. Bitte schalten Sie während dem Scan Ihren Computer nicht aus und verwenden Sie während dessen keine anderen Programme.

Sobald der Scan abgeschlossen ist, erscheint ein Dialog auf Ihrem Bildschirm, welcher Ihnen die Resultate des Scans sowie mögliche Bereinigungsoptionen anbietet.

Falls keine Schadsoftware gefunden wurde, sollte eine entsprechende Meldung auf Ihrem Bildschirm erscheinen:

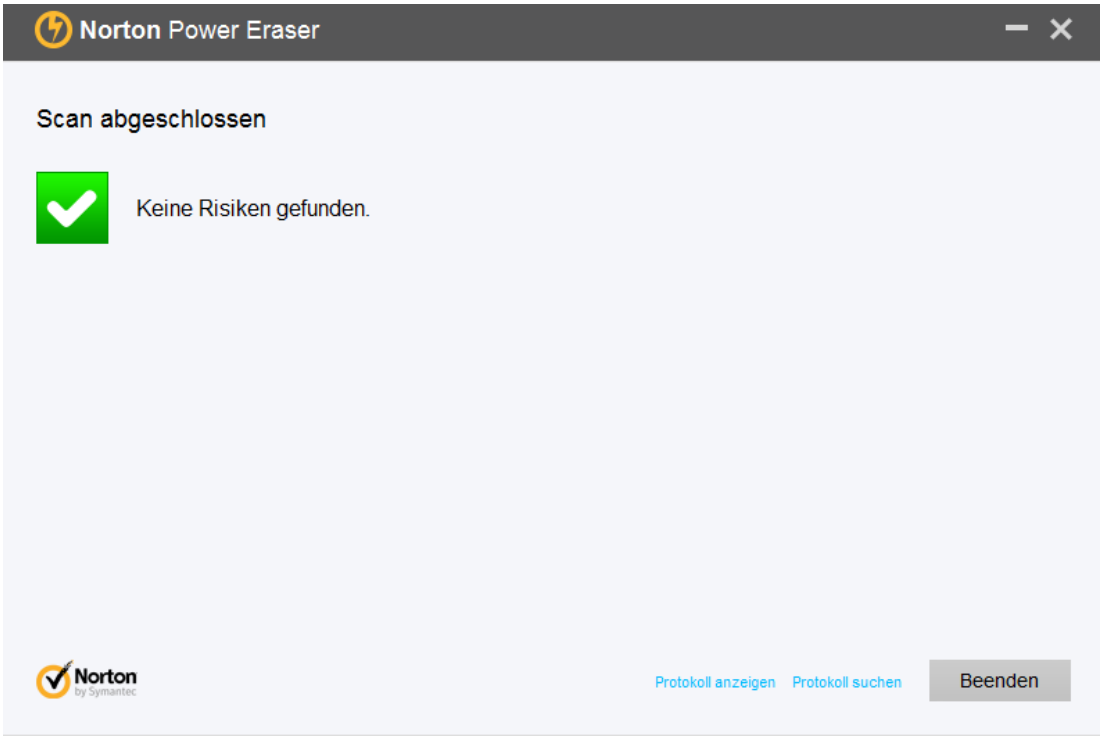

Abbildung 8 - Scan abgeschlossen - keine Schadsoftware gefunden

In diesem Fall ist der Prozess abgeschlossen. Sollten Sie weiterhin vermuten, dass Ihr Rechner infiziert ist, insbesondere wenn Sie von Ihrem Internetservice Provider (ISP) auf eine Infektion auf Ihrem Computer hingewiesen wurden, empfehlen wir Ihnen, den Computer mit weiteren Entfernungstools zu überprüfen (siehe Liste am Ende dieser Anleitung) und/oder einen IT-Fachmannperson zu konsultieren.

Falls *Norton Power Eraser* Schadsoftware findet, wird diese entsprechend aufgelistet:

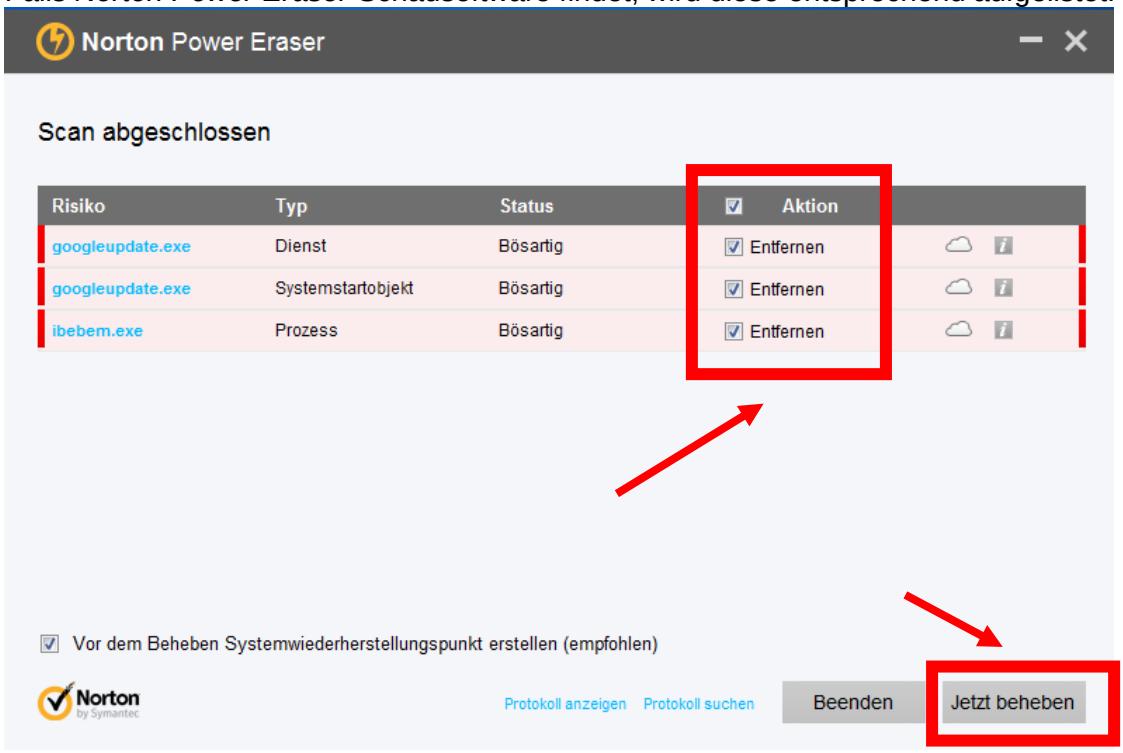

Abbildung 9 - Dialog, wenn Schadsoftware gefunden wurde

Für jede erkannte Schadsoftware kann nun festgelegt werden, ob diese durch *Norton Power Eraser* entfernt werden soll (oben ***rot*** markiert). Falls Sie nicht wissen, ob eine Schadsoftware entfernt werden soll oder nicht, empfiehlt sich die Standardeinstellung zu verwenden (üblicherweise „*Entfernen*“). Durch Klicken auf die Schaltfläche „*Jetzt beheben*“ (oben ***rot*** markiert) erstellt *Norton Power Eraser* einen *Systemwiederherstellungspunkt* und beginnt mit der Entfernung der Schadsoftware:

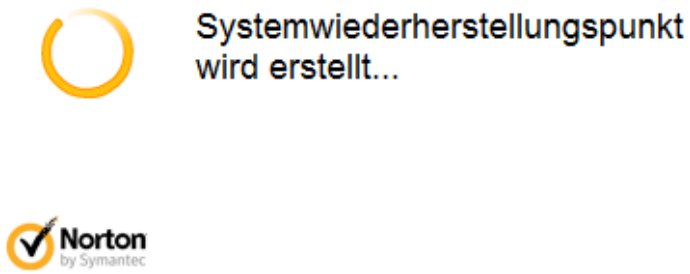

Abbildung 10 - Die Software erstellt einen Systemwiederherstellungspunkt

Damit die Schadsoftware vollständig entfernt werden kann, muss der Computer nun neugestartet werden:

Abbildung 11 - Zum Entfernen der Schadsoftware ist ein Neustart des Computers nötig

Durch einen Klick auf die Schaltfläche „*Jetzt neu starten*“ wird der Computer neugestartet.

Nach dem Neustart des Computers erscheint automatisch ein entsprechender Dialog am Bildschirm, welcher die Ergebnisse des Scans und der durchgeführten Aktionen (Entfernung/Bereinigung) ausgibt:

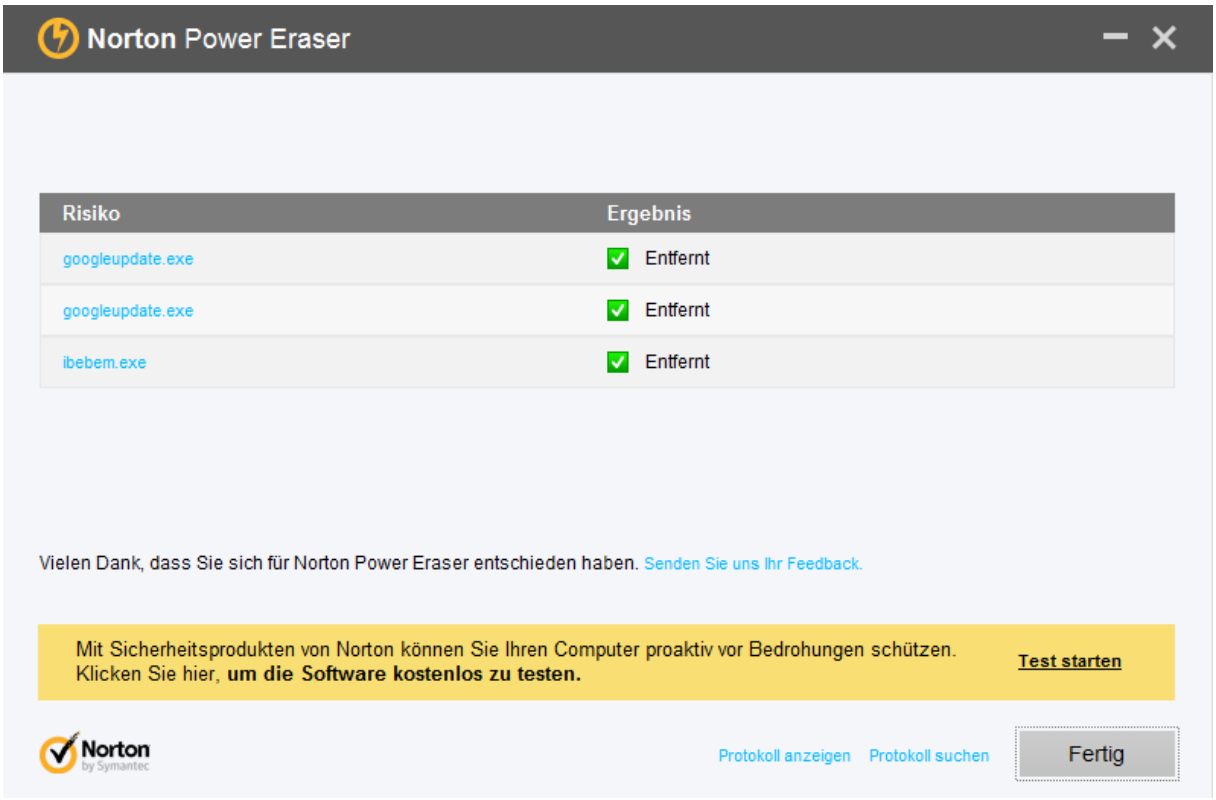

Abbildung 12 - Die detektierte Schadsoftware wurde erfolgreich entfernt

Die detektierte Schadsoftware wurde entfernt und *Norton Power Eraser* kann nun beendet werden.

Sollten Sie weiterhin Schwierigkeiten mit Ihrem Computer haben oder vermuten, Ihr Computer ist immer noch infiziert, empfehlen wir Ihnen, den Computer mit weiteren Entfernungstools zu überprüfen (siehe Liste am Ende dieser Anleitung) und/oder eine IT-Fachperson zu konsultieren.

***** Wichtig! *****

Schadsoftware gelangt üblicherweise auf Grund von Sicherheitslücken in veralteter, Software und/oder durch unvorsichtiges Verhalten des Anwenders auf den Computer. Um zu verhindern, dass Ihr Computer erneut von Schadsoftware befallen wird, empfehlen wir Ihnen folgende Anleitung:

Verhaltensregeln im Umgang mit dem Internet:
https://www.melani.admin.ch/verhaltensregeln

Weitere Erläuterungen

In diesem Dokument wird die Verwendung von *Norton Power Eraser* beschrieben. Es gibt weitere Software mit vergleichbarer Funktionalität von anderen Anbietern. Eine Liste von Antiviren-Software finden Sie hier:

https://www.melani.admin.ch/melani/de/home/dokumentation/links/sicherheitsloesungen.html

Auf der deutschen Seite botfrei.de finden Sie eine Schritt für Schritt Anleitung für ein weiteres Entfernungstool. Die Anleitung des EU-Cleaner ist unter folgendem Link erreichbar:

https://www.botfrei.de/eucleaner.html