Peters BiosPaßwort

Version 3.2, Copyright (c) 2000..2004 Peter Weigel

1 Kurzbeschreibung

Diese Anwendung dient der Rekonstruktion, Deaktivierung oder Umgehung des BIOS-Paßwortes (fast) aller BIOS-Typen und -Versionen. Es handelt sich hierbei um eine Windows-Anwendung mit grafischer Benutzeroberfläche, die sogar unter Windows NT/2K/XP lauffähig ist!

2 Vorbemerkung

BIOS-Paßworte dienen entweder zum Schutz des Computers vor unberechtigtem Zugriff oder zum Schutz der BIOS-Einstellungen vor unberechtigten Änderungen. Es kommt aber durchaus vor, daß man das Paßwort vergißt oder einen mittels Paßwort geschützten Computer aus zweiter Hand erwirbt und der Verkäufer sich nicht an das Paßwort erinnert. In diesen Fällen kann diese Anwendung zum Einsatz kommen.

Bitte beachten Sie, daß diese Anwendung nur auf dem eigenen Computer angewendet werden darf. Das Ausspionieren fremder Paßwörter ist hiermit ausdrücklich untersagt. Ich weise außerdem darauf hin, daß die Benutzung dieser Anwendung zu irreparablen Systemschäden führen kann und daher auf eigenes Risiko geschieht.

3 Funktionsbeschreibung

Diese Anwendung besteht aus nur einem Fenster, das mit Hilfe eines PageControls in mehrere Seiten aufgeteilt wird. Auf diesen Seiten werden verschiedene Funktionen zur Rekonstruktion, Deaktivierung oder Umgehung des BIOS-Paßwortes zur Verfügung gestellt.

3.1 Paßwort rekonstruieren

Mit Hilfe dieser Funktion können Sie BIOS-Paßwörter rekonstruieren. Es werden keine BIOS-Einstellungen verändert.

Eine Rekonstruktion ist nur möglich, wenn der Anwendung das Verschlüsselungsverfahren und die Position des verschlüsselten Paßwortes (im CMOS) bekannt sind (BIOS-Paßwort-Rekonstruktions-Informationen - BPRI). Daher ist diese Funktion nicht für alle BIOS-Typen oder -Versionen verfügbar.

Auf dieser Seite wird Ihnen eine Liste aller unterstützten BIOS-Typen, -Versionen und Paßwortarten angezeigt. Die meisten Einträge sind grau dargestellt. Diese wurden, durch beim Start der Anwendung durchgeführte Tests, als nicht zutreffend erkannt. Alle schwarz dargestellten Einträge sind prinzipiell zutreffend. Um weitere Eingrenzungen vorzunehmen, sollten Sie die Bezeichnung Ihres BIOS (Typ, Version) ausfindig machen. Diese Informationen finden Sie in der Regel direkt nach dem Einschalten des Computers (beim Speichertest) am oberen Bildschirmrand. Auch die BIOS-Identifikationsnummer (unterer Bildschirmrand) sowie das BIOS-Datum können hilfreich sein. Durch Doppelklick oder Klick mit der rechten Maustaste auf einen Eintrag der Liste erhalten Sie detailiertere Informationen zu dem jeweiligen Eintrag. Ein Abgleich dieser Zusatzinformationen mit den Informationen über Ihr BIOS bzw. Computer sollte ausreichen, um den für Ihren Computer zutreffenden Eintrag zu finden (falls dieser existiert). Bitte beachten Sie aber, daß die Informationen falsch, zu grob oder zu fein sein könnten und es somit keine Garantie gibt, daß eine Auswahl oder ein Ausschluß korrekt ist.

Falls bei den Zusatzinformationen eine BIOS-Identifikation angegeben ist, so bedeutet dies lediglich, daß die BIOS-Paßwort-Informationen auf diesem System ermittelt wurden bzw. die Rekonstruktion / Deaktivierung auf diesem System getestet wurde. Eine Übereinstimmung mit Ihrer BIOS-Identifikation

ist in der Regel nicht nötig und nach den Gesetzen der Wahrscheinlichkeit auch sehr unwahrscheinlich.

Wenn Sie einen Eintrag als den Richtigen identifiziert haben, wählen Sie diesen aus, woraufhin das Paßwort gelesen, entschlüsselt und angezeigt wird. Bitte beachten Sie, daß einige Paßwortverschlüsselungen (z.B. AWARD) keine eindeutige Rekonstruktion zulassen und somit lediglich Alternativpaßwörter generiert werden können. Beachten Sie außerdem, daß eine Anpassung des Paßwortes an das momentan verwendete Tastaturlayout automatisch vorgenommen wird und somit unter anderem die sonst übliche Vertauschung von Y und Z entfällt.

3.2 Paßwort deaktivieren

Mit Hilfe dieser Funktion können Sie aktive BIOS-Paßwörter deaktivieren. Es werden keine anderen BIOS-Einstellungen verändert.

Eine Deaktivierung ist nur möglich, wenn der Anwendung die für eine Deaktivierung nötigen Manipulationen der CMOS-Daten bekannt sind (BIOS-Paßwort-Deaktivierungs-Informationen – BPDI). Daher ist diese Funktion nicht für alle BIOS-Typen oder -Versionen verfügbar.

...(siehe "Paßwort rekonstruieren")...

Wenn Sie einen Eintrag als den Richtigen identifiziert haben, wählen Sie diesen aus und klicken anschließend auf "Deaktivieren". Daraufhin werden Änderungen an den BIOS-Einstellungen vorgenommen, die eine Deaktivierung des BIOS-Paßwortes zur Folge haben.

Ich weise hiermit ausdrücklich darauf hin, daß die Verwendung dieser Funktion zu irreparablen Systemschäden führen kann. Sollte sich herausstellen, daß das Paßwort doch nicht deaktiviert wurde bzw. sollte beim nächsten Bootvorgang ein Prüfsummenfehler angezeigt werden, so war Ihre Auswahl falsch. Ich empfehle in diesem Fall unbedingt die durch diese Anwendung vorgenommenen Änderungen rückgängig zu machen, da diese Änderungen nicht zum Erfolg geführt haben, aber möglicherweise andere fatale Folgen haben können.

3.3 Einstellungen zurücksetzen

Mit Hilfe dieser Funktion können Sie alle BIOS-Einstellungen auf ihre Standardwerte zurücksetzen. Unter anderem werden dabei auch aktive BIOS-Paßwörter deaktiviert.

Ein Deaktivieren mit dieser Funktion ist nur möglich, wenn das Paßwort im CMOS abgelegt wird und das BIOS im Falle ungültiger CMOS-Daten die BIOS-Einstellungen auf ihre Standardwerte zurücksetzt. Da diese Vorausetzungen für nahezu alle BIOS-Typen bzw. –Versionen zutreffen, sollte diese Funktion immer verfügbar sein.

Klicken Sie, nachdem Sie die gewünschte CMOS-Daten-Zerstörungs-Methode ("Intelligent" oder "Brutal") ausgewählt haben, auf den Button "Zurücksetzen" um die BIOS-Einstellungen für ungültig zu erklären. Beim nächsten Bootvorgang wird dies vom BIOS bemerkt, woraufhin in der Regel

eine Fehlermeldung ausgegeben wird. Anschließend werden vom BIOS alle wichtigen Einstellungen auf ihre Standardwerte zurückgesetzt, um korrekte BIOS-Einstellungen zu garantieren. Dadurch werden auch aktive BIOS-Paßwörter deaktiviert.

Durch das Zurücksetzen der Einstellungen gehen alle persönlich im BIOS vorgenommenen Einstellungen verloren. Das betrifft unter anderem auch die Festplatten-, Speicher- und CPU-Einstellungen. Das BIOS von Computern, die ca. nach 1995 hergestellt wurden, sollte in der Lage sein diese Informationen selbständig zu ermitteln. Ältere Computer besitzen in der Regel diese automatischer Datenträger-, Speicher- und CPU-Erkennung nicht. Hier müssen diese Informationen manuell von Ihnen wieder hergestellt werden, bevor sie mit dem Computer wieder arbeiten können. Bedenken Sie, daß auch bei neueren Computern die Standardeinstellungen nicht unbedingt die besten sind und somit auch hier Anpassungen nötig werden.

3.4 Tastatureingabe

Mit Hilfe dieser Funktion kann die beim Bootvorgang getätigte Tastatureingabe teilweise rekonstruiert werden.

Falls beim Starten des Computers eine Paßworteingabe erfolgte, so ist diese Teil der Tastatureingabe und kann auf diesem Weg ggf. teilweise sichtbar gemacht werden. Diese Form der Paßwortrekonstruktion funktioniert in der Regel bei allen BIOS-Typen und –Versionen, liefert aber nur Erfolge, wenn das Paßwort beim Booten eingegeben wurde und anschließend (bis zum Start von Windows) sehr wenig weitere Tastatureingaben erfolgten.

Technisch bedingt ist maximal eine Rekonstruktion der letzten 16 Zeichen möglich. Außerdem kommt es bei einigen BIOSen vor, daß alle Zeichen doppelt erscheinen (hier können also maximal 8 Zeichen rekonstruiert werden). Es ist auch möglich, daß die Reihenfolge der Eingabe nicht korrekt ermittelt werden kann. Beachten Sie außerdem, daß eine Anpassung des Paßwortes an das momentan verwendete Tastaturlayout automatisch vorgenommen wird und somit unter anderem die sonst übliche Vertauschung von Y und Z entfällt.

3.5 Master-Paßwörter

Auf dieser Seite finden Sie eine Liste möglicher Master-Paßwörter (auch Default-, Standard- oder Universalpaßwörter genannt). Das sind Paßwörter, die unabhängig vom momentan definierten Paßwort stets als gültig angesehen werden.

Viele BIOS-Typen bzw. –Versionen besitzen solche Hintertürchen. In den wenigsten Fällen sind diese aber bekannt und sobald diese bekannt werden, werden Sie in neueren BIOS-Versionen geschlossen. Das hat zur Folge, daß die meisten hier aufgeführten Master-Paßworter lediglich in älteren BIOS-Versionen funktionieren. Neuere Versionen besitzen entweder kein Master-Paßwort mehr oder aber es ist abhängig vom Motherboard-Hersteller und nicht mehr vom BIOS-Hersteller.

Stehen zwei Paßwörter in einer Zeile, so handelt es sich bei dem Zweiten um das an das momentan verwendete Tastaturlayout angepaßte. Welches von

beiden gültig ist abhängig davon, ob das BIOS den Hardware-Scancode oder den Software-Scancode auswertet.

Unter "Paßwort rekonstruieren" finden Sie unter anderem auch Einträge zur Rekonstruktion des Master-Paßwortes. Damit können ggf. auch mir unbekannte Master-Paßwörter rekonstruiert werden.

3.6 Änderungen rückgängig machen

Mit Hilfe dieser Funktion können Sie die zuletzt getätigten Änderungen an den BIOS-Einstellungen rückgängig machen.

Werden durch diese Anwendungen Änderungen an den BIOS-Einstellungen (CMOS-Daten) vorgenommen, so werden diese erst beim Beenden der Anwendung tatsächlich in das CMOS geschrieben. Gleichzeitig wird ein Backup der vorher gültigen CMOS-Daten angelegt.

Auf dieser Seite finden Sie eine Liste der 10 letzten Zeitpunkte, zu denen Änderungen an den BIOS-Einstellungen vorgenommen wurden. Wählen Sie einen Zeitpunkt aus und klicken auf den Button "Rückgängig machen", um die vor der Änderung gültigen BIOS-Einstellungen wiederherzustellen.

3.7 BIOS untersuchen

Hier können Sie die Liste der unterstützten BIOS-Typen bzw. -Versionen um das von diesem Computer verwendete BIOS erweitern, indem Sie der Anwendung helfen die zur Rekonstruktion bzw. Deaktivierung des BIOS-Paßwortes benötigten BIOS-Paßwort-Informationen (BPI) zu ermitteln.

Dazu müssen Sie im ersten Schritt ein bestimmtes BIOS-Paßwort einrichten und im zweiten Schritt deaktivieren. Außerdem müssen Sie im dritten Schritt einige Informationen über Ihr BIOS angeben (Typ, Version, Datum, ...), sofern Ihnen diese Informationen bekannt sind. Danach werden die BIOS-Paßwort-Informationen generiert mit deren Hilfe das Paßwort rekonstruiert bzw. deaktiviert werden kann.

Technisch bedingt ist das automatische Ermitteln der benötigten Informationen nicht immer möglich. Außerdem wird die Benutzung der generierten Informationen nur erlaubt, wenn diese mit hoher Wahrscheinlichkeit korrekt sind. Unabhängig davon ob die Benutzung erlaubt oder verboten wird, empfehle ich diese Informationen vor der Verwendung von mir prüfen zu lassen.

3.8 Allgemeine Hinweise zur Anwendung der Funktionen

Versuchen Sie zuerst die Funktionen, die keine Änderungen an den BIOS-Einstellungen bewirken. Dazu zählen "Paßwort rekonstruieren", "Tastatureingabe" und "Master-Paßwörter".

Falls die erste Gruppe von Funktionen erfolglos ist, versuchen sie die Funktionen, die kontrollierte Änderungen an den BIOS-Einstellungen durchführen. Dazu zählt die Funktion "Paßwort deaktivieren".

Falls auch die zweite Gruppe von Funktionen erfolglos ist, versuchen Sie die Funktionen, die die BIOS-Einstellungen komplett zerstören. Dazu dient die

Funktion "Einstellungen zurücksetzen". Die "brutale Methode" sollte aber nur verwendet werden, wenn die "intelligente Methode" fehlschlägt.

Falls die Funktion "Einstellungen zurücksetzen" erfolgreich war, empfehle ich anschließend die Funktion "BIOS untersuchen" auszuführen. Falls das Rekonstruieren oder Deaktivierung dadurch möglich gemacht werden konnte, sollte das Backup der vor dem "Zurücksetzen" gültigen BIOS-Einstellungen wiederhergestellt und das Paßwort rekonstruiert bzw. deaktiviert werden.

Sollte keine der durch diese Anwendung zur Verfügung gestellten Funktionen erfolgreich sein, so gibt es noch andere von dieser Anwendung nicht unterstützte Möglichkeiten das BIOS-Paßwort zu rekonstruieren, zu deaktivieren oder zu umgehen. Hierzu sei auf andere Paßwort-Cracker-Programme (CmosPwd, !BIOS) oder Internetseiten (www.bios-info.de, www.cgsecurity.org, www.11a.nu) verwiesen.

4 Anwendungsinformationen

4.1 Dateien

Diese Anwendung besteht aus folgenden Dateien:

- BiosPasswort.exe — Die Anwendung
- BiosPasswort.pdf — Hilfedatei
- smport.io — Gerätetreiber für direkte Portzugriffe
- file_id.diz — Kurzbeschreibungsdatei

Eine Installation ist nicht nötig. Bitte kopieren Sie diese Dateien in ein Verzeichnis Ihrer Wahl oder starten die Anwendung direkt von CD bzw. Diskette.

4.2 Systemvoraussetzungen

Diese Anwendung ist unter Windows 95/98/ME/NT/2K/XP oder höher lauffähig. Unter Windows NT/2K/XP müssen Sie Administratorrechte besitzen. Außerdem muß sich die Anwendung auf einem lokalen Datenträger befinden.

Wenn Sie die Anwendung auf einem schreibgeschützten Datenträger ausführen, sind die Funktionen "Änderungen rückgängig machen" und "BIOS untersuchen" nicht verfügbar, da keine Backups angelegt werden können. Um alle Funktionen nutzen zu können, ist das Kopieren der Dateien auf einen beschreibbaren Datenträger (z.B. Festplatte) nötig.

Die durch diese Anwendung angebotenen Funktionen mit Außnahme der Funktion "Master-Paßwörter" sind nur anwendbar, wenn die Anwendung auf dem betreffenden Computer ausgeführt werden kann. Sollte die Paßwortarfrage also beim Booten erscheinen (System-Paßwort), so ist diese Anwendung in der Regel wertlos.

4.3 Vertriebskonzept

Diese Anwendung ist Freeware: Das bedeutet, diese Anwendung besitzt keinerlei Einschränkungen und kann auf privater Ebene beliebig oft und lange verwenden werden. Im Gegenzug möchte ich Sie jedoch bitten mich bei der Anwendungsentwicklung sowohl durch Ihre eigene Mithilfe

als auch finanziell zu unterstützen. Zur Nutzung auf kommerzieller bzw. geschäftlicher Ebene ist eine Lizensierung erforderlich.

Ziel dieser Anwendung ist es, möglichst vielen Computeranwendern helfen zu können. Dafür benötigt die Anwendung aber wiederum Ihre Hilfe, denn die Liste der unterstützten BIOS-Typen, -Versionen und Paßwortarten ist keinesfalls vollständig.

Ich möchte Sie daher bitten die Funktion "BIOS untersuchen" auf Ihrem Computer auszuführen und mir das Ergebnis (BiosPasswort.bpi) per Mail zu übermitteln. Abgesehen davon, daß sie möglicherweise selbst einmal diese Anwendung benötigen, helfen sie dadurch einer Vielzahl von Computeranwendern. Außerdem werden Sie unter "Quelle (BPI)“ namentlich erwähnt.

Ich möchte Sie auch bitten mir das Master-Paßwort für Ihr BIOS mitzuteilen, sofern es Ihnen bekannt ist. Das gilt auch, wenn das Paßwort meiner Anwendung bereits bekannt sein sollte. Insbesondere ist dabei der BIOS-Typ, die BIOS-Version, der Motherboard-Herstellung, die BIOS-Identifikations-Nummer und das Paßwort selbst von Interesse.

Natürlich freue ich mich auch stets über Fehlermitteilungen und Verbesserungsvorschläge.

Sollte Ihnen diese Anwendung bei der Rekonstruktion, Deaktivierung oder Umgehung des BIOS-Paßwortes geholfen haben, so denken Sie bitte daran, daß die Anwendungsentwicklung viel Zeit und Geld in Anspruch genommen hat und auch weiterhin nehmen wird. Bedenken Sie auch, daß Sie die Rekonstruktion, Deaktivierung oder Umgehung des BIOS-Paßwortes durch andere Personen oder Firmen (z.B. dem BIOS- oder Motherboard-Hersteller) sie sehr viel Geld gekostet hätte.

Ich war so fair und habe Ihnen diese Anwendung kostenlos und ohne Einschränkungen zur Verfügung gestellt. Seien Sie bitte nun so fair und honorieren meinen Arbeit.

Überlegen Sie sich selbst, wie viel Ihnen diese Anwendung wert ist und überweisen den entsprechenden Geldbetrag auf mein Konto (Verwendungszweck: BiosPasswort). Ich freue mich über jeden Cent. Ab einer Spende von 5,00 EUR erhalten Sie auf Wunsch eine Lizenz für diese Anwendung.

Unabhängig davon, ob Sie bereit sind meine Arbeit zu honorieren, würde ich mich über einen Besuch meiner Homepage sehr freuen. Vielleicht möchten Sie sogar einen kleinen Eintrag in meinem Gästebuch hinterlassen?

Möchten Sie die Anwendung auf kommerzieller bzw. geschäftlicher Ebene einsetzen, so ist dies nur nach erfolgter Lizensierung gestattet. Bitte setzen Sie sich dazu mit mir in Verbindung.

5 Angaben zum Autor

5.1 Postadresse

Peter Weigel
Burger Hof 15
06124 Halle (Deutschland)

5.2 Internet- und E-Mail-Adresse

E-Mail: mail@peter-weigel.de
Homepage: http://www.peter-weigel.de

5.3 Bankverbindung

Institut: PSD Bank Braunschweig
Bankleitzahl: 27 09 09 00
Kontonummer: 56 02 51 26 00
IBAN / BIC: DE27 27090900 5602512600 / GENODEF1P02

6 Lizenzvereinbarung

Lesen Sie dieses Kapitel sorgfältig durch, bevor Sie diese Software verwenden. Sollten Sie mit dem Folgenden nicht einverstanden sein, so benutzen Sie die Software nicht und löschen diese von Ihren Datenträgern.

6.1 Nutzungserlaubnis

Ich gestatte hiermit ausdrücklich diese Software frei und kostenlos auf privater Ebene zu nutzen. Diese Anwendung besitzt keinerlei Einschränkungen. Es sind keine Lizenzabgaben an mich zu zahlen. Für die Nutzung auf kommerzieller bzw. geschäftlicher Ebene ist eine Lizensierung erforderlich. Ich verfüge über die erforderlichen Rechte, um diese Nutzungsgenehmigung zu erteilen.

6.2 Reproduktion und Weitervertrieb

Ich gestatte hiermit jedem eine unbegrenzte Anzahl Kopien dieser Software herzustellen und z.B. Online oder auf CD-ROM zu verbreiten, solange es sich um exakte Kopien ohne Veränderung (Weglassen oder Hinzufügen von Dateien, Verändern jeglicher Art) handelt. Es sind dabei keine Lizenzabgaben an mich zu zahlen. Die abgedruckte Softwarebeschreibung darf frei verwendet werden, um das Programm vorzustellen. Ich verfüge über die erforderlichen Rechte, um diese Vertriebsgenehmigung zu erteilen.

6.3 Produktunterstützung

Als Anwender dieser Software haben Sie keinen Anspruch auf Produktunterstützung (‘Support’) durch den Autor. Soweit technisch möglich wird jedoch kostenlose Produktunterstützung per Email angeboten.

6.4 Haftung

Der Autor übernimmt keinerlei Gewährleistung für diese Software. Er übernimmt insbesondere keine Haftung für die Tauglichkeit, die Eignung für einen bestimmten Zweck und die Nichtverletzung der Rechte Dritter. Da es nach aktuellem Stand der Technik nicht möglich ist, Fehler in Softwareprodukten auszuschließen wird darauf hingewiesen, daß diese Software möglicherweise technische Fehler enthält. Der Autor kann daher

keinerlei Gewährleistung für die Software übernehmen. In keinem Fall kann der Hersteller haftbar gemacht werden für Schäden, die aus Nutzungsausfall, Verlust von Daten oder entgangenem Gewinn resultieren und durch diese Software oder im Zusammenhang mit der Verwendung dieser Software entstanden sind. Ich versichere jedoch, daß diese Anwendung vor der Veröffentlichung ausführlich getestet wurde, und ich keine (schwerwiegenden) Mängel feststellen konnte.

6.5 Copyright

Alle Teile dieses Anwendungspackets gehören ausnahmslos mir und sind 100%ig mein geistiges Eigentum (Ausnahmen: siehe Abschnitt 7.1), sollten Sie die Teile einzeln oder unter ihrem Namen weitergeben, bin ich gezwungen rechtliche Schritte gegen Sie einzuleiten. Gleiches gilt für andere Verstöße gegen die o.a. Lizenzvereinbarungen.

6.6 Gültigkeit dieser Lizenzvereinbarungen

Die Lizenzvereinbarungen für diese Software können von Zeit zu Zeit angepaßt werden. Daher gelten stets die mit der aktuellsten Version dieser Software ausgelieferten Lizenzbestimmungen. Sollte eine der hier aufgeführten Klauseln ungültig sein, so bleibt der Rest unberührt gültig.

6.7 Hinweise

Alle erwähnten Warenzeichen und Copyrights gehören ihren jeweiligen Besitzern. Für alle Produkte gelten die allgemeinen Copyrightbestimmungen.

7 Anmerkungen

7.1 Idee

Die Idee zu dieser Anwendung hatte ich bereits 1998. Es handelte sich dabei um eine DOS-Anwendung zur Entschlüsselung des AMI-Paßwortes (Amipsw). Außerdem entstand zu dieser Zeit eine DOS-Anwendung zur Betrachtung des CMOS-Inhaltes (CMOSVIEW), die im Jahr 2000 komplett neu als Windows-Anwendung entwickelt wurde (Peters CmosInfo). Die ursprüngliche DOS-Variante wurde übrigens nie veröffentlicht. Im gleichen Jahr wurde eine Windows-Anwendung zum zeitgesteuerten automatischen Einschalten des Computers entwickelt (Peters PowerControl). Und auch die Ursprungsversion von Peters BiosPaßwort (Peters BiosPwd) stammt aus diesem Jahr. Die mit Hilfe dieser Anwendungen gesammelten Erfahrungen aus der Zeit zwischen 1998 und 2003 wurden nun gebündelt und dienten als Anstoß zur kompletten Neuentwicklung einer Anwendung zur Rekonstruktion, Deaktivierung oder Umgehung von Bios-Paßwörtern.

7.2 Quellcode

Zum CMOS-Zugriff unter Windows NT/2K/XP habe ich den Gerätetreiber von Alexander Weitzman (smport) in abgewandelter Form in diese Anwendung eingearbeitet. Diese Komponente ist Public Domain. Außerdem wurden von verschiedenen Personen entwickelte Entschlüsselungs-algorithmen für BIOS-Paßwörter in diese Anwendung integriert. Die zur Rekonstruktion oder Deaktivierung nötigen Bios-Paßwort-Informationen (BPI) wurden mir von verschiedenen Personen zur Verfügung gestellt, oder

anderen Anwendungen (Public Domain, GPL[1]) entnommen. Die einzelnen Quellen können den Zusatzinformationen zu den Einträgen unter "Paßwort rekonstruieren" bzw. "Paßwort deaktivieren" entnommen werden.

7.3 Bekannte Bugs

Unter Windows XP funktioniert der direkte Speicherzugriff nicht richtig. Dadurch funktioniert unter anderem die Funktion "Tastatureingabe" nicht. Da ich die Anwendung noch nicht ausführlich unter Windows XP testen konnte, konnte das Problem bisher auch noch nicht beseitigt werden. Möglicherweise ist das Problem in der aktuellen Version bereits behoben.

Die CMOS-Erkennung funktioniert nicht bei allen Computern korrekt, da es keinen einheitlichen Standard für den Zugriff auf die CMOS-Daten (≥ 128) gibt. Eine fehlerhafte Erkennung hat zur Folge, daß die CMOS-Größe falsch erkannt wird, der Zugriff auf die CMOS-Daten fehlerhaft ist und somit die meisten durch diese Anwendung zur Verfügung gestellten Funktionen nicht korrekt funktionieren. Selbst wenn Ihr CMOS nicht korrekt erkannt wurde, sollten Sie mit die BPIs zusenden, da ich nur dadurch die CMOS-Erkennung verbessern kann.

Der Zugriff auf die CMOS-Daten funktioniert nicht bei allen Computern korrekt. Bisher habe ich das Phänomen lediglich bei einem relativ neuen PC (Phoenix-Award BIOS v6.00PG, 01/20/2003-AK32-6A6LVH28C-00) festgestellt. Hierbei lieferten die CMOS-Zugriffe völlig falsche Daten. Die Ursache ist zur Zeit unbekannt, da ein ausführlicher Test nicht möglich war.

Nach dem Neustart des Computers dauert der erste Start der Anwendung unter Windows NT/2K/XP unter Umständen sehr lange. Ursache dafür ist das Laden des Gerätetreibers für direkte Portzugriffe, dessen erstmaliges Laden (pro Sitzung) etwas länger dauern kann.

7.4 Shareware-Autoren-Vereinigung

Als Sharewareautor bin ich Mitglied der Shareware-Autoren-Vereinigung (SAVE). Neben hochrangigen Shareware- und Freewareprodukten andere Autoren bin auch ich mit meinen Anwendungen dort vertreten. Schauen Sie doch einfach mal auf der Internetseite http://www.s-a-ve.com oder http://www.deutsche-shareware.de vorbei! Diese Anwendung finden Sie dort unter der Kennung PWE – BPC (**P**eter **We**igel – **B**ios-**P**aßwort-**C**racker).

8 Versionsgeschichte

03.10.2000	Version 1.00	Erste Realisierung dieser Programmidee.
17.03.2001	Version 1.01	Probleme beim Entschlüsseln (Endlosschleifen) behoben.
21.01.2002	Version 2.00	Design geändert, neue Funktionen hinzugefügt und Windows NT/2K/XP-tauglich gemacht.

[1] Die Tatsache daß diese Anwendung nicht unter GPL steht, obwohl Code von GPL-Anwendungen verwendet wurde, stellt keinen Verstoß gegen die GNU GPL dar. Denn: Die Anwendung zählt als unabhängige und eigenständige Arbeit (siehe Ende Abschnitt 2 GNU GPL). Die BPIs unterliegen nicht der GPL, selbst wenn diese Informationen solchen Anwendungen entnommen wurden. Die Entschlüsselungsalgorithmen stellen in der Regel einfache Bitmanipulationen dar, bestehen also in den meisten Fällen aus einer einzigen Codezeile, und sind, sofern diese Algorithmen nicht durch Patente geschützt sind, ohnehin frei.

07.02.2002	Version 2.10	INPUT-Funktion verbessert, kleine Bugs beseitigt und Design optimiert.
09.03.2002	Version 2.20	Das Paßwort kann jetzt direkt deaktiviert werden (AMI, AWARD).
05.04.2003	Version 2.21	Fehler beim Start unter Windows XP durch Deaktivierung direkter Speicherzugriffe beseitigt.
15.03.2004	Version 3.0	Komplette Neugestaltung der Anwendung (Funktion, Design). Namensänderung von „Peters BiosPwd“ zu „Peters BiosPasswort“.
29.03.2004	Version 3.1	Automatischen Anpassung an die verwendete Bildschirmschriftgröße. Startseite ist „BIOS untersuchen“, falls gerade eine Analyse durchgeführt wird. Beim Neustart des Computers mittels dieser Anwendung wird diese automatisch wieder gestartet. Korrektur des Entschlüsselungsalgorithmus ACER. Hinzufügen einiger neuer BPIs.
20.09.2004	Version 3.2	Kleine Anpassung der Dokumentation. InfoBox überarbeitet. Analyseinformationen (BIOS untersuchen) ergänzt.

... die nächste Version kommt bestimmt.