ERNW Newsletter 22 / März 2008

Liebe Partner, liebe Kollegen,

willkommen zur 22. Ausgabe des ERNW-Newsletters mit dem Thema:

Sicherheitsbetrachtungen von Wechselmedien, insbesondere USB-Sticks unter Windows

Version 1.0 vom 24. März 2008

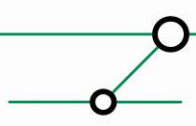
von: Friedwart Kuhn (fkuhn@ernw.de)

Dieses Dokument verfügt über eine eingebettete digitale Signatur[1]. Wenn Sie Fragen zur Darstellung der Signatur haben, wenden Sie sich bitte an cwerny@ernw.de .

Abstract

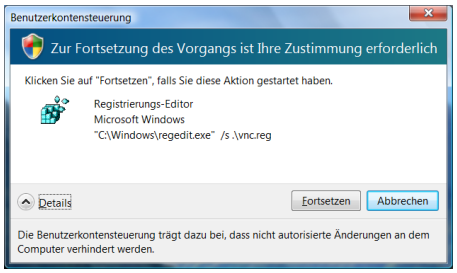
Dieser Newsletter beschreibt ausgehend von einem Fallbeispiel die Fragen, die sich das IT-Sicherheitsmanagement beim unternehmensweiten Einsatz von USB-Laufwerken stellen sollte. Neben einer Risikobetrachtung werden technische und organisatorische Maßnahmen zur Problemlösung unter Einbezug von Windows Vista behandelt.

[1] *Der Verfasser autorisiert den Geschäftsführer der ERNW GmbH, Roland Fiege, dieses Dokument digital zu signieren.*



1 EIN (UN)GEWÖHNLICHER ANGRIFF?

In Ihrer Organisation wurden kürzlich neue U3-USB-Sticks[2] zentral angeschafft. Diese Sticks ermöglichen für vorbereitete U3-Anwendungen eine mit dem Stick transportable Arbeitsumgebung, die nach Konfiguration eine per 256-Bit AES-verschlüsselte Speicherung von Dokumenten zulässt[3]. Gängige Applikationen, die für U3 vorbereitet sind (wie etwa der Browser), sollen vom Stick ohne Installation auf dem Rechner, in den der Stick gesteckt wird, laufen. Sie machen jedoch Begegnung mit einem leicht modifizierten Exemplar dieser Gattung: Nach der automatisch verlaufenden Gerätetreiberinstallation auf Ihrem Microsoft Windows Vista-PC verfügen Sie über eine neues CD-ROM-Laufwerk[4], das Sie, wie gewohnt, mit einem Doppelklick öffnen. Darauf hin erscheint die Benutzerkontensteuerung (UAC)[5], und zwar zunächst mit einer Meldung, die von einer vertrauenswürdigen Betriebssystemkomponente – dem Registrierungseditor – stammt:



Wenn Sie an dieser Stelle auf *Fortsetzen* klicken, wird auf Ihrem System ein VNC-Server ohne weitere Rückfragen installiert[6].

---

[2] *U3 ist eine Technologie, die von Speicherherstellern (u. a. SanDisk) entwickelt wurde, um Applikationen und Arbeitsumgebung eines Benutzers portabel zu machen.* U3 *soll dabei für die drei wesentlichen Gedanken dieser Technologie stehen:* Simplified for You, Smarter about You, As mobile as You (siehe auch: http://www.u3.com/default.aspx)

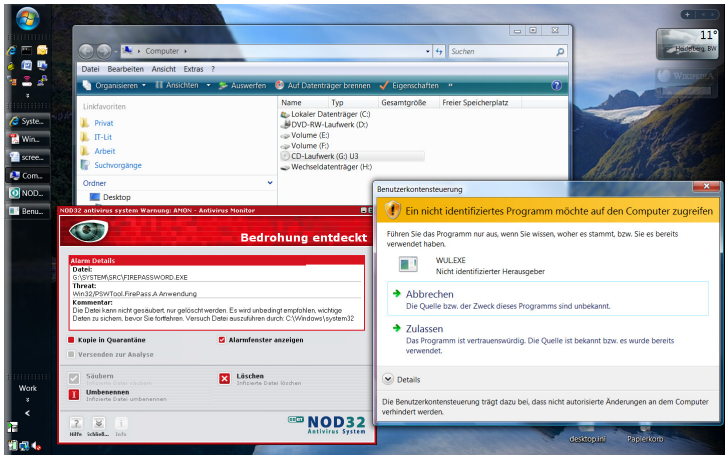
[3] *Ein Vertreter dieser Gattung ist etwa der* Cruzer Enterprise *von SanDisk (Datenblatt siehe: http://www.sandisk.com/Assets/File/pdf/Sandisk_Cruzer_Enterprise.pdf).*

[4] *U3-USB-Sticks wirken auf den ersten Blick wie gewöhnliche USB-Sticks, sie emulieren jedoch ein zusätzliches CD-ROM-Laufwerk, so dass Windows-Rechner beim Einstecken des Sticks ein (USB-) CD-ROM-Laufwerk und einen (USB-) Wechseldatenträger erkennen.*

[5] *UAC = User Account Control, zu deutsch* Benutzerkontensteuerung. *Angenommen wird eine Vista-Installation, in der die Benutzerkontensteuerung* ***nicht*** *deaktiviert wurde (dies ist die Defaulteinstellung). Wenn die Benutzerkontensteuerung deaktiviert wurde – wovon dringed abzuraten ist, was jedoch aus vermeintlichen Bequemlichkeitsargumenten häufig geschieht – erscheint die Meldung der Benutzerkontensteuerung nicht, und der VNC-Server wird (administrative Berechtigungen vorausgesetzt) installiert, ohne dass der Benutzer davon etwas erfährt.*

[6] *Die Befehlszeile, mit der der Registrierungseditor aufgerufen wird, wird erst durch das Klicken auf* Details *sichtbar; ansonsten wird ein gewöhnlicher Vista-Benutzer diese UAC-Meldung – die auch noch von einer vertrauenswürdigen Komponente kommt, höchstwahrscheinlich einfach bestätigen. Im Übrigen vermittelt auch Microsoft mit der Betonung, dass der dargestellte Typ von UAC-Meldung von einer (vertrauenswürdigen) Betriebssystemkomponente erzeugt wird, den Eindruck, die dadurch ausgeführten Aktionen seinen ebenfalls vertrauenswürdig. Es gilt jedoch, sich stets vor Augen zu halten, dass nur die Komponente (nämlich der Registrierungseditor) per se vertrauenswürdig ist, nicht aber die Aktion die damit ausgeführt wird (in diesem Fall die klammheimliche Installation eines VNC-Servers).*
Der Secure Desktop *wurde für alle UAC-Screenshot deaktiviert. Dies beeinflusst in diesem Fall ausschließlich die Darstellung der Warnmeldung (mit aktiviertem* Secure Desktop *wäre ein Screenshot nicht möglich, denn es ist genau die Aufgabe des* Secure Desktop*, den Zugriff für jede weitere Anwendung für die Zeit der Darstellung des Dialogs durch die Benutzerkontensteuerung zu unterbinden).*

Hellhöriger werden Sie vermutlich dann bei der darauf folgenden Meldung (ebenfalls nach dem Doppelklick auf das U3-CD-ROM-Laufwerk):



…doch vielleicht erst einmal der Reihe nach[7].

2 MOTIVATION

Szenarien des *Social Engineering* und der Unachtsamkeit

Stellen Sie sich vor, Sie bitten Ihren Kollegen, Ihnen seinen USB-Stick zu geben, damit Sie ihm kurz die Powerpoint-Präsentation geben, die er für Sie fertig machen soll. Sie verwenden in Ihrem Unternehmen die neuen und sicheren USB-Sticks eines bekannten Herstellers und genau einen solchen hält Ihnen Ihr Kollege hin. Sie stecken den USB-Stick in Ihr Notebook und…
Wie die Geschichte weiter geht, hängt von der Sicherheitspolicy Ihres Unternehmens, von dem auf Ihrem Notebook ausgeführten Betriebssystem und von der Betriebssystem-Konfiguration selbst ab.

Die Geschichte hätte aber auch noch unverfänglicher, was in diesem Fall heißt, sie hätte gänzlich außerhalb Ihres Bewusstseins statt finden können. In diesem Fall könnte die Geschichte folgendermaßen begonnen haben: Stellen Sie sich vor, Sie sind an Ihrem Büro und Arbeiten an der Präsentation, die Sie gleich Ihrem Kollegen per E-Mail schicken wollen. Sie gehen kurz auf die Toilette und im Gang begegnen Sie einem Mitarbeiter der IT-Firma, von deren Besuch Sie Ihr IT-Leiter unterrichtet hat. Sie grüßen. Drei Minuten später sind Sie wieder an Ihrem Arbeitsplatz.
Auch hier hängt das, was in der Zwischenzeit geschehen sein könnte – kriminelle Energie des Mitarbeiters der IT-Firma vorausgesetzt[8] – wieder von der Sicherheitspolicy

[7] *Weitere Screenshots zum Beispielverhalten der getesteten Malware zusammen mit einem Vista-System finden sich in Abschnitt 8.*
[8] *Oder vielleicht war es auch nur jemand, der den Anschein erweckte, zu dieser Firma zu gehören.*

Ihres Unternehmens, von dem auf Ihrem Notebook ausgeführten Betriebssystem und von der Betriebssystem-Konfiguration selbst ab.

Was ist diesen beiden Szenarien gemein? Dass – wie der Leser im zweiten Fall zu Recht vermutet – ein fremder USB-Stick (oder allgemeiner *Wechselmedium*) in das eigene Gerät gesteckt wird. Doch es gibt auch das dazu inverse Szenario: Der eigene USB-Stick (oder das eigene Wechselmedium) wird in einen fremden Rechner gesteckt.
Oder: Stellen Sie sich vor, ein Freund bittet Sie, ihm kurz Ihren USB-Stick zu geben, damit er Ihnen die Fotos vom letzten gemeinsamen Wochenende im Schwarzwald kopieren kann. Die Firmendaten auf Ihrem USB-Stick haben Sie ja in einem Passwortgeschützten Zip-Archiv abgelegt. In Ihrer Firma verwenden Sie schließlich Winzip in der bewährten Version 8.0. Oder: Sie könnten versehentlich Firmendaten auf einem privaten USB-Stick (oder auch umgekehrt!) gespeichert haben, selbst wenn es eine Policy gibt, die dies verbietet. Auch hier gilt wieder, wie in den vorherigen fiktiven -;) Beispielen: Wie die Geschichte ausgeht hängt von der Sicherheitspolicy Ihres Unternehmens (bzw. wie die Mitarbeiter die Policy leben) und – in diesem Fall – von dem Betriebssystem und dessen Konfiguration ab, das auf dem Rechner Ihres Freundes ausgeführt wird.

Im ungünstigen aber nicht unwahrscheinlichen Fall landen Firmen- wie private Daten in den Händen von Ihnen unbekannten und nicht vertrauenswürdigen Personen. Und wenn sich diese Daten als wertvoll erweisen, dann können sie etwa an Ihren ärgsten Konkurrenten verkauft werden, und Sie fragen sich, weshalb der Konkurrent das Produkt früher auf den Markt bringen konnte, obwohl es doch so schien, als ob sie vorne gelegen hätten. Wie anfällig viele Unternehmen für *Social Engineering* oder einfache Unachtsamkeit mit Datensicherheit im Zusammenhang mit USB-Sticks sind, zeigt eine im Januar 2007 durchgeführte *Security Awareness Campaign* der britischen NCC Gruppe: Sie verschickte 500 präparierte USB-Sticks an Finanzverantwortliche britischer Unternehmen mit einer anonymen Einladung zu einer Feier. Die Bestätigung sollte über eine Webseite geschehen, die von dem USB-Stick aufgerufen wurde, sobald dieser in den Rechner gesteckt wurde. 47% der Empfänger steckten den USB-Stick in den Rechner, klickten eine Warnung beiseite und die Webseite wurde geöffnet.[9]

Es gilt also zwei grundsätzlich unterschiedliche Szenarien bei der Sicherheits-betrachtung von Wechselmedien, insbesondere USB-Sticks zu untersuchen:

- den fremden USB-Stick im eigenen PC

- den eigenen USB-Stick im fremden PC

Doch noch einmal der Reihe nach: Vor der Betrachtung der Bedrohungsszenarien steht die Betrachtung dessen, was das schützenswerte Gut ist, und welches die Schutzziele hinsichtlich dieses Guts sind.

[9] *Vgl. http://www.nccgroup.com/cms_content_ncc/attachments/Interims%20Presentation%20January%202007.pdf.*

3 'VERMÖGENSGEGENSTÄNDE' (ASSETS) UND SCHUTZZIELE (OBJECTIVES)

Der englische Begriff *Asset*, der je nach Kontext eine Vielzahl von Bedeutungen tragen kann, lässt sich nur unzureichend mit 'materiellen und immateriellen Vermögenswerten' übersetzen und wird daher beibehalten. Hier sind unter Asset Kundendaten oder auch eigene Firmendaten, insbesondere solche, die einen Vermögenswert darstellen, zu verstehen.

Etwas allgemeiner betrachtet, gelten zwar für jedes Asset die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, im Fall von Wechselmedien, für die die exemplarischen Bedrohungsszenarien beschrieben wurden, ist das vorrangige Schutzziel jedoch die Wahrung der Vertraulichkeit.[10]

4 BEDROHUNGEN UND VULNERABILITIES

Welche Bedrohungen gibt es gegen die Assets? Da der Schutz der Vertraulichkeit das primäre Schutzziel ist, ist die Bedrohung dieses Schutzziels der Verlust oder auch Bruch eben dieser Vertraulichkeit. Der Bruch der Vertraulichkeit kann dabei in Abhängigkeit von der existenten – oder aber auch nicht existenten – Policy und in Abhängigkeit davon, wie diese Policy gelebt wird, aus einem der beiden oder aus der Kombination der beiden folgenden generischen Vertraulichkeitsbrüche bestehen:

- dem Bruch der Vertraulichkeit durch unautorisierten physischen Zugriff
- dem Bruch der Vertraulichkeit durch unautorisierten logischen Zugriff

Für beide Arten des unautorisierten Zugriffs sind dabei wieder die beiden Szenarien:

- fremder USB-Stick im eigenen PC und
- eigener USB-Stick im fremden PC zu betrachten.

Um unautorisierten physischen Zugriff handelt es sich, wenn eine fremde Person etwa in unserer Abwesenheit ihren uns fremden USB-Stick in unseren Rechner steckt. Um einen unautorisierten physischen Zugriff handelt es sich aber auch, wenn eine uns vertrauenswürdige Person ihren USB-Stick in unseren Rechner steckt, obwohl es eine Firmenpolicy gibt, die die Verwendung nur von definierten Firmen-USB-Sticks und die Verwendung von diesen nur zum Datentransport zwischen definierten Rechnern gestattet.

Um einen unautorisierten logischen Zugriff handelt es sich, wenn sich Malware auf dem fremden USB-Stick etwa die administrativen Berechtigungen des angemeldeten

[10] *Zwar könnte auch die Integrität der jeweils betrachteten Daten (auf dem USB-Stick oder auf dem lokalen PC) eine Rolle spielen, doch beträfe dies eher ganz spezielle Angriffsmethoden und –ziele (sog.* targeting attacks*), die bei dieser Untersuchung* out of scope *sind. Auch das Sicherheitsziel* Verfügbarkeit *spielt bei der Speicherung von Daten auf Wechselmedien eine untergeordnete Rolle und wird daher vernachlässigt.*

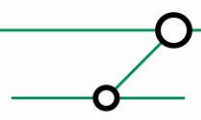
Benutzers zunutze macht, um unautorisiert Passwort-Hashes oder beliebige Dateien vom Rechner auf den USB-Stick zu kopieren. Um unautorisierten logischen Zugriff handelt es sich auch, wenn Malware auf einem Rechner einer vertrauenswürdigen Person unautorisierte Daten vom eigenen USB-Stick auf diesen (infizierten) Rechner kopiert.

Ganz konkret ergeben sich aus der Bedrohung durch unautorisierten physischen und /oder unautorisierten logischen Zugriff Bedrohungen wie:

- Datendiebstahl
- Booten eines fremden Betriebssystems
- Malware-Infektion
- Systemkompromittierung
- Non-Compliance (durch Mischung von privaten mit Geschäftsdaten)

Diese Bedrohungen bestehen aufgrund von Vulnerabilities (oder 'Schwächen'). Vulnerabilities können ihren Ursprung im Design, in der Technik oder in der Organisatorik haben. Vulnerabilities sind etwa:

- Dateien sind meistens nicht verschlüsselt
- Benutzer arbeiten besonders bei Windows-Betriebssystemen häufig mit administrativen Berechtigungen
- Kennwörter sind schwach
- Benutzer verfügen über keine Sensibilisierung beim Umgang mit eigenen und fremden Daten
- Rechner befinden sich nicht auf dem aktuellen Patchlevelstand



5 RISIKOBETRACHTUNG

Die nachfolgende generische und qualitative Risikobetrachtung setzt Bedrohungen, ihre Eintrittswahrscheinlichkeiten und Vulnerabilities zusammen mit den Auswirkungen in ein Verhältnis und liefert eine Aussage darüber, welche Risiken zuerst adressiert werden müssen. Für die hier aufgeführte Risikobetrachtung gelten die folgenden Randbedingungen:

- Die Zahlenwerte für Eintrittswahrscheinlichkeit, Vulnerability und Auswirkung (Impact) werden aus einer Skala von eins bis fünf mit *eins* als niedrigstem und *fünf* als höchstem möglichen Wert gewählt[11].

- Die gewählten Werte für die Eintrittswahrscheinlichkeiten entsprechen grob gemittelten Erfahrungswerten.

- Die gewählten Werte für die Auswirkungen hängen in hohem Maße von der individuellen Umgebung, ihrer Konfiguration und von der Bewertung durch das Management ab.

- Das berechnete Risiko entsteht aus einfacher Multiplikation der Faktoren *Eintrittwahrscheinlichkeit, Vulnerability* und *Auswirkung*.[12]

- Benutzer-Sensibilisierung – meistens als *Security Awareness* bezeichnet – kann den Umgang mit USB-Sticks erheblich beeinflussen. Dieser Faktor ist bei der Analyse nicht einbezogen. In einer detaillierteren Analyse könnte er als Gewichtungsfaktor einbezogen werden.

Dazu sollen noch zwei weitere Faktoren berücksichtigt werden: Unautorisierter physischer Zugriff kann zumindest teilweise durch eine Policy eingeschränkt werden, die etwa die Verwendung von eigenen USB-Sticks in 'fremden' Rechnern regelt (z. B. verbietet). Unautorisierer logischer Zugriff kann gut durch Kryptoverfahren vereitelt werden, da das Ziel des unautorisierten logischen Zugriffs, nämlich die Erlangung der eigentlichen (unverschlüsselten) Daten mit Kryptoverfahren ins Leere läuft. Sowohl die Verwendung von Kryptoverfahren als auch das Vorhandensein einer Policy sind zwei Faktoren, die Auswirkung (Impact) und Risiko der geschilderten Bedrohungen vermindern. Deshalb werden bei beiden Szenarien (fremder Stick im eigenen PC, eigener Stick im fremden PC) das Vorhanden- und das Nichtvorhanden-Sein dieser beiden Faktoren getrennt bewertet.

Das unter diesem Abschnitt bisher Gesagte gilt nun für die beiden von einander zu unterscheidenden Szenarien: fremder USB-Stick im eigenen PC und eigener USB-Stick im fremden PC:

---

[11] *Kleinere Skalen – etwa eins bis drei – bieten i. d. R. zu wenig Flexibilität, größere Skalen – z. B. eins bis zehn – machen die Bewertung meistens zu komplex.*

[12] *In einem ersten Schritt genügt eine solchermaßen durchgeführte Risikoanalyse, um sich einen Überblick zu verschaffen. Für die Beantwortung detaillierter Fragestellungen und für Feintuning können die einzelnen Multiplikatoren mit unterschiedlichen Faktoren gewichtet werden.*

Fremder USB-Stick im eigenen PC

Bedrohung	Eintrittswahr-scheinlichkeit	Vulnerability	Auswirkung (Impact)	Risiko
Boot eines fremden Betriebssystems (mit Policy[13])	1	1	4	4
Boot eines fremden Betriebssystems (ohne Policy)	1[14]	2[15]	4	8
Malware-Infektion (mit Policy)	1	2	5	10
Malware-Infektion (ohne Policy)	2[16]	2	5	20
Datendiebstahl[17] (mit Policy)	1	3	4	12
Datendiebstahl (ohne Policy)	2	3	4	24
Systemkompromittierung (mit Policy)	1	3	5	15
Systemkompromittierung (ohne Policy)	2[18]	3	5	30

[13] *Das bloße Vorhandensein einer Policy als geschriebenes oder auch publiziertes Dokument ist noch keine Aussage darüber getroffen, ob diese Policy auch gelebt wird. Bei der Analyse wird bei dem Attribut* mit Policy *davon ausgegangen, dass diese Policy auch implementiert ist, d. h. gelebt wird.*
[14] *Bleibt auch ohne Policy sehr gering, da das Booten eines fremden Betriebssystems vom USB-Stick einen vom Benutzer kaum zu übersehenden Eingriff darstellt.*
[15] *Die Vulnerability ist höher, denn es könnte eine Policy geben, die eine sichere BIOS-Konfiguration vorschreibt (und damit das Booten über USB verhindert).*
[16] *Ohne Policy höher, da der Umgang mit USB-Sticks eben nicht geregelt ist.*
[17] *Wie in der nachfolgenden Tabelle in bezug auf die Data Exposure, so könnten auch in dieser Tabelle beim Datendiebstahl die Fälle mit und ohne Kryptoverfahren betrachtet werden. Da der Fokus der Analyse jedoch auf Wechselmedien (USB-Stick) und nicht auf Endgeräte-Sicherheit liegt, wird diese Unterscheidung hier nicht vorgenommen.*
[18] *Ebenso.*

Eigener USB-Stick im fremden PC

Bedrohung	Eintrittswahr-scheinlichkeit	Vulnerability	Auswirkung (Impact)	Risiko
Data exposure[19] nicht klassifizierter[20] Daten (mit Krypto)	3[21]	1[22]	1[23]	3
Data exposure nicht klassifi-zierter Daten (ohne Krypto)	3	2	1	6
Data exposure klassifizierter Daten (mit Krypto)	3	1	4	4
Data exposure klassifizierter Daten (ohne Krypto)	3	2	4	24
Infektion des fremden[24] Rechners (mit Policy[25])	1	1	5[26]	5
Infektion des fremden Rechners (ohne Policy)	2	2	5	20
Non-Compliance /Haftungs-fragen (mit Policy)	2	1	4-5[27]	8-10
Non-Compliance /Haftungs-fragen (ohne Policy)	3	2[28]	3[29]	18

[19] Data exposure *umfasst hier sowohl den Datendiebstahl durch unautorisiertes Kopieren der Daten vom USB-Stick auf den Fremdrechner als auch den in der Praxis viel häufiger anzutreffenden Fall der möglichen Offenlegung der Daten auf dem USB-Stick durch Verlust (oder auch Diebstahl) des USB-Sticks.*

[20] *Wegen des großen Unterschieds hinsichtlich des Impacts erweist es sich erfahrungsgemäß als sinnvoll, klassifizierte Daten in der Risikoanalyse von nicht klassifizierten Daten zu unterscheiden. Erst eine weiter führende Analyse würde eine Unterscheidung von verschiedenen Klassifizierungsstufen sinnvoll machen.*

[21] *Erfahrungsgemäß ist die Eintrittswahrscheinlichkeit ganz grob gemittelt 'mittel' (3).*

[22] *Der Wert für die Vulnerability, die der Eintrittswahrscheinlichkeit für Data Exposure Vorschub leistet, ist in sehr hohem Maße von den eingesetzten Kryptoverfahren abhängig. Bei der Punktvergabe werden nach aktuellem Maßstab noch sichere Verfahren angenommen, also mindestens 128-Bit bei symmetrischen und mindestens 1024-Bit bei asymmetrischen Verschlüsselungsverfahren.*

[23] *Das in bezug auf die Vulnerability Gesagte ist auch hinsichtlich der Auswirkung zu beachten.*

[24] *Als 'fremder' Rechner wird ein Kunden- /Geschäftspartner-PC angenommen.*

[25] *Um die generische Analyse nicht unnötig komplex zu gestalten, wird nicht zwischen einer Policy des eigenen Unternehmens und /oder einer Policy des fremden Unternehmens unterschieden; es geht bei der Punktvergabe mit Policy darum, dass es (irgend) eine den Umgang mit USB-Geräten regelnde Policy gibt.*

[26] *Infektion eines Kunden- /Geschäftspartner-PCs wird als ungünstigster Impact bewertet.*

[27] *Non-Compliance trotz Policy kann zu einer fünf führen.*

[28] *Das Fehlen der Policy leistet der Eintrittswahrscheinlichkeit gerade in punkto Vulnerability als ein primärer Faktor Vorschub (dies ist etwa im Fall des Datendiebstahls der vorausgehenden Tabelle nicht der Fall; weshalb der Punktwert in bezug auf die dortige Vulnerability unabhängig von einer Policy ist).*

[29] *Non-Compliance ohne Policy kann nicht mit einem hohen (vier) oder sehr hohen (fünf) Wert belegt werden.*

Interpretation und Bemerkungen zu den Tabellen

Aus den Werten lassen sich folgende allgemeine Schlüsse ziehen:

(1) Die Tabellen verdeutlichen tendenzartig die Verhältnisse verschiedener Risiken zu einander und zeigen auf, welche Risiken zuerst adressiert werden müssen.

(2) Bei dem Szenario des fremden USB-Sticks im eigenen Rechner sind Systemkompromittierung und Datendiebstahl die größten und deshalb zuerst zu adressierenden Risiken.

(3) Bei dem Szenario des eigenen USB-Sticks im fremden Rechner sind dagegen Daten Exposure und Infektion des Fremdrechners die größten und deshalb zuerst zu adressierenden Risiken.

(4) Durch die Implementierung einer Policy zum Umgang mit Wechselmedien (USB-Sticks) können einige Risiken in beiden Szenarien deutlich gesenkt werden.

(5) Durch die Verwendung von Kryptoverfahren zur Speicherung von Daten auf USB-Sticks /Wechselmedien kann das Risiko der Daten Exposure (durch die Wechselmedien) drastisch gesenkt werden.

Nicht direkt in der Bewertung berücksichtigt, aber bei der individuellen Umgebung einzubeziehende Aspekte sind:

(a) Die Stärke des Authentifizierungsverfahrens beeinflusst die Sicherheit der darunter liegenden Kryptoverfahren: Wenn die Verschlüsselung etwa durch eine schlechte Implementierung[30] auf einfache Art und Weise gebrochen werden kann, dann ist die Vertraulichkeit nicht gesichert. Werden Dateien etwa per PGP-Verschlüsselung gespeichert, so hängt der 'Grad ihrer Vertraulichkeit' von der Passparaphrase des Schlüssels ab. Gleiches gilt für den Verschlüsselungsschlüssel[31] bei Verwendung von EFS in Windows-Systemen. Noch sichere Verschlüsselungsmethoden werden durch Multifaktor-Authentifizierung, z. B. mit Hilfe von Smartcards erreicht. So können Daten mit einem auf einer Smartcard oder auf einem Hardware-Token gespeicherten Verschlüsselungszertifikat sehr sicher verschlüsselt gespeichert werden[32].

(b) Das Least Privilege-Prinzip: Systemkompromittierung und Infektion durch Malware werden deutlich erschwert, wenn auf den betroffenen Systemen nicht mit administrativen Berechtigungen gearbeitet wird.

---

[30] *So die EFS-Implementierung von Windows 2000, oder auch ein aktuelleres Beispiel: http://www.heise-online.co.uk/security/Enclosed-but-not-encrypted--/features/110136*

[31] *Gemeint ist der* FEK (= File Encryption Key).

[32] *Produkte, die dies leisten, sind z. B.* Sign-it *von S-TRUST*, File Security *von Kobil oder* digiSeal *von Secrypt. Jedes der genannten Produkte kann darüber hinaus ebenso mit fortgeschrittenen wie auch mit qualifizierten Zertifikaten umgehen.*

(c) Der Patchlevel stand der betroffenen Systeme: Systemkompromittierung und Infektion durch Malware, werden durch einen aktuellen Patchlevel deutlich erschwert.

6 SCHUTZMAßNAHMEN (MITIGATING CONTROLS)

Für Maßnahmen ergeben sich die folgenden grundlegenden Ansätze:

- **Policies**
- **Technische Lösung**
- **Benutzer-Training /-Sensibilisierung**

Am nachhaltigsten wirkt dabei eine sinnvolle Kombination dieser drei Ansätze.

Um jedoch etwas konkreter zu werden, lassen sich aus den vorausgehenden Untersuchungen zunächst folgende (noch nicht plattformspezifische) Schutzmaßnahmen[33] ableiten:

(1) **Implementieren Sie eine Policy, die den Umgang mit Wechselmedien regelt.** Diese (organisatorische) Policy sollte in allgemeinverständlicher Art und Weise beschreiben, wozu USB-Sticks im Unternehmen verwendet werden dürfen und wozu nicht. Die Policy könnte etwa die Verwendung von nur einem definierten Typus (zwecks einfacherem USB-Gerätemanagement) vorschreiben. Die Policy sollte den Fokus nicht nur auf den fremden und den eigenen USB-Stick legen, sondern Sie sollte sich auch explizit auf die Verwendung von Notebooks oder anderen mobilen Geräten zusammen mit Wechselmedien beziehen.

(2) **Sensibilisieren Sie Ihre Benutzer.** Auch wenn sich diese Schutzmaßnahme nicht unmittelbar aus den vorausgehenden Sicherheitsbetrachtungen ergibt, möchte ich sie hier an zweiter Stelle anführen. Wie Steve Riley und Jesper Johansson so treffend in einem Artikel zum Security Management über Sicherheitslegenden (in Bezug auf die Legende *Sicherheitskonfigurationen stoppen Würmer und Viren*) schreiben:

> *Bei der Wahl zwischen tanzenden Schweinchen und Sicherheit werden Benutzer jedes einzelne Mal tanzende Schweinchen wählen. Bei der Wahl zwischen Bildern von nackten Leuten, die fröhlich am Strand herumtollen, und Sicherheit, würde ungefähr die Hälfte der Bevölkerung die nackten Leute, die fröhlich am Strand herumtollen, wählen. Nehmen Sie dazu die Tatsache, dass die Benutzer unsere Sicherheitsdialogfenster nicht verstehen, und wir haben die Katastrophe. Wenn ein Dialogfenster, das den Benutzer um eine Sicherheitsentscheidung bittet, die einzige Barriere zwischen dem Benutzer und nackten Leuten, die fröhlich am Strand herumtollen, ist, hat die Sicherheit keine Chance*[34].

---

[33] *Es sei darauf hingewiesen, dass jede der hier angeführten Maßnahmen konform zu Forderungen von ISO 27002:2005 ist.*

[34] *Jesper M. Johansson und Steve Riley:* Sicherheits-Management – April 2005, http://www.microsoft.com/germany/technet/sicherheit/newsletter/legenden2.mspx

Die Sensibilisierung kann z. B. durch ein an alle Benutzer verteiltes Faltblatt mit den '10 Goldenen Sicherheitsregeln', durch kurze Schulungen oder durch regelmäßige Publikationen an prominenter Stelle im Intranet statt finden. Konstruktiven Möglichkeiten sind hier kaum Grenzen gesetzt.

(3) **Wenn Sie die Verwendung von eigenen USB-Sticks gestatten, verwenden Sie Kryptoverfahren zur Speicherung von Daten auf den USB-Sticks.** Die Möglichkeiten sind dabei vielfältig: Sie können das bei Benutzern weithin bekannte Winzip ab der Version 9.0 einsetzen. Diese Version unterstützt 128- und 256-Bit AES-Verschlüsselung. Achtung: Vorgängerversionen unterstützen keine sicheren Verschlüsselungsverfahren. Sie können PGP einsetzen oder Produkte von Aladdin, Kobil oder weiteren Herstellern verwenden. In der Windows-Welt können Sie Dateien und Verzeichnisse NTFS formatierter USB-Sticks mit EFS verschlüsseln, ab Windows Vista können Sie auch auf einfachere Weise als unter Windows XP Zertifikate für die Verschlüsselung benutzen. Wenn Sie planen, Verschlüsselung unternehmensweit einzusetzen und verschlüsselte Dateien beispielsweise per Mail zu verschicken, dann sollte eventuell der Einsatz von PKI, mindestens jedoch eines Schlüsselmanagements erwogen werden. Für die einfache Verschlüsselung von Daten auf einem USB-Stick ist Winzip oder eine ähnliche Lösung dagegen vollkommen ausreichend. Ferner empfiehlt es sich, die vorgeschriebenen Verfahren zur Verwendung von Krypto in die Policy einzubinden. Es sei denn, Sie verwenden eine unternehmensweite technische Lösung zum Devicemanagement wie etwa den *Pointsec Protector* oder *DriveLock* von CenterTools.

(4) **Verwenden Sie starke Passwörter.** Dies ist insbesondere dann wichtig, wenn Verschlüsselungsschlüssel (wie etwa bei EFS und PGP aber auch allen weiteren nicht-multifaktoriellen Authentifizierungsverfahren) von dem Passwort abgeleitet oder durch das Passwort geschützt werden.

Weitere Maßnahmen, die sich nicht direkt als dedizierte Maßnahmen aus der Risikobetrachtung ergeben, dafür jedoch als flankierende Massnahmen einen direkten Einfluss auf das Ausnutzen von Schwachstellen und die Systemkompromittierung besitzen sind:

(5) **Aktueller Patchlevel.** Viele Angriffsmethoden nutzen (nie auszuschliessende) Softwarefehler aus, um einen Dienst, eine Applikation oder das Betriebssystem und damit den Rechner zu kompromittieren. Ein hoher Patchlevelstand schließt den Großteil aktueller Bedrohungen und Kompromittierungsmöglichkeiten des Systems aus.

(6) **Least Privilege.** Alle Benutzer, Dienste und Applikationen sollen nur mit dem für ihre Funktion minimal notwendigen Maß an Berechtigungen ausgestattet sein und das auch nur in der Zeitspanne, in der dies erforderlich ist. Wenn Benutzer nicht mit administrativen Berechtigungen arbeiten, dann können Schadprogramme auch nicht einfach Passwort-Hashes von Benutzern auf den USB-Stick kopieren oder auf Zweige der Registry zugreifen, die administrative Privilegien erfordern.

(7) **Minimal Machine.** Das Prinzip des Minimalsystems gilt sowohl für Software als auch für Hardware: Auf einem System sollen nur die Teilkomponenten installiert

sein, die für die Anforderungen an dieses Systems notwendig sind. Alle weiteren Devices, Module, Dienste oder Applikationen machen das System anfälliger für Sicherheitslücken und sollen weder logisch noch physisch installiert oder – wenn sie in der Defaultinstallation vorhanden sind – wieder deinstalliert werden. Wenn USB-Anschlüsse nicht benötigt werden, dann sollen sie deaktiviert und die entsprechenden Treiber deinstalliert werden. Wenn nur eine bestimmte Klasse von USB-Geräten genutzt wird, dann soll auch nur genau diese Klasse zugelassen werden.

7 WECHSELMEDIEN UNTER WINDOWS UND SCHUTZMAßNAHMEN

Windows-Betriebssysteme unterscheiden Hardware-Geräte anhand ihrer Geräteklasse[35].

Windows[36] unterscheidet beim Einsatz von USB-konnektierten Speichermedien zwei Geräteklassen[37]:

- Sog. „Wechseldatenträger“ (typischerweise USB-Sticks)
- Sog. „Lokale Datenträger“ (typischerweise etwa USB-Festplatten oder CD-Laufwerke)

Bei Einlegen/Konnektierung eines Wechselmediums sind insbesondere die Möglichkeiten der automatischen Code-Ausführung (*Auto-Run*) relevant. Hier sind drei Varianten zu unterscheiden:

- Einfache Sticks („Wechseldatenträger“ im Sinne der obigen Unterscheidung). Hier ist zunächst keine automatische Infektion möglich (wohl aber eine bei fehlerhaftem Benutzerverhalten, s.u.)

- Sog. U3-Sticks, die neben dem eigentlichen USB-Speicher ein virtuelles CD-ROM Laufwerk mounten, für das wiederum per default AutoRun aktiviert ist.

- „Lokale Datenträger“ im Sinne der obigen Unterscheidung, für die per default AutoRun aktiviert ist.

Die **technischen Maßnahmen** lassen sich nicht immer komfortabel, aber unter Windows zufriedenstellend realisieren zum einen **durch Windows-Bordmittel**:

- Deaktivierung der AutoRun-Funktionalität durch Registry-Modifikation[38]. Dies ist eine effiziente und (per Reg-File) auch absehbar leicht ausrollbare Massnahme. Sie sollte daher priorisiert werden und würde mögliche Probleme grossflächig adressieren können.

- Deaktivierung von USB-Speichermedien durch Entfernung des notwendigen Treibers usbstor.inf und/oder Anpassung von dessen Berechtigungen[39] (für bestehende Systeme; diese Maßnahme ist mit gewissem Skript-Aufwand ausrollbar). Die Maßnahme hätte den Nebeneffekt, dass überhaupt keine Nutzung von USB-Sticks (und –Massenspeichergeräten) mehr möglich wäre.

---

[35] *Siehe http://msdn2.microsoft.com/en-us/library/ms791126.aspx. Dies gilt für Windows-Betriebssysteme ab Windows 95.*
[36] *Einbezogen sind Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008.*
[37] *Eine gute Übersicht bietet http://www.uwe-sieber.de/usbstick.html.*
[38] *AutoRun-Eintrag beim CD-Device sowie* NoDriveTypeAutorun *mit dem (Dezimal-) Wert 255 im Policies-Subkey unter* HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
[39] *Siehe dazu auch http://support.microsoft.com/kb/823732/en-us.*

- Komplette Deaktivierung von USB auf Geräte- (BIOS-) Ebene oder Betriebssystem-Ebene. Diese Massnahme hätte den Nebeneffekt, dass überhaupt keine Nutzung von USB-Geräten mehr möglich wäre.

Windows Vista bietet darüber hinaus die folgenden Möglichkeiten:

- Granulare Kontrolle nicht nur von USB-Geräten über Gruppenrichtlinien[40]. Dieses ist eine effektive, jedoch nicht immer einfach zu konfigurierende Funktionalität, da sie die Ermittlung von korrektem Hardware-IDs erfordert.[41]

- Das grundsätzliche Deaktivieren der Funktion *Automatische Wiedergabe für alle Medien und Geräte verwenden* in der Systemsteuerung, bzw. die Auswahl von *Keine Aktion durchführen* für alle Medien und Geräte[42].

Darüber hinaus gibt es **kommerzielle Lösungen von Drittherstellern**, von denen exemplarisch genannt seien:

- *DriveLock* von CenterTools, das eine Integration mit Active Directory sowie das Setzen von granularen Berechtigungen für Benutzer und Gruppen gestattet.[43]

- *Pointsec Protector* von Check Point, der mit ähnlichen Features aufwartet.[44]

- *Safeend Auditor* und *Safeend Protector*, die Active Directory-Integration, die Verwendung von Benutzern, Gruppen und Computern und mit dem *Safeend Auditor* ein Vulnerability-Assessment-Tool bieten.[45]

Weitere technische Massnahmen, wie etwa Verschlüsselung von USB-Sticks, wurden im vorausgehenden Abschnitt angeführt. Ebenso die organisatorischen Maßnahmen, von denen insbesondere eine Policy zum Umgang mit USB-Geräten und die Sensibilisierung von Mitarbeitern zu nennen sind.

---

[40] *Siehe dazu besonders: http://www.microsoft.com/technet/windowsvista/library/9fe5bf05-a4a9-44e2-a0c3-b4b4eaaa37f3.mspx, darüber hinaus auch: http://technet2.microsoft.com/windowsserver2008/en/library/a8a66e55-c3b3-47b6-b7d2-9805b13f73c81033.mspx?mfr=true*

[41] *Vgl. dazu http://msdn2.microsoft.com/en-us/library/ms791083.aspx, http://msdn2.microsoft.com/en-us/library/ms791079.aspx und http://msdn2.microsoft.com/en-us/library/ms801484.aspx.*

[42] *Wurde der bereits oben genannte Registryschlüssel (vgl. Anmerkung 38) auf den Wert 255 gesetzt, so kommt der in der Systemsteuerung vorgenommene Einstellung keine Bedeutung mehr zu.*

[43] *http://www.centertools.com/drivelock.aspx.*

[44] *http://www.checkpoint.de/products/datasecurity/protector/index.html.*

[45] *http://www.safend.com/11-en/Safend.aspx.*

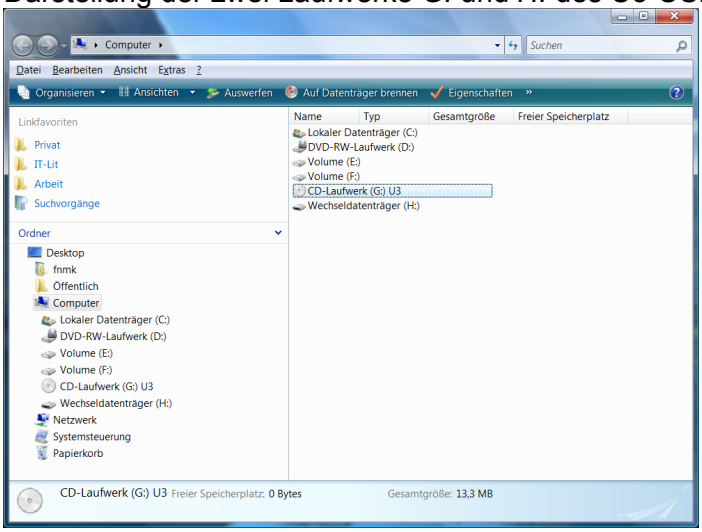
8 ANHANG: SCREENSHOTS ZUM VERHALTEN DES PRÄPARIERTEN U3-STICKS UNTER WINDOWS VISTA

Folgendes geschieht in Abhängigkeit von der Konfiguration der Malware *USB-Switchblade* auf dem USB-Stick[46]:

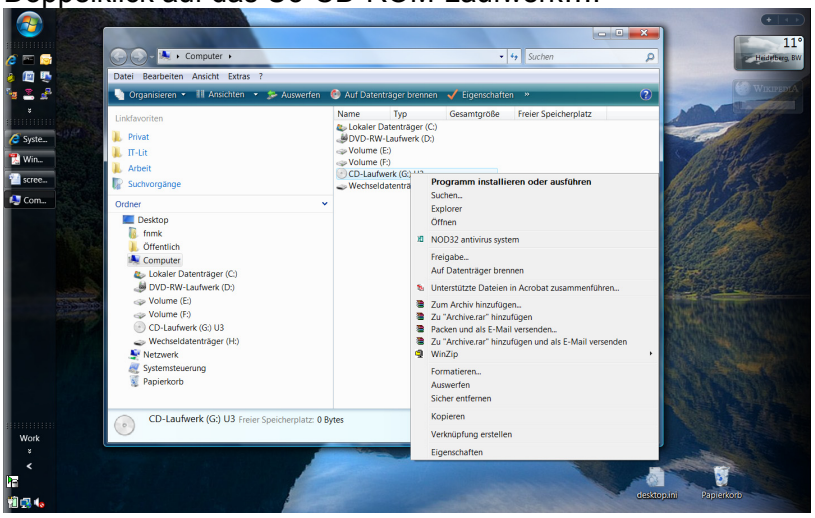
1. Einstecken des U3-USB-Sticks.

2. Automatisches Installieren der Gerätetreiber durch Windows Vista für den USB-Stick.

3. Darstellung der zwei Laufwerke *G:* und *H:* des U3-USB-Sticks im *Explorer*:



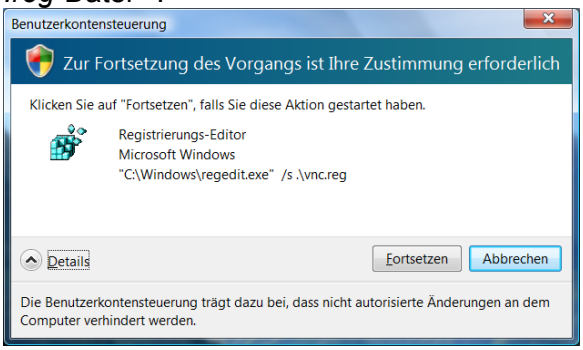
4. Ein Rechtsklick auf das U3-CD-ROM-Laufwerk offenbart die Default-Aktion bei Doppelklick auf das U3-CD-ROM-Laufwerk…:



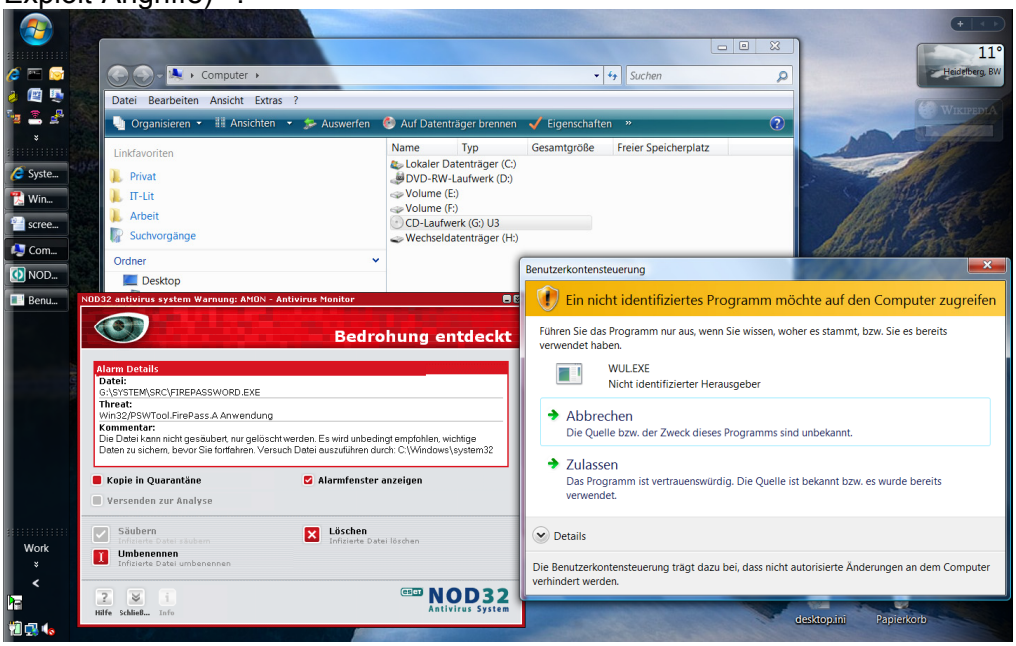
[46] *Eine detaillierter Beschreibung der in dieser Software verwendeten Techniken finden sich unter: http://wiki.hak5.org/wiki/USB_Switchblade.*

5. …die modifizierte *AUTORUN.INF* startet nicht den U3-Launcher *LAUNCHU3.EXE*, sondern das Skript *GO.VBS*. Dies führt zum Aufruf der von der AV-Lösung *NOD32* des getesteten Rechners korrekt erkannten Malware; es werden in der Reihenfolge der Screenshots aufgerufen[47]:

   Versuch der Installation eines VNC-Servers über den rückfragelosen Import einer *.reg*-Datei[48]:



   Firepassword.exe zum Auslesen der in Firefox gespeicherten versteckten Passwörter und *wul.exe* zum Auslesen des Patchlevelstands (für eventuelle spätere Exploit-Angriffe)[49]:



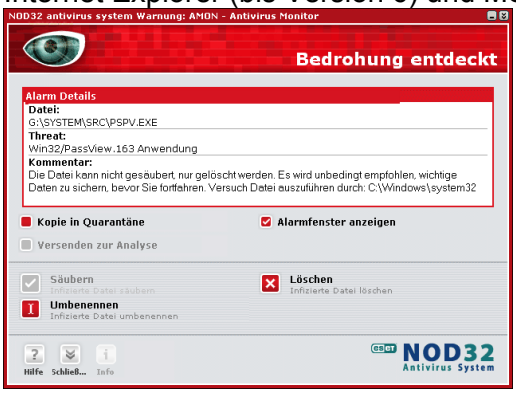
---

[47] *Achtung: Was an Warnmeldungen auf einem System angezeigt wird und wie diese präsentiert werden, hängt von der zusätzlichen Sicherheitssoftware ab, die auf dem betroffenen Rechner installiert ist. Der in Windows Vista enthaltene Windows Defender etwa schlägt nicht Alarm, ebenso einige (einzelne) AV-Produkte. Gängige Komplettpakete – sog. Internet Security-Suiten – geben (wenn auch unterschiedliche) Warnmeldungen aus.*

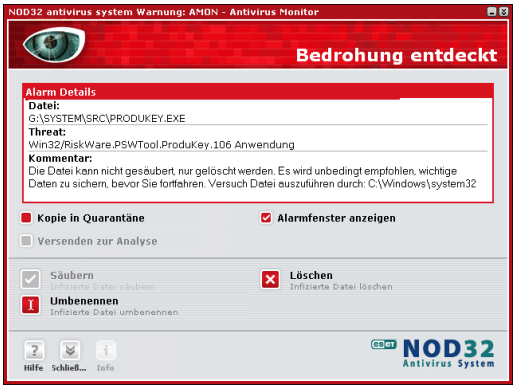
[48] *Wenn* USB-Switchblade *so konfiguriert wurde.*

[49] *Ebenso.*

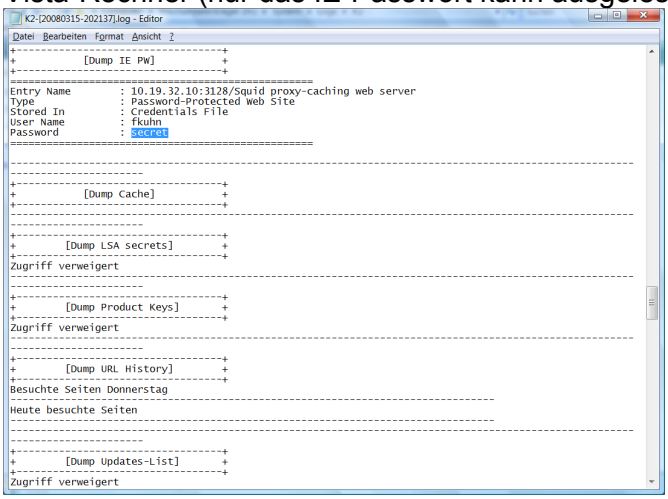
Pspv.exe zum Auslesen von Passwörtern, die gespeichert wurden, in: Outlook, Internet Explorer (bis Version 6) und MSN Explorer[50]:



Produkey.exe zum Auslesen von Produktschlüsseln von Microsoft Windows, Office und SQL-Server[51]:

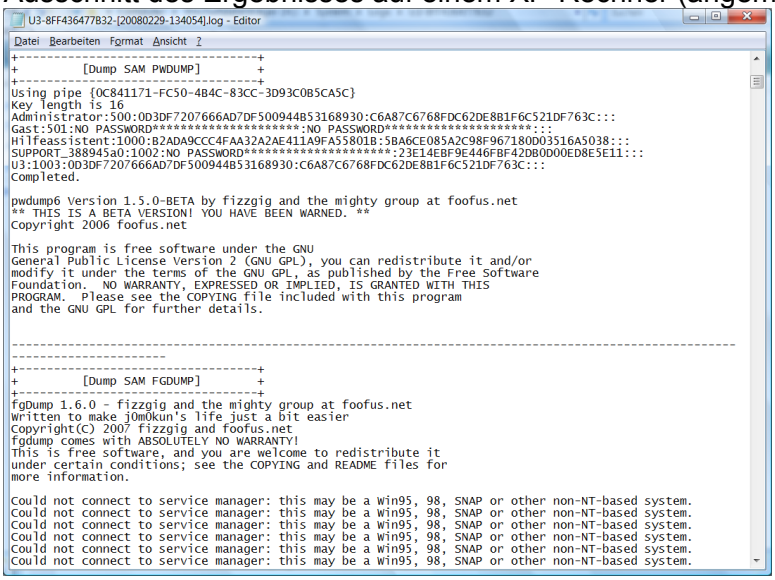


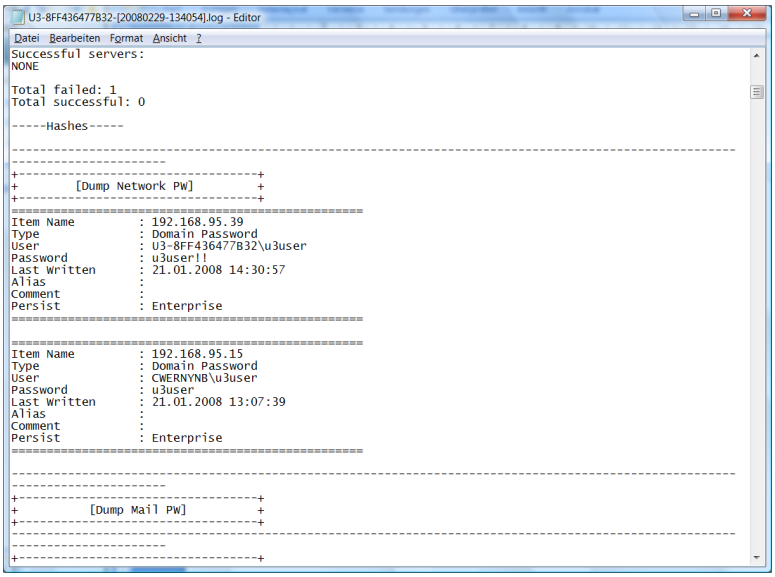
Ausschnitt des Ergebnisses des von der Malware geschriebenen Logs auf einem Vista-Rechner (nur das IE-Passwort kann ausgelesen werden[52]):



[50] *Ebenso.*
[51] *Ebenso.*
[52] *Passwörter können bis zu Outlook 2003 ausgelesen werden, für Outlook 2007 wird ein zusätzliches Tool benötigt.*

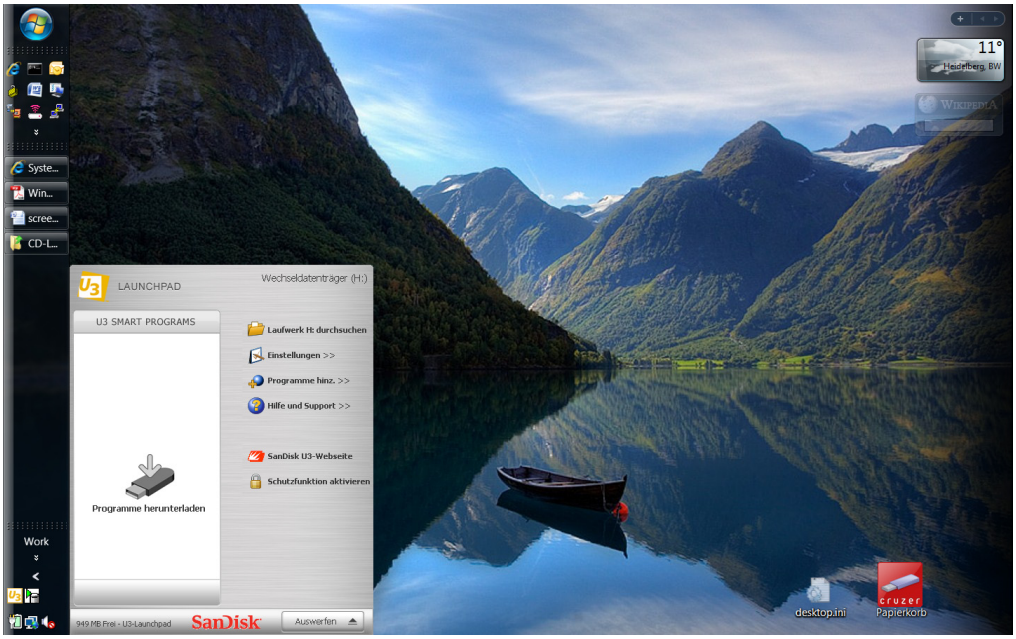
Ausschnitt des Ergebnisses auf einem XP-Rechner (angemeldet als Administrator)[53]:





[53] *Die Passwörter können dann mit einem der vielen verfügbaren Passwortknacker aus den Passwort-Hashes berechnet werden.*

6. Das Aufrufen des eigentlichen über *AUTORUN.INF* zu startenden U3-Launcher *LAUNCHU3.EXE* führt zur eigentlichen Darstellung des U3-Startmenüs:



Für weitere Fragen steht Ihnen das Team von **ERNW-Deutschland** und **ERNW-Portugal** gern zur Verfügung.

Mit freundlichen Grüßen,

Friedwart Kuhn.

ERNW GmbH
Friedwart Kuhn
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 15152411855
Mobil (Portugal): +351 91 8763637
www.ernw.de