

Automatisierte Installationen

Einführung

In grösseren Umgebungen werden Windows Workstations üblicherweise automatisch mit einem sogenannten Unattended-Setup installiert. Compass Security konnte im Rahmen von internen Penetration-Tests wiederholt feststellen, dass die dazu benutzten Installationsquellen ungenügend geschützt werden. Dies ermöglicht einem Hacker im Intranet umfangreichen Zugriff (Domain Administrator) innerhalb von kurzer Zeit zu erlangen. Mit diesem Artikel möchte Compass Security AG auf diesen Sachverhalt hinweisen und Empfehlungen zum Schutze Ihrer Netzwerke abgeben.

Ablauf

Eine klassische automatisierte Installation läuft folgendermassen ab:

1. Starten des PCs. Entweder von einer Bootdiskette oder per Netzwerk
2. Verbinden eines Netzlaufwerkes mit den Installationsdateien
3. Starten der eigentlichen Installation mit Antwortdateien für die Automation
4. Ablauf von zusätzlichen Skripten um weitere Software zu installieren und das System zu konfigurieren

Sicherheitsprobleme

Beim oben erwähnten Ablauf kommen nun einige Dateien zum Zuge, die Passwörter enthalten können, um:

- den Computer am Netzwerk anzumelden, damit das Netzlaufwerk mit den Installationsdateien verbunden werden kann
- lokale Administrator Passwörter festzulegen
- Computer automatisch einer Windows-Domäne hinzuzufügen
- weitere Software zu installieren oder Konfigurationen vorzunehmen

Die entsprechenden Dateien können innerhalb kurzer Zeit ausgemacht und die darin enthaltenen Passwörter missbraucht werden.

Schwachstellen

Netzwerk-Boot

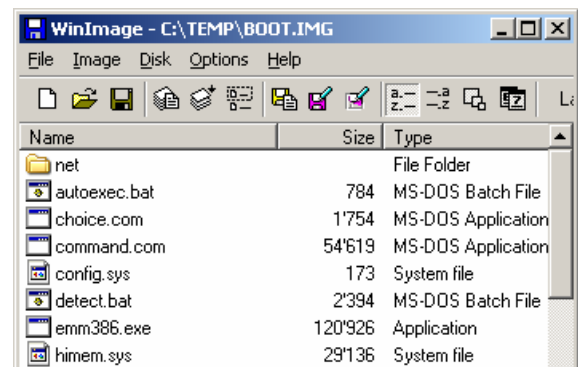
Beim Start der Installation werden Bootdisketten oder TFTP-Server mit Bootimages (Netzwerk-Boot) verwendet. Benutzeraccounts sowie Passwörter können auf beiden Medien gefunden werden. Wird per Netzwerk gebootet, werden via DHCP Optionen verteilt, die dem Client Ort und Namen des Bootimages mitteilen:

```

Bootstrap Protocol
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 10.1.1.50
Next server IP address: 10.1.1.240
Client hardware address: 00:06:5g:c9:7k:9x
Option 53: DHCP Message Type = DHCP Offer
Option 54: Server Identifier = 10.1.1.222
Option 15: Domain Name = "foo.com"
Option 3: Router = 10.1.1.1
Option 6: Domain Name Server IP: 10.1.1.10
Option 66: TFTP Server Name = dc.foo.com
Option 67: Bootfile name = "netboot.pxe"
End Option
  
```

Vom Netzwerk geschnittes DHCP-Paket

Ein Angreifer kann die angegebene PXE-Datei (pre-boot execution environment) ebenfalls herunterladen. Da in dieser Datei der Name des eigentlichen Bootimages enthalten ist, kann dieses auch via TFTP (keine Anmeldung nötig) angefordert werden. Mit Hilfe eines Image-Tools, können die Dateien aus dem Image entpackt werden.



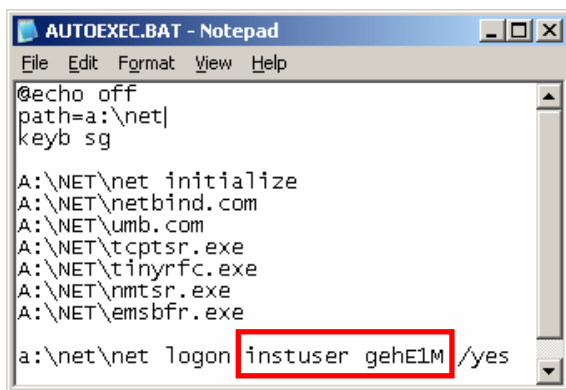
Ansicht des Bootimages mit dem Tool Winimage

Sicherheit bei automatisierten Windows Installationen

von Christoph Schnidrig
christoph.schnidrig@csnc.ch

Das Bootimage, das per Netzwerk geladen wird, enthält im wesentlichen die Bootdiskette für die automatische Installation. Darin können die Zugangsdaten der Installationsbenutzer enthalten sein.

Nach dem Systemstart per Bootimage resp. Bootdiskette wird die Installationsfreigabe verbunden und von dort die eigentliche Installation gestartet.



```

AUTOEXEC.BAT - Notepad
File Edit Format View Help
@echo off
path=a:\net|
keyb sg

A:\NET\net initialize
A:\NET\netbind.com
A:\NET\umb.com
A:\NET\tcptsr.exe
A:\NET\tinyrfc.exe
A:\NET\nmtsr.exe
A:\NET\emsbfr.exe

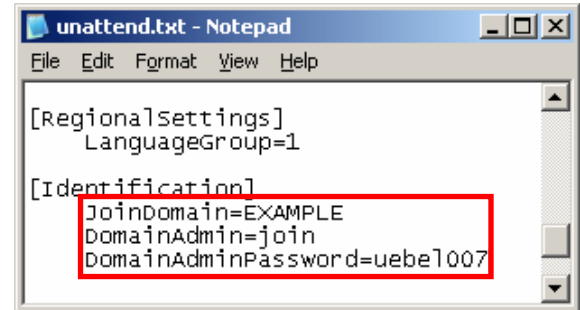
a:\net\net logon instuser gehE1M /yes
    
```

Autoexec.bat einer Bootdiskette/-image mit Benutzernamen und Passwort

Unattended-Dateien und Skripte

Dateien und Skripte auf Installationsfreigaben können weitere Passwörter enthalten. Beispiele dafür sind Passwörter für den lokalen Administrator oder für die erste automatische Anmeldung zu Konfigurationszwecken. Leider sind die entsprechenden Netzwerkfreigaben meist schlecht geschützt, d.h. für interne Benutzer (Domain Users) zugänglich. Die betreffenden Dateien sind jeweils unterhalb des Betriebssystemverzeichnis (i386) im \$OEM\$-Verzeichnis abgelegt. Dieses Verzeichnis wird bei der Installation automatisch auf den zu installierenden Computer übertragen, um die entsprechenden Skripte während resp. nach der Installation auszuführen. Passwörter könnten also einerseits in der Installationsfreigabe oder direkt auf dem installierten Computer gefunden werden.

Bei automatisierten Installationen besteht die Möglichkeit, den Computer in die Windows Domäne einzufügen.



```

unattend.txt - Notepad
File Edit Format View Help

[RegionalSettings]
    LanguageGroup=1

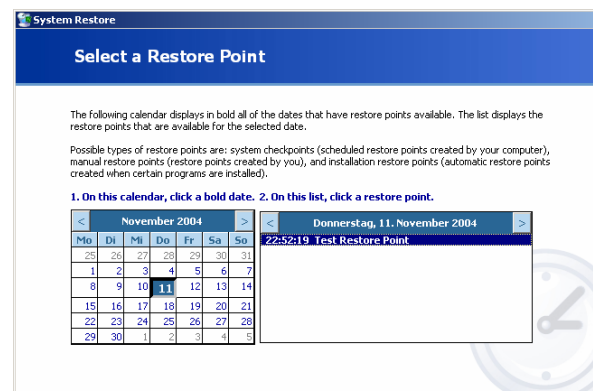
[Identification]
    JoinDomain=EXAMPLE
    DomainAdmin=join
    DomainAdminPassword=uebe1007
    
```

Zugangsdaten in der Unattended-Datei

Dazu ist jedoch ein erweitertes Benutzerprivileg nötig. Vielerorts wird für diesen Schritt ein Domänen Administrator (wie oben in der Unattended-Datei suggeriert) benutzt. Ist dies der Fall, fallen einem neugierigen Leser der Installationskripte direkt die höchstmöglichen Rechte einer Windows Domäne in die Hände.

System Restore bei Windows XP

Wie zuvor erwähnt, werden bei der Installation unter Umständen Dateien mit Passwörtern auf den zu installierenden Computer kopiert. Auch wenn diese nach Verwendung sachgemäss gelöscht werden, könnten die entsprechenden Dateien noch auf dem System verbleiben. Eine neue Funktionalität überwacht bei Windows XP Betriebssystemdateien und erstellt bei Bedarf sogenannte Restore Points.



Systemwiederherstellung mit System Restore

Sicherheit bei automatisierten Windows Installationen

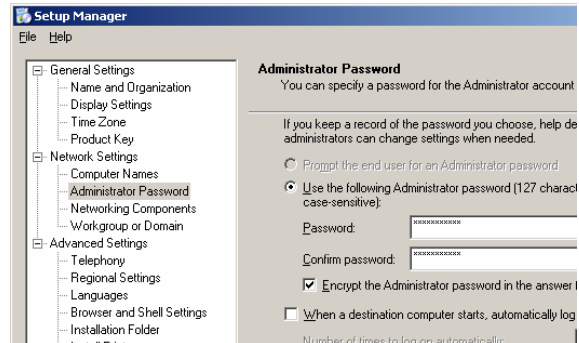
von Christoph Schnidrig
christoph.schnidrig@csnc.ch

Damit ist es möglich z.B. nach einer fehlgeschlagenen Patch-Installation den Computer wiederherzustellen. Die Restore Points befinden sich im „System Volume Information“ Verzeichnis auf dem System Laufwerk. Standardmässig hat nur das System Zugriff auf diesen Ordner. Lokale Administratoren können sich aber einfach selbst entsprechende Rechte zuordnen. Mittels einer Boot-CD mit integriertem NTFS-Treiber kann auch ohne erweiterte Berechtigungen auf die Restore Points zugegriffen und Einsicht in die sensitiven Dateien erlangt werden.

Gegenmassnahmen

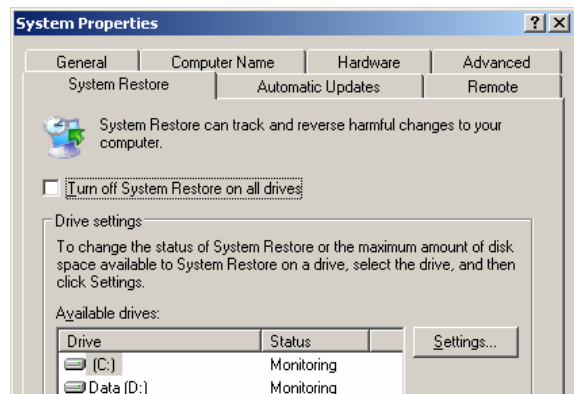
Um die erwähnten Schwachstellen zu beseitigen und die Installationsquellen abzusichern, empfiehlt Compass Security folgende Gegenmassnahmen:

- Verwenden Sie einen niedrig privilegierten Benutzer für die Installation (Bootdiskette).
- Passen Sie die Berechtigungen der Installationsfreigabe so an, dass nur der Installationsbenutzer und ev. Administratoren Zugriff erhalten.
- Speichern Sie keine Zugangsdaten auf Startdisketten oder Bootimages ab. Allenfalls können die Passwörter mit Installationssoftware von Drittherstellern verschlüsselt werden.
- Für die Zuordnung in die Domäne sollten Sie einen normalen Benutzer mit dem zusätzlichen Privileg „Add Computers to the Domain“ erstellen. Dies wird in der Group Policy der Domäne unter „Computer Configuration-Windows Settings-Security Settings-Security Options“ bewerkstelligt.
- Verschlüsseln Sie wenn möglich die Passwörter in den Installationskripts. Microsoft bietet die Möglichkeit das Passwort des lokalen Administrators zu verschlüsseln, nicht aber vom Benutzer für den „Domain-Join“. Installationssoftware von Drittherstellern bieten hier zum Teil erweiterte Möglichkeiten an.



Verschlüsseln vom Passwortes des lokalen Admins mit dem Setup Manager von Microsoft

- Löschen Sie alle System Restore Points nach dem Abschluss der Installation. Dies wird erreicht indem, die Funktionalität aus- und eingeschaltet wird.



System Restore Einstellungen werden in den System Eigenschaften vorgenommen

Dies kann auch per Skript erreicht werden. Siehe Referenzen.

- Stellen Sie sicher, das die auf dem Computer benutzten Skripte nach Gebrauch gelöscht werden. Der sicherste Weg ist es danach den gesamten leeren Diskbereich zu überschreiben, weil die gelöschten Dateien theoretisch wiederhergestellt werden könnten. Dazu kann das Tool cipher (in Win2000 und XP enthalten) benutzt werden:

```
cipher /w:c:\ überschreibt den gesamten „leeren“ Festplattenplatz auf c: .
```



Sicherheit bei automatisierten Windows Installationen

von Christoph Schnidrig
christoph.schnidrig@csnc.ch

Referenzen

Tools

- Winimage
<http://www.winimage.com>
- Setup Manager von Microsoft
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3E90DC91-AC56-4665-949B-BEDA3080E0F6>
- Open Source Unattended Installation
<http://unattended.sourceforge.net>

Dokumentation

- Webseite mit Beschreibungen zu automatisierten Installationen
<http://unattended.msfn.org>
- Knowledge Base Artikel zum Thema Verschlüsselung
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q299969>
- Frequently Asked Questions Regarding System Restore in Windows XP
<http://www.microsoft.com/technet/community/newsgroups/faqsrxwp.mspx>

Anleitung (SR per Skript abschalten)

Um die System Restore Funktionalität per Skript abzuschalten müssen folgende Änderungen in der Registry vorgenommen werden:

Erstellen Sie einen DWORD-Wert mit dem Namen „DisableSR“ und dem Wert 1 unter HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore.

Danach muss der entsprechende Systemdienst noch abgeschaltet resp. gestoppt werden. Dies erreicht man indem der Wert „Start“ im Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sr auf 4 (Abgeschaltet) gesetzt wird und der Dienst gestoppt wird (`net stop "System Restore Service"`).

Über den Autor

Nach der Informatik TS arbeitete Christoph Schnidrig 3 Jahre als System Engineer bei Comline AG. Anfangs 2001 wechselte er zu Compass Security und nahm die Tätigkeit als Security Analyst auf. Ende 2001 schloss er ein Nachdiplomstudium in Wirtschaft ab.

Compass Security AG

Wir sind ein Schweizer Unternehmen aus Rapperswil SG und führen professionelle IT Sicherheitsüberprüfungen durch. Mit Whitehat oder Blackhat Approach untersuchen wir IT-Infrastrukturen und Webapplikationen der Kunden. Sei es im Rahmen eines Produkte Sign-off, oder in regelmässigen Abständen - Compass ist Ihr Partner für die Identifikation von Schwachstellen und Sicherheitslücken. Nationale und internationale Unternehmen im In- und Ausland vertrauen auf unsere Kompetenz, wenn es um die Beurteilung von IT-Risiken geht.

Wir verbessern die eingesetzten Assessment Methoden ständig. Schwerpunkt wird auch auf die Schulung gelegt. Aus diesem Grund bieten wir regelmässig Kurse an. Dieses Jahr haben wie den Evidence Lab Kurs in das Programm aufgenommen. Dabei wird auf die praktische Spurensuche in Computer Systemen eingegangen.

Weiteres siehe: <http://www.csnc.ch>

16. November 2004, V1.0