

Whitepaper

Produkt: cRM, AM

Sicherheitswarnung beim Öffnen einer Exe-Datei ausschalten

Inhalt

Hintergrund		3
W	/arnhinweis	3
	Unsignierte Exe-Datei	3
	Signierte Exe-Datei	3
Lē	ösung	4
	Hinweis für Administratoren	6

Hintergrund

Seit Windows XP SP2 hat Microsoft in Windows und allen folgenden Windows-Versionen ein neues Sicherheitsfeature implementiert, das bei Dateien, die aus dem Internet kommen oder über das Netzwerk gestartet werden, eine Sicherheitswarnung mit Bestätigungsdialog anzeigt. Dieses Feature heißt "Ausführungsdienst der Anlagenverwaltung" ("Attachment Execution Service" - AES), da es eigentlich dazu gedacht ist, heruntergeladene Dateien als solche zu kennzeichnen und ihre Ausführung zu steuern. Ob eine Datei heruntergeladen wurde, wird in einem zusätzlichen Datenstrom einer Datei – ein Feature des NTFS-Dateisystems – gespeichert.

Die Meldung unterscheidet sich geringfügig je nachdem, ob die Datei signiert ist oder nicht.

Warnhinweis

Unsignierte Exe-Datei

Wird eine unsignierte Exe-Datei gestartet, ist der Herausgeber unbekannt bzw. kann nicht verifiziert werden wird ein rotes Warnschild eingeblendet.

Datei öffnen - Sicherheitswarnung						
Der Herausgeber konnte nicht verifiziert werden. Möchten Sie diese Software ausführen?						
	Name:	Z:\AMLOGIN.EXE				
	Herausgeber:	Unbekannter Herausgeber				
	Typ:	Anwendung				
	Von:	Z:\AMLOGIN.EXE				
		Ausführen Abbrechen				
Diese Datei verfügt über keine gültige digitale Signatur, die den Herausgeber verifiziert. Sie sollten nur Software ausführen, die von Herausgebern stammt, denen Sie vertrauen. <u>Welche Software kann</u> ausgeführt werden?						

Signierte Exe-Datei

Bei einer signierten Exe-Datei kann der Herausgeber überprüft werden. Das Warnschild ist gelb.

Datei öffnen - Sicherheitswarnung						
Möchten Sie diese Datei ausführen?						
	Name: Z:\ Herausgeber: <u>co</u> Typ: Ar Von: Z:\	,cRM.exe <u>mbit Software GmbH</u> wendung ,cRM.exe				
		Ausführen Abbrechen				
٢	Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Führen Sie nur Software von Herausgebern aus, denen Sie vertrauen. <u>Welches</u> <u>Risiko besteht?</u>					

Lösung

Indem man das Netzlaufwerk dem lokalen Intranet oder den vertrauenswürdigen Sites hinzufügt, wird das AES Sicherheitsfeature für dieses Laufwerk umgangen. Da die Zone "Vertrauenswürdige Sites" sich mehr auf das Internet bezieht, ist es ratsam das Netzlaufwerk der Zone "Lokales Intranet" hinzuzufügen. Dies kann über den Internet Explorer geschehen. Auf der Registerkarte Sicherheit unter Extras > Internetoptionen sollte die Zone "Lokales Intranet" ausgewählt werden und anschließend die Schaltfläche "Sites" gedrückt werden.

Internetoptionen				? <mark>×</mark>
Verbindunger Allgemein	Sicherheit	Programme	enschutz	Erweitert Inhalte
Wählen Sie eine Zo	ne aus, um dere	en Sicherheits	einstellungen	festzulegen.
Lokales II	itranet ve	Sites	lige Einge	schrankte Sites
•				4
Diese Zone ist für alle Websites, die im Intranet Sites Version der Firma ermittelt wurden. Sicherheitsstufe dieser Zone Für diese Zone zugelassene Stufen: Alle Niedrig - - - Angemessen für Websites im lokalen Netzwerk (Intranet) - - Die meisten Inhalte werden ohne Eingabeaufforderung - - Kein Download nicht signierter ActiveX-Steuerelemente - - Entspricht mittlerer Stufe, mit Ausnahme der Eingabeaufforderung -				
Geschütztern	ouus akuvierei	Stufe annass	en St	andardstufe
Alle Zonen auf Standardstufe zurücksetzen				
OK Abbrechen Übernehmen				

Im folgenden Dialog muss die Option "Intranetnetzwerk automatisch ermitteln" deaktiviert werden.

Lokales Intranet	x		
Verwenden Sie die Einstellung, um festzulegen, welche Websites zur lokalen Intranetzone gehören.			
Intranetnetzwerk automatisch ermitteln			
Alle lokalen Sites (Intranet), die nicht in anderen Zonen aufgeführt sind, einbeziehen			
Alle Sites, die den Proxyserver umgehen, einbeziehen			
Alle Netzwerkpfade (UNCs) einbeziehen			
Was sind Intraneteinstellungen? Erweitert OK Abbrechen			

Danach muss die Schaltfläche "Erweitert" betätigt werden. Im folgenden Dialog kann dann die IP-Adresse des Servers des Netzlaufwerks oder der UNC-Pfad (\\Servername\Freigabename) eingegeben werden. Das Häkchen bei "Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich" sollte ebenfalls deaktiviert werden.

Lokales Intranet	-X		
Sie können Websites zu dieser Zone hinzufügen und aus ihr entfernen. Für alle Websites in dieser Zone werden die Sicherheitseinstellungen der Zone verwendet.			
Diese Website zur Zone hinzufügen:			
	Hinzufügen		
Websites:			
192.168.10.40	Entfernen		
Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich			
	Schließen		

Hinweis für Administratoren

Dieselbe Einstellung kann auch über die folgende Gruppenrichtlinie aktiviert werden.

Administrative Vorlagen – Windows-Komponenten – Internet Explorer – Internetsystemsteuerung – Sicherheitsseite – Liste der Site zu Zonenzuweisungen (engl. Computer Configuration - Administrative Templates - Windows Components - Internet Explorer -Internet Control Panel - Security Page - Site to Zone Assignment List)

Beim Doppelklick öffnet sich ein weiterer Dialog über den diese Richtlinie aktiviert werden kann. Über die Schaltfläche "Anzeigen" lassen sich die Zonenzuweisungen eintragen. Als Wertname kann z.B. die IP eingetragen werden und als Wert die 1 für Intranetzone.

Hinweis: combit macht keine Angaben zu einer bestimmten Eignung obiger Informationen. Irrtümer und Fehler bleiben ausdrücklich vorbehalten, die Angaben erfolgen ohne Gewähr und enthalten keine Zusicherung. Die Informationen können z.T. auch ein Versuch sein, Ihnen bei einer Aufgabenstellung zu helfen, selbst wenn das Produkt eigentlich nicht für diesen speziellen Zweck vorgesehen wurde.