

Zusammenfassung

Der Zugriff auf EDV-Ressourcen muss aus den zwei nachfolgend aufgeführten Gründen namentlich und identifizierbar erfolgen:

- Vermeidung des Zugriffs auf die EDV-Ressourcen durch unbefugte Personen,
- Identifikation möglicher bösartiger oder ungewollter Aktionen.

In diesem Dokument werden die Zugangskontrollen per Berechtigungsprüfung zu EDV-Systemen beschrieben.

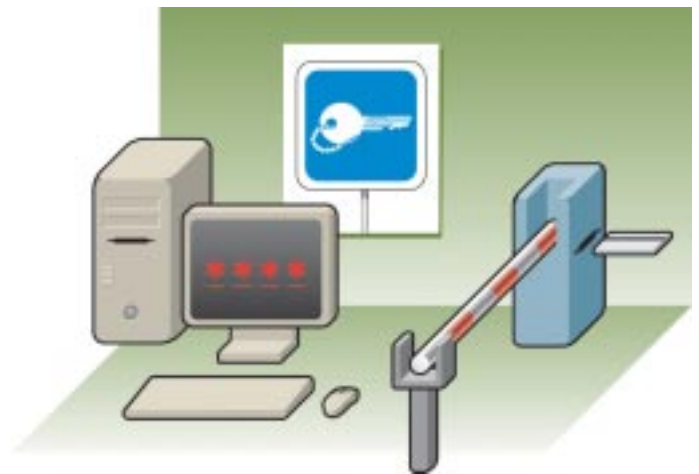
Die Berechtigungsprüfung oder Authentifizierung ist ein Zugangskontrollmechanismus, der auf dem Schlüssel-/Schloss-Prinzip beruht. Die klassische Lösung basiert auf folgendem Elementenpaar: Kennung und Passwort.

Die verschiedenen, dieser Lösung inne wohnenden Schwächen sind: wenig resistente oder fehlende Passwörter; Vorhandensein standardmäßig installierter Benutzerkonten; Passwörter, die ihren geheimen Charakter verloren haben; Software, die Benutzerkonten zur internen Verwendung erstellt; unzuverlässige Passwort-Verschlüsselungscodes; Speicherung der Passwörter auf Workstations ohne Überwachung oder Blockierung bei fehlerhaften Zugriffsversuchen. Die Bedrohungen hinsichtlich der Aufhebung der Verschlüsselung sind das brutale "Cracken", Wörterbuchattacken sowie Web-Bugs. Dieses Dokument beschreibt, wie man sich gegen die aufgeführten Sicherheitslücken und Bedrohungen schützen kann.

Achtung: Der physikalische Zugang zu Rechenzentren und der Zugang zu PCs wird von diesem Dokument nicht abgedeckt.

Inhalt

- 1 Zugriffsberechtigungsprüfung, was ist das? →
- 2 Welche inne wohnenden Sicherheitslücken gibt es? →
- 3 Welche Bedrohungen bestehen hinsichtlich der Dechiffrierung? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Maßnahmen →



1 Zugriffsberechtigungsprüfung, was ist das?

Die Berechtigungsprüfung oder Authentifizierung ist ein Zugangskontrollmechanismus, der auf dem Schlüssel-/Schloss-Prinzip beruht. Dieser Schlüssel ermöglicht die Herstellung einer Verbindung zwischen der Zugriffsanforderung zur Infrastruktur und einer physikalischen Person oder einer anderen Komponente des EDV-Systems. Im Idealfall wird diese Kennung mit einem Passwort oder einem anderen Element kombiniert, von dem

angenommen wird, dass es sich nur im Besitz der Person befindet, die über einen Zugang verfügen darf.

Die Berechtigungsprüfung stellt daher für sich genommen keine Sicherheitslücke dar. Die falsche Verwendung der Berechtigungsprüfungsverfahren ist jedoch eine der von den Piraten/Crackern am häufigsten genutzte Sicherheitslücke.

2 Welche inne wohnenden Sicherheitslücken gibt es?

Die Grundsätze der Berechtigungsprüfung sind auf die "Benutzer"- und "Administrator"-Zugriffsebene, auf Server und auf Softwareprogramme anwendbar. Bei der Betrachtung der Sicherheitslücken darf auch nicht der Zugriff auf die physikalischen Elemente des EDV-Systems wie beispielsweise die Router, die Switches etc. vergessen werden...

Diese gängige Authentifizierungslösung basiert auf einer Kombination aus einer vom Administrator bereit gestellten Kennung und einem vom Endbenutzer selbst festgelegten Passwort.

Diese Lösung unterliegt diversen ihr inne wohnenden Sicherheitslücken:

Die klassische Lösung = Kennung und Passwort

2.1 Vorhandensein von Benutzerkonten mit wenig resistenten oder fehlenden Benutzerkonten

Für die Einrichtung eines Passwortes gibt es einige Qualitätskriterien, die beachtet werden sollten, um zu vermeiden, dass spezielle Softwareprogramme das Passwort innerhalb kürzester Zeit cracken können. Cracken ist ein englischer Begriff, der knacken oder dechiffrieren des Passworts bedeutet. Diese Kriterien sind in Kapitel 5 des vorliegenden Dokuments beschrieben.

2.2 Einrichtung von standardmäßigen Benutzerkonten bei der Installation der Software

Bei der Installation von Softwareprogrammen wie etwa einem Betriebssystem werden Standard-Benutzerkonten eingerichtet. Diese Konten verwenden ein Passwort, das allen Piraten/Crackern bekannt ist. Es liegt auf der Hand, dass diese Konten die ersten Ziele von übel gesinnten Personen sind. Es ist daher erforderlich, dieses Benutzerkonto durch ein zuverlässiges Passwort zu schützen.

2.3 Passwörter, die ihren geheimen Charakter verloren haben

Ein Passwort ist das Mittel zur Identifikation des Benutzers eines Kontos. Es folgt der gleichen Logik wie die Eingabe einer PIN-Nummer an automatischen Bankschaltern. Leider kommt es jedoch viel zu häufig vor, dass Passwörter am Bildschirm angezeigt werden oder mehreren Personen bekannt sind.

2.4 Software, die Benutzerkonten zur internen Verwendung erstellt

Bestimmte Softwareprogramme wie etwa Datenbanken oder andere erstellen Benutzerkonten, die intern verwendet werden, um mit den anderen Komponenten des EDV-Systems zu kommunizieren. Diese Kennungen und ihre Passwörter, die häufig wenig resistent oder sogar gar nicht vorhanden sind, sind dokumentiert und folglich allen Piraten/Crackern bekannt.

2.5 Chiffrierungscodes unzuverlässiger Passwörter

Die Übertragung oder Speicherung von Passwörtern erfolgt in den meisten EDV-Systemen auf verschlüsselte Art und Weise. Es ist jedoch ratsam, sich zu vergewissern, dass die standardmäßige Parametrierung kein schwaches und leicht zu dechiffrierendes Verschlüsselungsverfahren nutzt. Es ist mit Sicherheit davon auszugehen, dass weniger leistungsfähige Verschlüsselungsverfahren in der Welt der Piraten/Cracker bekannt sind.

2.6 Speicherung von Passwörtern in den Workstations

Zahlreiche Softwareprogramme verwenden Passwörter, welche die Möglichkeit bieten, sie so zu speichern, dass diese beim nächsten Mal nicht mehr eingegeben werden müssen. Selbstverständlich wird trotz des praktischen Aspekts von diesem Verfahren abgeraten, da es fast so ist, als hätte man gar kein Passwort eingerichtet.

2.7 Fehlende Überwachung oder Blockierung bei fehlerhaften Zugriffsversuchen

Die wiederholte fehlerhafte Eingabe von Passwörtern für ein und dasselbe Benutzerkonto ist ein deutliches Warnsignal für den Administrator.

Obwohl die Mehrheit der EDV-Systeme eine Sperrung eines Benutzerkontos nach einer gewissen Anzahl von fehlerhaften Passwordeingaben unterstützt, kommt es nicht selten vor, dass diese Möglichkeit nicht genutzt wird, was folglich den in diesem Dokument beschriebenen Cracker-Softwareprogrammen Tür und Tor öffnet.

3

Welche Bedrohungen bestehen hinsichtlich der Dechiffrierung?

Bei der Untersuchung der vom SANS (System Administration, Audit, Network, Security institute - www.sans.org) veröffentlichten "Top20"-Sicherheitslücken stellt man fest, dass die Verwundbarkeit der Berechtigungsprüfungsverfahren seit mehr als einem Jahr zu den "Top10" der am häufigsten genutzten Sicherheitslücken gehört.

Für derartige Attacken verwenden die Piraten/Cracker/Hacker spezielle Decodierungsprogramme, die auf zwei verschiedenen Technologien beruhen:

3.1 Das brutale

Dieser Softwaretyp probiert alle Kombinationen aus. Die Kombinationen enthalten sowohl Hybrid- als auch alphanumerische Zeichen. Diese Lösung ist äußerst effizient, erfordert jedoch viel Zeit zum Cracken von komplexen Zeichenketten.

Einige dieser Tools wurden für spezielle Softwareprogramme wie etwa Microsoft Word oder andere entwickelt.

3.2 Wörterbuchattacken

Ce logiciel va essayer tous les termes stockés dans un dictionnaire qui reprend les mots de passe habituellement utilisés. Cette méthode un peu plus rapide ne permet pas de donner les mêmes résultats que la méthode brutale.

Dieses etwas schnellere Verfahren liefert jedoch nicht dieselben Ergebnisse wie die brutale Methode.

3.3 Die «Web-Bugs»

Ein anderes, leider weit verbreitetes Verfahren, ist die Ausnutzung bestimmter "Web-Bugs". Das Ziel dieser Methode besteht darin, die gesamte Verschlüsselung der Tastatureingabe abzuhören und sie an eine bestimmte Adresse zu übertragen. Das Dokument bezüglich der "Bugs" enthält ausführlichere Informationen über die Gegenmaßnahmen.

4

Warum sollte man sich schützen?

Die Auswirkungen der Ausnutzung der in Abschnitt 2 beschriebenen Sicherheitslücken lassen sich leicht ausmalen, da durch diese Ausnutzung ein EDV-System einschließlich der Softwareprogramme und aller darin enthaltenen Daten öffentlich gemacht werden.

(siehe auch "Auswirkungen der Angriff auf ein EDV-System").

Im schlimmsten Fall kann ein derartiger Angriff zum vollständigen Verlust der Kontrolle über das EDV-System führen, bei dem keine andere Möglichkeit bleibt, als das System von Grund auf neu aufzubauen.

5

Vorbeugende Maßnahmen

Die nachfolgend aufgeführten Ratschläge gelten für die Nutzung der Berechtigungsprüfung per Benutzerkonto/Passwort. Diese Regeln sind von Ihnen in der Verwaltungssoftware so anzuwenden, dass sie automatisch auf alle erstellten Benutzerkonten angewandt werden.

5.1 Nutzen Sie schwer zu hackende Passwörter

Wenn die Passwörter der folgenden Beschreibung entsprechen, können Sie davon ausgehen, dass die Cracker-Programm dermaßen viel Zeit erfordern, dass mögliche Piraten/Cracker den Mut verlieren:

- ➔ **Passwörter dürfen keinen Teil des Benutzernamens enthalten.**
- ➔ **Passwörter sollten mindestens 6 bis 8 Zeichen lang sein.**
- ➔ **Passwörter sollten mindestens drei Zeichen der folgenden Zeichengruppen enthalten:**
 - > **klein geschriebene alphabetische Zeichen**
 - > **groß geschriebene alphabetische Zeichen,**
 - > **Ziffern (0 bis 9),**
 - > **nicht alphanumerische Zeichen (!, *, # etc.).**

5.2 Protokollieren Sie die Passwörter

- ➔ **Protokollieren Sie die verwendeten Passwörter. Auf diese Weise ist es für die Benutzer nicht möglich, immer dieselben zwei oder drei Passwörter zu verwenden.**
- ➔ **Weisen Sie dem Passwort eine maximale Gültigkeitsdauer zu. Auf diese Weise wird gewährleistet, dass der Benutzer nach Ablauf der Gültigkeitsdauer sein Passwort ändert.**
- ➔ **Weisen Sie dem Passwort eine minimale Gültigkeitsdauer zu. Dies mag erstaunlich klingen, aber wenn Sie diese minimale Dauer nicht beachten, ist die Protokollierung der Passwörter nutzlos, da ein Benutzer nur zehn Mal innerhalb einer Minute sein Passwort ändern muss, um wieder sein ursprüngliches Passwort nutzen zu können.**

5.3 Tricks und Kniffe

Um zu vermeiden, dass die Abwesenheit eines Systemadministrators zur vollständigen Sperrung eines EDV-Systems führen kann, ist es manchmal erforderlich, einer Person einen Notzugang zu verleihen. Es sollte jedoch vermieden werden, dass diese Person diesen Zugang grundlos nutzen kann. Zu diesem Zweck ist es möglich, das Passwort in einem versiegelten Umschlag in einem Tresor aufzubewahren oder ein Passwort einzurichten, das sich aus zwei verschiedenen Teilen zusammensetzt, wobei einer Person nur jeweils ein Teil dieses Passworts bekannt ist.

Um ein komplexes, jedoch leicht zu merkendes Passwort einzurichten, können Sie das Anfangsbuchstaben-Verfahren nutzen. Beispiel: "Ich bin am 13. Juli '61 in Luxemburg geboren" > "Iba13J61iLg".

5.4 Kontrollieren Sie die EDV-Architektur

Es ist äußerst wichtig, in regelmäßigen Abständen die Protokolle zu überprüfen, um mögliche Zugriffsversuche durch unbefugte Personen zu erkennen.

Es ist genauso wichtig, die Liste der Benutzer einschließlich ihrer Profile und ihrer Rechte innerhalb des EDV-Systems immer auf dem aktuellen Stand zu halten.

5.5 Begrenzen Sie die Anzahl der

Die Benutzerkonten des Typs "Administrator", die mit zahlreichen Rechten versehen sind, sind das bevorzugte Ziel von Piraten und Crackern. Es wird geraten, dieses Konto nicht für eine gesamte EDV-Abteilung oder Gruppe einzurichten, sondern entsprechende, den jeweiligen Anforderungen jedes Teammitglieds entsprechende Profile zu erstellen.

Im Betriebssystem Microsoft Windows ist es eventuell sogar erforderlich, alle Rechte des "Administrator"-Benutzerkontos einzuschränken und ihm ein sehr komplexes Passwort zuzuweisen. Anschließend reicht es aus, die Aufgaben auf andere, weniger sichtbare Benutzerkonten aufzuteilen. Auf diese Weise verschwenden Piraten/Cracker ihre Zeit auf einen Köder, der ihnen rein gar nichts ermöglicht. Dies ist jedoch unter Unix mit dem Benutzerkonto Root leider nicht möglich.

5.6 Verwenden Sie Softwareprogramme zur Überprüfung der Zuverlässigkeit von Passwörtern

Es sind verschiedenste Softwareprogramme zur Überprüfung der Zuverlässigkeit von Passwörtern erhältlich. Da diese Softwareprogramme jedoch leider sehr kostspielig sind, könnte es für Sie günstiger sein, externe Unternehmen mit der Durchführung dieser Art von Überprüfung zu beauftragen.

Achtung : Vor der Durchführung jeglicher Art von Überprüfung der Zuverlässigkeit von Passwörtern müssen Sie die für die Verwaltung des Zugangs verantwortliche Person informieren und die möglichen Auswirkungen analysieren. Die Verwendung dieser Art von Softwareprogrammen kann nämlich bis hin zur Sperrung jeglicher Benutzerkonten führen.

5.7 Alternativlösungen

Seit einiger Zeit sind neue Berechtigungsprüfungslösungen wie etwa die PKI (Public Key Infrastructure), die Biometrie und Chipkarten auf dem Markt. Diese Lösungen werden in separaten Dokumenten beschrieben.

Der Vorteil dieser Lösungen besteht in der Beseitigung des Problems der Enthüllung von Passwörtern oder der Übertragung kritischer Daten über das Netzwerk. Leider sind diese Lösungen noch sehr kostspielig und nur schwer zu implementieren.