

Zusammenfassung

Die Benutzerkonten sind der Schlüssel für den Zugang zu den Ressourcen von EDV-Systemen und deren Nutzung. Die Verwaltungsaufgaben von EDV-Systemen erfordern gewisse Sonderrechte gegenüber den Konten der Benutzer, die nur über eingeschränkte Rechte verfügen dürfen. Die Verwaltung der Benutzerkonten dient der Aufrechterhaltung eines hohen Sicherheitsniveaus bei den verschiedenen Prozessen in der Verwaltung der Zugangskennungen zum System und den Ressourcen.

Inhalt

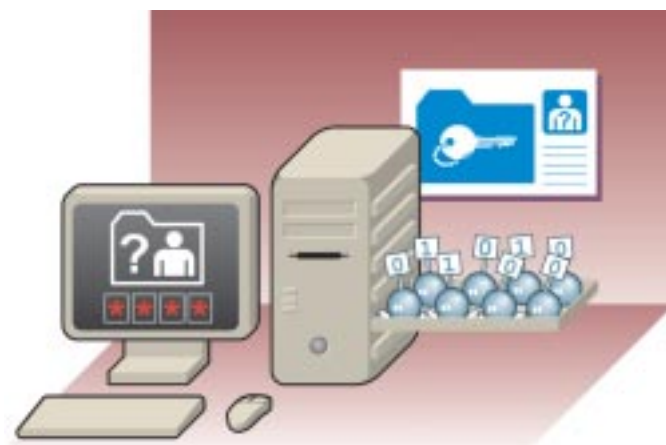
- 1 Was ist die Verwaltung der Konten? →
- 2 Die üblichen Schwachstellen →
- 3 Les impacts potentiels →
- 4 Schutzmaßnahmen →

Dieses Dokument steht in enger Verbindung mit demjenigen über die Authentifizierung der Benutzer in einem EDV-System. Dieses Dokument befasst sich allerdings genauer mit der Verwaltung der Benutzerkonten statt mit der Kombination Benutzername/Passwort.

Hauptziele bei der Verwaltung der Konten sind die Prävention und Begrenzung unzulässiger Handlungen durch identifizierte

Die Benutzer müssen auf die Risiken in Verbindung mit der Verwendung von Benutzerkonten aufmerksam gemacht werden.

Hauptziele bei der Verwaltung der Konten sind die Vorbeugung und Begrenzung unzulässiger Handlungen durch identifizierte Benutzer und die Verhinderung und/oder Kontrolle des Zugangs durch unbefugte externe Personen.



Benutzer und die Verhinderung und/oder Kontrolle des Zugangs durch unbefugte externe Personen.

Die in diesem Dokument enthaltenen Hinweise sind vor allem auf Unix- und Microsoft-Plattformen ausgerichtet. Manche der hier beschriebenen Funktionen stehen auf einigen Systemen nicht zur Verfügung, und ihre Konfiguration kann unterschiedlich ablaufen.

1 Was ist die Verwaltung der Konten?

Unter diesem Begriff sind alle Aufgaben in Verbindung mit dem Erstellen, Ändern und Löschen von Benutzerprofilen eines EDV-Systems sowie die Verfahren zur Kontoführung zusammengefasst.

1.1 Das Benutzerkonto

In der EDV ermöglichen Betriebssysteme die Verwaltung von Sitzungen. Bei der Verbindung mit dem System über eine Kennung und ein Passwort eröffnet das System eine Sitzung mit den Zugangsrechten des Benutzers, der die Sitzung startet.

Das Benutzerkonto ist die Identifizierung eines Benutzers, die ihm die Eröffnung einer Sitzung ermöglicht, und zwar über:

- ➔ die Netzwerk-Domain, um auf die auf diesem Netz verfügbaren Informationen zuzugreifen,
- ➔ seinen lokalen Computer, um auf lokale Ressourcen zugreifen zu können.

1.2 Erstellen von Konten

Bei der Installation des Systems wird automatisch ein Benutzerkonto mit allen Rechten innerhalb des Systems erstellt. Dieses Konto heißt auf Microsoft -Plattformen "Administrator"-Konto und auf Unix -Plattformen "Root"-Benutzer.

Normalerweise wird ein zweites Konto des Typs "Gast/Guest" erstellt. Dieser Benutzer verfügt standardmäßig nicht über alle Rechte innerhalb des Systems, sondern lediglich über diejenigen eines einfachen Benutzers.

Der Systemverwalter ist dafür zuständig, weitere Konten für die Benutzer zu erstellen und ihnen entsprechende Rechte innerhalb des Systems zuzuweisen.

➔ RATSCHLAG:

Diese beiden stets standardmäßig vorhandenen Benutzerkonten sind Zielscheibe von Hackern. Es wird daher dringend empfohlen, diese Konten nicht für die Ausführung von Aufgaben zu verwenden, für die keine Sonderrechte erforderlich sind, und Benutzerkonten mit Sonderrechten umzubenennen, damit deren allgemein bekannte Standardnamen nicht von Hackern missbraucht werden können. Außerdem sollten unbedingt alle Benutzerkonten deaktiviert werden, die nicht mehr genutzt werden - sei es aufgrund des Ausscheidens oder der Versetzung eines Mitarbeiters oder weil diese Benutzerkonten bei der Installation oder Konfiguration von Systemen oder Anwendungen automatisch erstellt wurden.

1.3 Das Profil

Unter Profil versteht man die einem Benutzer zugewiesenen Rechte.

Für eine praxisgerechte und optimale Verwaltung der Benutzer wird die Verwendung von Benutzergruppen empfohlen. Einige Gruppen werden übrigens bei der Initialisierung des Systems automatisch erstellt.

Die Rechte werden dann der Gruppe zugewiesen, und jeder, der dieser Gruppe angehört, hat damit automatisch diese Rechte. Diese Arbeitsweise ermöglicht die einfachere Erstellung und Verwaltung von Benutzern nach ihrer Funktion und beschränkt die Verbreitung komplizierter oder individueller Profile, die in der Praxis nicht verwaltbar sind (RBAC = Role-Bases Access Control).

1.4 Wahl der Konten-Namen

In diesem Bereich muss ein Kompromiss zwischen Sicherheitsbestrebungen und Benutzerfreundlichkeit dieser Kennungen gefunden werden. Allerdings steht ein wichtiger Grundsatz unwiderruflich fest: Die Kennung muss in einer Domain oder auf einem PC absolut einmalig sein.

2

Die üblichen Schwachstellen

Die Schwachstelle der Konten stellen bedeutende Sicherheitslücken dar, die bei Angriffen auf EDV-Systeme ausgenutzt werden. Diese Schwachstellen finden sich auf zwei Ebenen:

- ➔ Verwaltung der Kombinationen Kennung/Passwort,
- ➔ schlechte Verwaltung der Benutzerkonten innerhalb des Systems.

Im Folgenden sind einige der häufigsten Schwachstellen aufgeführt, die bei der Überprüfung von EDV-Systemen festgestellt werden:

In der Regel wird eine Kombination aus dem Familiennamen und den Anfangsbuchstaben des Vornamens gewählt.

➔ RATSCHLAG:

In dieser Kennung darf die Funktion des Nutzers nicht offensichtlich enthalten sein, weil damit Personen mit unlauteren Absichten die Möglichkeit gegeben wird, ihre Attacken auf eine Funktion auszurichten, die ihnen Vorteile verspricht.

1.5 Kritische Konten

Kritisch an den Konten sind lediglich die Rechte, die mit ihrem Profil verbunden sind. Man muss jedoch einräumen, dass gewisse Konten stets in hohem Maße kritisch sind. Es handelt sich dabei um Konten:

- ➔ von System-, Geräte-, Datenbankverwaltern,
- ➔ von Benutzern mit Fernzugang,
- ➔ von Mitarbeitern der EDV-Abteilung,
- ➔ die von Anwendungen zur Kommunikation untereinander verwendet werden.

1.6 Weitere Parameter des Benutzerkontos

Neben direkt definierten Rechten für ein Konto und den Rechten aufgrund der Zugehörigkeit zu gewissen Gruppen kann man auch andere Parameter festlegen, z. B.:

- ➔ privaten Speicherplatz,
- ➔ ein Verfallsdatum des Kontos,
- ➔ ein Verfallsdatum des Kontos,
- ➔ verschiedene Parameter der Passwort-Verwaltung.

2.1 Steigende Anzahl gemeinsam genutzter Konten

En dehors des droits directement définis pour le compte, et des droits hérités par l'appartenance à certains groupes, on peut définir d'autres paramètres, tels que :

Aus unterschiedlichen betrieblichen Gründen teilen sich oft mehrere Benutzer ein Konto. Dieses Phänomen findet sich häufig bei EDV-Teams und tritt in diesem Zusammenhang zur Erhöhung des Risikos bei.

Wo eine Kennung gemeinsam genutzt wird, wird in der Regel auch das dazugehörige Passwort nur selten geändert.

2.2 Steigende Anzahl von Konten mit Administratorrechten

Die Zunahme der Administratorkonten erhöht das Risiko von Sicherheits- und Zuverlässigkeitsproblemen aufgrund der Vielzahl von Konten mit wichtigen Sonderrechten und der sich daraus ergebenden Möglichkeit, dass ein Hacker auf ein Administratorkonto mit einem einfach zu erratenden Passwort stößt und damit über Sonderrechte innerhalb des Systems verfügt.

2.3 Mehrfachsitzen pro Benutzerkonto

Es ist möglich, die gleichzeitige Eröffnung mehrerer Sitzungen mit ein und demselben Konto zuzulassen. Das führt oft dazu, dass Sitzungen auf Rechnern laufen, ohne benutzt zu werden, und daher von Unbefugten zu unlauteren Zwecken verwendet werden können.

2.4 Völliges Fehlen einer Kontenverwaltung

Nicht selten existiert überhaupt keine Kontenverwaltung, was unmittelbar zur Folge hat, dass Konten für Personen offen bleiben,

die nicht mehr dem Unternehmen angehören. Manche dieser Konten sind immer noch mit umfangreichen Vollmachten und sogar mit der Möglichkeit des Fernzugangs versehen.

Unter solchen Umständen findet oft auch keine Überwachung der Protokolle statt, anhand derer man gegebenenfalls unbefugte Zugriffsversuche feststellen könnte.

2.5 Uneinheitliche Kontenverwaltung

Der Verzicht auf die Verwendung von Gruppen führt zur Schaffung zahlreicher persönlicher Profile, die über nach Gutdünken zugewiesene Sonder- und Zugangsrechte verfügen, und damit zu Benutzerkonten mit jeweils anderen Zugriffsrechten auf das System, die, wenn überhaupt, nur sehr schwierig zu verwalten sind. Die Erstellung von Gruppen entsprechend der Funktion der Benutzer (z. B. Verkaufsabteilung, Buchhaltung) ermöglicht es, Rechte auf einfache, praktische und effiziente Art zuzuweisen oder zu entziehen.

3 Mögliche Auswirkungen

Welche Auswirkungen die in Kapitel 2 beschriebenen Schwachstellen haben, kann man sich leicht vorstellen. Derartige Schwachstellen führen nämlich dazu, dass der öffentliche Zugang zu einem EDV-System mit allen seinen Daten und Anwendungen möglich wird.

Ein durchaus vorstellbares Katastrophenszenario wäre ein vollständiger Kontrollverlust über das System, der nur dadurch zu beheben ist, dass man wieder bei Null anfängt, d. h. die Festplatte formatiert, da die Korruption des Systems so weit gehen kann, dass es den Administratoren unmöglich ist, wieder die Kontrolle über dieses System zu erlangen.

4 Schutzmaßnahmen

Im Folgenden sind einige grundlegende Empfehlungen für die Verwaltung der Benutzerkonten aufgeführt:

4.1 Einführung einer Kontenverwaltungspolitik

Nur durch die Einführung von Verfahren für die Verwaltung und Kontrolle der Konten kann ein standardmäßiges, für die Mehrzahl der Konten zufriedenstellendes Sicherheitsniveau gehalten werden. Die Ausnahmen müssen im Anschluss gesondert untersucht werden.

Die Einhaltung dieser Verfahren setzt ein Minimum an Zusammenarbeit zwischen der EDV- und der für Einstellungen, Versetzungen und Entlassungen zuständigen Personalabteilung voraus.

Der jährliche Audit der Kontenverwaltung durch Personen, die nicht der EDV-Abteilung angehören, trägt ebenfalls dazu bei, Lücken und menschlichen Fehlern in diesem Bereich vorzubeugen,

indem die Prozesse in der Produktion und die Rechte und Sonderrechte der Benutzer mit unbefangenen Blick beobachtet werden.

4.2 Verwendung der integrierten Audit-Funktionen

Die meisten Systeme bieten die Möglichkeit, Audit-Dateien des Systems zu erstellen, in denen die Informationen zu den Konten, Versuche zur Erstellung, Änderung, Löschung und Verbindung von Benutzern angegeben sind.

Diese Berichte können Probleme, Fehler und besondere Aspekte der Kontenverwaltung deutlich machen. So deuten beispielsweise Benutzerkonten, die außerhalb der betrieblichen Arbeitszeiten (nachts und am Wochenende) eine Verbindung aufbauen, auf ein Problem bei diesen Benutzerkonten hin. Danach muss eine Untersuchung durchgeführt werden, um die Ursachen festzustellen.

Verwaltung der Konten

4.3 Vermeidung von Mehrfachsitzen und gemeinsam genutzten Konten

Es empfiehlt sich, Profile entsprechend der Funktion der Informatiker zu erstellen, statt ein einziges Konto zu verwenden, das mit sämtlichen Rechten ausgestattet ist.

Eingeschränkte Rechte können in der Tat manchmal verhindern, dass es bei Installationen zu unvorhergesehenen Reaktionen kommt (Löschen von Dateien).

Außerdem ermöglicht die Verwendung von nicht gemeinsam genutzten Konten, unter Einhaltung der geltenden Gesetze und Vorschriften den Urheber eines Fehlers oder einer Veruntreuung festzustellen, während gemeinsam genutzte Konten alle derartigen Ermittlungen verhindern.

4.4 Verwendung gesonderter Konten für Netzwerkverbindungen

Es ist üblich, dass Informatiker von zu Hause aus eine Verbindung aufbauen, um die Funktion gewisser Prozesse zu kontrollieren. Es wird empfohlen, zu diesem Zweck so genannte "Remote" (Fern)-Konten zu erstellen, die nicht identisch mit denjenigen Konten sind, die diese Benutzer/Administratoren verwenden, wenn sie persönlich im Unternehmen anwesend sind. Diese Fernzugangskonten müssen mit dem Minimum an Funktionen und Rechten versehen sein und strengsten Regeln für die Verwendung der Kennungen und der ihnen zur Verfügung gestellten Ressourcen unterliegen, sodass alle Probleme vermieden werden, die aufgrund ihres Standorts außerhalb des für die Benutzer innerhalb des Unternehmens eingerichteten Sicherheitsbereichs entstehen, was sie zum bevorzugten Ziel möglicher Hacker-Angriffe macht.