Warum Mitarbeitende keine Administrator-Rechte auf IT-Systemen benötigen

Management Summary

Die Vergabe von Administrator-Rechten an Mitarbeitende stellt eines der größten vermeidbaren Sicherheitsrisiken in Unternehmen dar. Studien belegen: Ein sehr großer Anteil kritischer Sicherheitslücken in IT-Systemen ließe sich durch die Entfernung von Administratorrechten entschärfen. Für kleine und mittelständische Unternehmen in Deutschland liegt die durchschnittliche Schadenhöhe nach einem erfolgreichen Cyberangriff im hohen fünf- bis sechsstelligen Bereich.

Die Beschränkung auf Benutzerrechte ist keine Einschränkung der Arbeitsfähigkeit, sondern eine strategische Schutzmaßnahme – sowohl für das Unternehmen als auch für die Mitarbeitenden selbst. Moderne Lösungen ermöglichen es, notwendige Funktionen bereitzustellen, ohne die Sicherheit zu gefährden.

Die Bedrohungslage: Fakten statt Vermutungen

Cyberangriffe zielen gezielt auf privilegierte Rechte ab

Die Cybersicherheitslage hat sich in den vergangenen Jahren deutlich verschärft. Ein Großteil moderner Angriffe nutzt identitätsbasierte Methoden, bei denen Angreifer versuchen, sich Zugang zu Konten mit erhöhten Berechtigungen zu verschaffen. Haben sie erst einmal einen Account mit Administratorrechten kompromittiert, können sie:

- Schadsoftware tief im System verankern und Sicherheitsmechanismen deaktivieren

- Auf vertrauliche Unternehmensdaten zugreifen und diese exfiltrieren
- Weitere Systeme im Netzwerk infiltrieren (laterale Bewegung)
- Ransomware installieren, die das gesamte Unternehmen lahmlegt
- Backdoors für zukünftige Angriffe einrichten

Die Erwartung, dass jedes Unternehmen früher oder später von einem kompromittierten Konto betroffen ist, ist angesichts der aktuellen Bedrohungslage realistisch – nicht pessimistisch.

Reale Beispiele zeigen die Folgen

Die Ransomware-Angriffe **WannaCry** und **NotPetya** verursachten weltweit Schäden in Milliardenhöhe. Beide Angriffe hätten durch elementare Sicherheitsmaßnahmen wie konsequentes Privilegien-Management deutlich entschärft werden können. Besonders betroffen waren Unternehmen, in denen Mitarbeitende mit lokalen oder Domänen-Administratorrechten arbeiteten – dort konnte sich Malware ungehindert ausbreiten.

Kleine und mittlere Unternehmen besonders gefährdet

Der Satz „Wir sind zu klein, um interessant zu sein“ ist ein gefährlicher Irrtum. Zahlen zeigen:

- Ein erheblicher Anteil der Kleinstunternehmen (bis 9 Mitarbeitende) war bereits Opfer von Cyberangriffen
- Der Anteil betroffener Unternehmen steigt mit der Unternehmensgröße deutlich an
- Insgesamt waren bereits weit über eine Million KMU in Deutschland von Cyberangriffen betroffen

Kleinere Unternehmen geraten verstärkt in den Fokus, weil sie häufig geringere Sicherheitsmaßnahmen haben und Angreifer hier mit wenig Aufwand hohe Wirkung erzielen können. Zudem dienen sie oft als Einfallstor für Angriffe auf größere Kunden.

Die Zahlen sprechen eine klare Sprache

Vermeidbare Sicherheitslücken durch Admin-Rechte

Auswertungen großer Schwachstellen-Reports (u. a. zu Microsoft-Produkten) über viele Jahre zeigen:

- Ein Großteil der als kritisch eingestuften Schwachstellen könnte entschärft werden, wenn Benutzer nicht mit Administratorrechten arbeiten würden
- In manchen Produktgruppen (z. B. Browser, Office) wären nahezu alle kritischen Sicherheitslücken ohne Admin-Rechte deutlich weniger gefährlich

Das bedeutet: **Die einfache Maßnahme, Administratorrechte zu entfernen, reduziert die Angriffsfläche drastisch.**

Die finanziellen Folgen sind erheblich

Cyberangriffe verursachen für Unternehmen:

Direkte Kosten:

- hohe fünf- bis sechsstellige durchschnittliche Schäden bei KMU
- bis in den Millionenbereich bei großen Unternehmen

Indirekte Kosten:

- Betriebsunterbrechungen von mehreren Tagen
- Reputationsschäden und Vertrauensverlust bei Kunden
- Kundenverluste und Auftragsstornierungen
- Rechts- und Beratungskosten
- mögliche Schadenersatzforderungen

Ein einziger schwerer Vorfall kann insbesondere kleine und mittelständische Unternehmen existenziell gefährden.

Konkrete Risiken durch Administratorrechte

1. Schadsoftware erhält erweiterte Privilegien

Wenn ein Mitarbeitender mit Administratorrechten versehentlich eine infizierte E-Mail öffnet oder auf einen präparierten Link klickt, erhält die Schadsoftware automatisch dieselben erweiterten Rechte. Dadurch kann sie:

- systemweit installiert werden
- Sicherheitssoftware deaktivieren
- Systemdateien manipulieren
- sich dauerhaft im System verankern

Bei Standard-Benutzerkonten ohne Administratorrechte scheitern viele dieser Aktionen an den Betriebssystem-Sicherheitsmechanismen. Das schränkt die Wirkung von Malware massiv ein oder verhindert sie komplett.

2. Menschliche Fehler mit schwerwiegenden Folgen

Menschliche Fehler sind eine der häufigsten Ursachen für Sicherheitsvorfälle. Administratorrechte verstärken die Auswirkungen solcher Fehler erheblich:

Typische Szenarien:

- Versehentliche Löschung wichtiger Daten oder ganzer Verzeichnisse
- Unbeabsichtigte Änderungen von Systemeinstellungen, die Ausfälle verursachen
- Installation unsicherer oder nicht freigegebener Software
- Falsche Vergabe von Berechtigungen, die unbefugten Zugriff ermöglichen

Ohne Administratorrechte sind die Auswirkungen solcher Fehler deutlich begrenzt. Viele kritische Aktionen werden vom System gar nicht erst zugelassen.

3. Gezielte Angriffe auf privilegierte Accounts

Admin-Konten sind für Angreifer besonders attraktiv, da sie damit:

- schnell umfassenden Zugriff auf Systeme und Daten erhalten

- weitere Konten kompromittieren können
- Sicherheitsmechanismen aushebeln
- Spuren verwischen

Typische Angriffsmethoden:

- Phishing-Mails an Mitarbeitende mit erweiterten Rechten
- Social Engineering (z. B. angebliche IT-Hotline)
- Ausnutzen wiederverwendeter oder schwacher Passwörter
- Ausnutzung von Schwachstellen in Anwendungen und Betriebssystemen

Ein einziges kompromittiertes Admin-Konto kann ausreichen, um das gesamte Unternehmen zu kompromittieren.

4. Insider-Bedrohungen und Schatten-Administratoren

Nicht jede Bedrohung kommt von außen. Risiken entstehen auch durch:

- unzufriedene oder ausscheidende Mitarbeitende
- externe Dienstleister mit zu weitgehenden Berechtigungen
- „Schatten-Administratoren“: Konten, die versehentlich oder historisch bedingt mehr Rechte haben als notwendig

Solche überprivilegierten Konten sind schwer zu überblicken und damit ein enormes Sicherheits- und Compliance-Risiko.

Der Schutz der Mitarbeitenden selbst

Haftungsrisiken für Administratoren

Mitarbeitende mit Administratorrechten tragen auch persönlich höhere Risiken:

- Strafrechtliche Risiken (z. B. unzulässiger Zugriff auf Daten, die nicht für sie bestimmt sind)
- Arbeitsrechtliche Konsequenzen (Abmahnung, Kündigung) bei grober Fahrlässigkeit oder Datenmissbrauch
- Zivilrechtliche Regressforderungen des Arbeitgebers in Extremfällen

Wichtig: Nur weil jemand technisch auf bestimmte Daten zugreifen kann, heißt das nicht, dass er das rechtlich darf. Administratorrechte schützen nicht vor straf- oder arbeitsrechtlicher Haftung.

Entlastung durch klare Verantwortlichkeiten

Die Beschränkung von Rechten entlastet Mitarbeitende:

- Keine Verantwortung für systemweite Sicherheitsentscheidungen
- Klare Abgrenzung, wofür sie zuständig sind – und wofür nicht
- Weniger Druck und Unsicherheit bei IT-relevanten Entscheidungen
- Geringeres Risiko, sich unbewusst „falsch“ zu verhalten

Als Unternehmen schützen wir unsere Mitarbeitenden vor Situationen, in denen sie aus Unwissenheit oder Zeitdruck schwerwiegende Entscheidungen treffen könnten.

Schutz vor unbeabsichtigten Fehlern

Die meisten Mitarbeitenden handeln in bester Absicht, verfügen aber nicht über tiefes IT-Sicherheitswissen. Typische Fehler:

- Klicken auf täuschend echt wirkende Phishing-Mails
- Ausführen vermeintlich hilfreicher Tools aus dem Internet
- Unbedachte Bestätigung von Sicherheitsabfragen

Ohne Administratorrechte dienen die Sicherheitseinstellungen des Systems als „Airbag“, der viele dieser Fehler abfängt, bevor daraus ein Schaden entsteht. Das ist gelebter Mitarbeiterschutz.

Das Least-Privilege-Prinzip: Die professionelle Lösung

Was bedeutet Least Privilege?

Das **Least-Privilege-Prinzip** (Prinzip der minimalen Berechtigung) bedeutet:

> Jede Person und jede Anwendung erhält nur genau die Rechte, die zur Erfüllung der konkreten Aufgabe unbedingt erforderlich sind – nicht mehr.

Kernelemente:

- Minimierung der vergebenen Rechte
- Beschränkung auf das notwendige Maß
- Zeitliche Begrenzung, wo sinnvoll
- Regelmäßige Überprüfung und Anpassung

Dieses Prinzip ist etablierter Standard in der Informationssicherheit und Bestandteil nahezu aller relevanten Normen und Richtlinien (DSGVO, ISO 27001, NIS2, BSI IT-Grundschutz).

Praktische Umsetzung ohne Produktivitätsverlust

Ein häufiges Argument lautet: „Meine Mitarbeitenden brauchen diese Rechte, sonst können sie nicht arbeiten.“ Mit modernen Konzepten und Werkzeugen ist das meist nicht mehr zutreffend.

1. Separate Konten für Admin-Aufgaben

Personen, die administrative Aufgaben haben (z. B. IT), arbeiten im Alltag mit einem normalen Benutzerkonto und verwenden ein getrenntes Admin-Konto nur für reine Administrationsaufgaben. So ist der Großteil der Arbeit abgesichert, während administrative Tätigkeiten bewusst und kontrolliert stattfinden.

2. Granulare Berechtigungsvergabe

Statt pauschaler „Admin für alles“-Rechte werden Berechtigungen möglichst fein zugeschnitten vergeben, z. B.:

- Installationsrechte nur für bestimmte, freigegebene Anwendungen
- Zugriff nur auf die wirklich benötigten Ordner und Systeme
- spezielle Rechte für definierte Aufgaben, nicht für das gesamte System

3. Just-in-Time-Rechte (temporäre Rechte)

Erhöhte Rechte werden nur für einen begrenzten Zeitraum vergeben, z. B.:

- Mitarbeitender beantragt Installation einer bestimmten Software
- Führungskraft oder IT gibt dies für einen begrenzten Zeitraum frei
- Rechte verfallen automatisch nach Abschluss der Aktion

So stehen Rechte nur dann zur Verfügung, wenn sie wirklich benötigt werden – und nicht dauerhaft.

4. Self-Service mit Freigabe-Workflow

Mitarbeitende können bei Bedarf zusätzliche Berechtigungen anfragen:

- Anfragen laufen über definierte Workflows
- Genehmigung durch Vorgesetzte oder Datenverantwortliche
- IT setzt die Berechtigungen strukturiert um
- Alle Schritte werden dokumentiert

Damit lassen sich Produktivität und Sicherheit in Einklang bringen.

Compliance und rechtliche Verpflichtungen

DSGVO (Datenschutz-Grundverordnung)

Art. 32 DSGVO verpflichtet Unternehmen, ein dem Risiko angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicherzustellen. Dazu gehören insbesondere:

- Zugriffskontrollen
- Berechtigungskonzepte
- Dokumentation der vergebenen Rechte
- Regelmäßige Überprüfung und Anpassung

Ein unkontrolliertes Vergabeverhalten von Administratorrechten kann im Falle eines Datenschutzvorfalls als Verstoß gegen diese Pflichten gewertet werden und sich negativ auf Bußgelder auswirken.

ISO 27001

Die ISO 27001 fordert unter anderem:

- kontrollierte Vergabe privilegierter Zugriffsrechte
- klare Regelungen für Access Management

- regelmäßige Überprüfungen von Zugriffsrechten

Least Privilege ist hier etablierte Best Practice. Unternehmen, die zertifiziert sind oder eine Zertifizierung anstreben, müssen ein sauberes Berechtigungsmanagement nachweisen.

NIS2

Die NIS2-Richtlinie verstärkt die Anforderungen an Unternehmen in kritischen und wichtigen Sektoren. Kernelemente in Bezug auf Berechtigungen:

- Need-to-know und Need-to-use als Grundprinzip
- Aufgabentrennung und kein unnötiger Rechte-Mix
- Genehmigungspflicht für Zugriffsrechte
- Register aller Zugriffsrechte
- regelmäßige Überprüfung und Protokollierung

Hier ist ein strukturiertes Berechtigungsmanagement zwingend erforderlich.

BSI IT-Grundschutz

Der BSI IT-Grundschutz konkretisiert Anforderungen an Identitäts- und Berechtigungsmanagement, u. a.:

- Berechtigungen nach täglichem Bedarf
- zeitnahe Entfernung nicht mehr benötigter Rechte
- Dokumentation aller Berechtigungen und Änderungen
- nur Administratoren dürfen sicherheitsrelevante Änderungen vornehmen

Auch hier ist das Least-Privilege-Prinzip grundlegend.

Handlungsempfehlungen: Der Weg zu mehr Sicherheit

Sofortmaßnahmen (Woche 1–2)

1. **Bestandsaufnahme**
   - Welche Mitarbeitenden haben aktuell lokale oder Domänen-Adminrechte?

- Welche Dienstkonten besitzen erhöhte Rechte?
- Wo gibt es „Schatten-Administratoren“?

2. **Risikobewertung**
   - Welche Systeme und Daten sind besonders schützenswert?
   - Wo wären die Auswirkungen eines Vorfalls am größten?
3. **Kommunikation**
   - Mitarbeitende frühzeitig informieren, warum Änderungen notwendig sind
   - Zielbild erklären: Schutz des Unternehmens UND der Mitarbeitenden
   - Transparenz schaffen, um Widerstände zu reduzieren

Mittelfristige Umsetzung (Monat 1–3)

4. **Berechtigungskonzept erstellen**
   - Rollen definieren (z. B. Vertrieb, Buchhaltung, IT, Management)
   - pro Rolle die notwendigen Rechte festlegen (Need-to-know/Need-to-use)
   - Vorgaben für temporäre Rechte und Sonderfälle definieren
   - Freigabeprozesse (z. B. Vier-Augen-Prinzip) festlegen
5. **Technische Lösungen einführen**
   Je nach Größe und Komplexität:
   - Nutzung von integrierten Bordmitteln (z. B. in Microsoft-Umgebungen)
   - Einführung von Privileged-Access-Management-Lösungen (PAM)
   - zentrale Verwaltung lokaler Admin-Konten
   - Automatisierte Prozesse für Rechteanträge und -freigaben
6. **Schrittweise Rechte-Reduktion**
   - Pilotgruppen definieren und umstellen
   - Erfahrungen auswerten und Prozesse anpassen
   - sukzessive Umsetzung im gesamten Unternehmen

Langfristige Verankerung (laufend)

7. **Regelmäßige Überprüfung**
   - Mindestens jährlich: komplette Rechte-Überprüfung („Rezertifizierung“)
   - Bei Rollenwechseln: sofortige Rechteanpassung
   - Bei Austritt: umgehende Sperrung und Entzug aller Berechtigungen
8. **Schulungen**
   - Regelmäßige Sensibilisierung zu IT-Sicherheit und Berechtigungen
   - Schulungen für Führungskräfte zur Rolle im Berechtigungsprozess
   - praktische Hinweise zum sicheren Arbeiten (E-Mail, Passwörter, Homeoffice)
9. **Monitoring und Incident Response**
   - Überwachung auffälliger Aktivitäten (z. B. ungewöhnliche Logins, Massenänderungen)
   - definierter Notfallplan bei Sicherheitsvorfällen

    - regelmäßige Backups und Wiederherstellungstests
10. **Dokumentation und Nachweis**
    - Führen eines Berechtigungsregisters
    - Protokollierung von Änderungen
    - Dokumentation von Entscheidungen (warum hat wer welche Rechte?)

Wirtschaftliche Betrachtung: Kosten vs. Nutzen

Kosten der Maßnahmen

Je nach Unternehmensgröße entstehen Kosten u. a. für:

- Software/Lizenzen (z. B. PAM, IAM, zusätzliche Sicherheitsfunktionen)
- Implementierung und Konfiguration
- Schulungen für Mitarbeitende und Administratoren
- laufende Betreuung und Pflege

Nutzen und Einsparpotenzial

Dem stehen gegenüber:

- deutlich reduziertes Risiko eines schwerwiegenden Cyberangriffs
- geringere Ausfallzeiten
- weniger Aufwand für Störungsbeseitigung
- geringere rechtliche und finanzielle Risiken durch Compliance-Verstöße
- bessere Position in Audits, Kundenprüfungen und Zertifizierungen

In vielen Szenarien amortisiert sich die Investition bereits mit der Vermeidung eines einzigen größeren Vorfalls.

Fazit: Verantwortung wahrnehmen, Risiken minimieren

Die Vergabe von Administratorrechten an Mitarbeitende ist ein unnötiges und vermeidbares Risiko. Die wichtigsten Punkte:

- Administratorrechte vervielfachen die Wirkung von Fehlern und Angriffen
- Die meisten kritischen Schwachstellen werden erst durch überhöhte Rechte wirklich gefährlich
- Moderne Arbeitsweisen erfordern in der Regel keine dauerhaften Adminrechte
- Least Privilege ist Best Practice und rechtlich wie normativ verankert
- Die Beschränkung auf Benutzerrechte schützt Unternehmen UND Mitarbeitende

Die Einführung eines strukturierten Berechtigungsmanagements ist ein zentraler Baustein moderner Informationssicherheit. Es ist nicht nur eine technische Frage, sondern Ausdruck gelebter Verantwortung gegenüber Mitarbeitenden, Kunden und dem Unternehmen selbst.

Kernaussage für das Management:
Dauerhafte Administratorrechte für normale Mitarbeitende sind aus Sicherheits-, Compliance- und Haftungssicht nicht vertretbar. Ein gut durchdachtes Rechtekonzept mit konsequentem Least-Privilege-Prinzip ist Pflicht – nicht Kür.

Version #2
Erstellt: 2026-01-30 12:45:21 UTC von Frank Böttger
Zuletzt aktualisiert: 2026-01-30 12:49:23 UTC von Frank Böttger