

# Den Admins auf die Finger geschaut

IT-Verantwortliche wissen in vielen Fällen nicht, was mit sensiblen Daten passiert

IT-Sicherheit bedeutet nicht nur Sicherheit der Daten gegen Zerstörung oder unbefugten Zugriff. Auch berechnete Zugriffe können zu Rechtsverstößen mit schwerwiegenden Folgen für das gesamte Unternehmen führen. Deshalb gilt auch hier: Vertrauen ist gut, ein effektives Kontrollsystem ist besser.

Unternehmen müssen ihre Infrastruktur und Data Center zwangsläufig einer Vielzahl von Dritten öffnen. Outsourcing-Partner benötigen Zugang für Remote-Administration, Soft- und Hardware-Partner erhalten Zugang, um Wartungsarbeiten durchzuführen oder im Ernstfall schnell Probleme beheben zu können. Auch den eigenen Administratoren wird der Weg von außen ins Intranet geöffnet, damit sie für ein schnelles Trouble Shooting aus dem Home Office sorgen können. Der sichere Zugriff wird in der Regel durch technische Lösungen wie IPSEC VPN, SSL VPN, Modems, dezidierte Standleitungen, Citrix und andere Terminal Services gewährleistet. Damit ist aber lediglich die interne Infrastruktur gegen unberechtigten Zugriff von außen abgesichert. Sind Nutzer mit Administrator-Rechten am System erst einmal angemeldet, können ihre Aktivitäten nur schwer kontrolliert werden. Häufig ist nicht nachvollziehbar, wer welche Schritte im System unternommen hat. Der IT-Verantwortliche weiß in vielen Fällen nicht, was mit sensiblen Daten passiert. Die vorgesehene Kontrolle wird durch Vertrauen ersetzt. Dies ist ein Zustand, der für Banken und Versicherungen schon aus Eigeninteresse nicht tragbar ist. Aber auch gesetzliche Vorgaben schreiben eine Kontrolle vor.

## Management in Verantwortung

Das US-Bundesgesetz Sarbanes-Oxley Act legt beispielsweise in Abschnitt 404 fest: „Das Management ist dafür verantwortlich, angemessene interne Kontrollstrukturen sowie Maßnahmen zur Finanzberichterstattung einzurichten und zu pflegen.“ Auch die Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin fordert in Abschnitt AT 7.2 „Insbesondere sind Prozesse

für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.“ Somit wird es immer wichtiger, Infrastrukturen zu schaffen, in denen zumindest Administrationsvorgänge transparent dokumentiert und beweissicher protokolliert werden können.

Technisch gibt es einige Ansätze, der lokalen Allmacht der Administratoren mit lückenloser Kontrolle zu begegnen. Remote-Logging von Systemereignissen oder der Einsatz von lokalen Monitor-Plugins ist dabei wenig empfehlenswert. Diese Lösungen protokollieren zwar die Aktivitäten der Administratoren, weisen in der Regel jedoch eine hohe Komplexität in der Administration auf. Besonders kritische Aktivitäten wie beispielsweise das illegale Kopieren von vertraulichen Daten lassen sich mit diesen Methoden zudem selten aufzeichnen und nachweisen.

Es stellt sich also zunächst die Frage, wie man Rollenkonzepte und die damit verbundenen Zugriffsrechte im täglichen IT-Betrieb so durchsetzen kann, dass die Wartung und die Administration dieser speziellen Infrastruktur nicht zu einer neuen und kostspieligen Herausforderung wird. Die Lösung dieses Problems ist nicht neu aber nach wie vor effektiv: Ähnlich dem Prinzip eines Proxys wird eine direkte Übertragung von schützenswerten Dateien auf das System des Benutzers verhindert. Viele der gängigen Produkte im Markt setzen auf ein zentrales IT-System, über das jegliche Administration erledigt werden muss. Im einfachsten Fall meldet sich der Administrator über einen Webbrowser von einem beliebigen Web-fähigen Endgerät an dem System an.

## Zugriffsrechte verwalten

Schon an diesem Punkt können Unternehmen die Verwaltung der Zugriffsrechte zentralisieren – sowohl für Benutzer als auch Administratoren. In Access-Profilen legt der IT-Verantwortliche fest, welcher Benutzer sich in welchem Zeitraum auf welches

„Insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.“

MaRisk, AT 7.2

System einloggen darf und welche Applikationen ihm zur Verfügung stehen. Dieses System ist sicher und flexibel: Muss zur Lösung eines Problems der Supporter eines Partners auf das System zugreifen, erhält er nur für einen begrenzten Zeitraum Zugriff. Damit ist die Gefahr gebannt, diese Freischaltung nach dem Service zu vergessen und offen zu lassen. Eher Kür als Pflicht: Ein Task-basierendes Ticketing System erlaubt auch noch die Überprüfung der Einhaltung von Service Level Agreements und unterstützt die internen ITIL-Prozesse.

## Vier-Augen-Prinzip

Sensible Daten, wie zum Beispiel personenbezogene Daten, dürfen Administratoren nur in Anwesenheit des betrieblichen Datenschutzbeauftragten oder anderer Dritter zugänglich sein. Dazu zählen im Prinzip schon so alltägliche Informationen wie die, die sich aus den Log-Dateien des E-Mail-Verkehrs und Webnutzung einzelner Benutzer ergeben. Unternehmen sollten deshalb bei der Anschaffung darauf achten, dass das System auch die technische Einhaltung des Vier-Augen-Prinzips unterstützt.

## VideoLog und Keystroke Recording

Wenn die präventiven Systeme nicht greifen, geht es darum, wenigstens den Verantwortlichen zu finden. Grundlage für den Erfolg ist, dass sämtliche Administrationsaktivitäten in command shells und grafischen Sitzungen so aufgezeichnet werden, dass sie auch vor Gericht Beweiskraft haben. Die Protokolle sollten also zuverlässig signiert sein, um ihre Authentizität nachweisen zu können. Eine zusätzliche Verschlüsselung der Daten schützt vor den Augen Neugieriger. Um die anfallenden Datenberge im Notfall auszuwerten zu können, sollten Unternehmen darauf achten, dass das System eine effiziente Suche ermöglicht. Thumbnails

sind beispielsweise durchaus nützlich, wenn der IT-Verantwortliche in einer kurzen RDP-Sitzung etwas schnell finden muss. Auch die Möglichkeit der Suche nach speziellen Keywords in einer RDP-Sitzung ist mittlerweile Standard und hilft Zeit zu sparen. In modernen Rechenzentren wird auch heute noch eine Vielzahl von Sprachen gesprochen, wenn es um die Kommunikation mit Systemen geht. Die Protokolle X11, RDP, VNC, telnet, SSH, tn3270, tn5250 und ICA sind nahezu allgegenwärtig. Deshalb sollte bei der Auswahl des Kontroll-Systems ein Produkt gewählt werden, das möglichst viele dieser Protokolle unterstützt. So hängen zukünftige Strategie-Entscheidungen nicht von den Fähigkeiten des Überwachungssystems ab.

## Von der Pflicht zur Kür

Wenn die gesetzlichen Vorgaben nach Kontrollierbarkeit und Nachvollziehbarkeit von IT-Prozessen technisch erfüllt sind, stellt sich die Frage, in welchen Bereichen ein solches System weitere Vorteile ausspielen kann. Dies hängt von den individuellen Gegebenheiten im Unternehmen ab. Beispielsweise können Features wie Desktop-Sharing das Incident-Management unterstützen. Der Helpdesk hat hier die Möglichkeit direkt, nur sehend oder auch interaktiv den Anwendern bei der Schilderung eines Incidents über die Schulter zu schauen.



Autor:  
Dr. Jörg Kümmerlen  
Berater der DV-RATIO  
Unternehmensberatung

„Das Management ist dafür verantwortlich, angemessene interne Kontrollstrukturen sowie Maßnahmen zur Finanzberichterstattung einzurichten und zu pflegen.“

Sarbanes-Oxley Act, 404