

## Richtlinien für Systemkoordinatoren (m/w)

Die Rolle des Systemkoordinators (m/w) erfordert die konsequente und permanente Pflege der IT-Umgebung seines Arbeitgebers.

Die wichtigsten Grundlagen zur Vorgehensweise werden im Seminar „Systemkoordinator III“ vermittelt. Außerdem wird in einem Zusatzseminar die „Hard- und Softwareumgebung und gevis Umgebungen für Systemkoordinatoren“ geschult. Der nachfolgende Artikel fasst die wichtigsten Aufgaben des Systemkoordinators zusammen. Arbeiten der GWS, die im Aufgabenbereich des Systemkoordinators liegen, sind immer kostenpflichtig. Die „Rechtlichen Bedingungen“ am Ende dieses Dokuments sind Grundlage und fester Bestandteil dieses Dokuments.

## Netzübergabe und Kennwörter

Bei Übergabe eines Netzwerks von der GWS an den Kunden ist das Netzwerk mit „Auslieferungswerten“ ausgestattet. Außerdem sind die Systeme zunächst mit einem generischen „Passwort ab Werk“ vorbetankt. Der Systemkoordinator hat die Aufgabe, nach eigenem Ermessen das Ändern und Aktualisieren der Passwörter vorzunehmen. Im Dokument „passwortaenderungskonzept.doc“ auf der Seminar-CD ist beschrieben, welche Abhängigkeiten es bei den administrativen Konten gibt und wie man die Kennwörter ändert. Da jedes Netz ein Einzelfall ist, sind weitere, undokumentierte Abhängigkeiten möglich. Daher ist es zwingend erforderlich, dass der Systemkoordinator Passwortänderungen zuvor mit seinem Betreuer der GWS abstimmt. Begleitend zu diesen Selbsthilfe-Maßnahmen kann durch einen Vorort-Einsatz eines GWS-Beraters bei Bedarf ein Sicherheits-Check mit anschließender Aktualisierung erfolgen.

Ansprechpartner ist Patrick Bärenfänger [pba@gws.ms](mailto:pba@gws.ms)

## Sicherheitsupdates Microsoft

Von der GWS ausgelieferte Neusysteme werden jeweils mit den wichtigsten Sicherheitsupdates vorinstalliert geliefert. Schon wenige Tage nach Übergabe der Systeme können aber neue Sicherheitslücken bekannt werden. Die Aktualisierung der Systeme kann nur vor Ort erfolgen und gehört zu den Pflichten des Systemkoordinators. Zur Vereinfachung der Updateverteilung bietet Microsoft ein kostenloses Produkt namens „WSUS“, das aber vom Microsoft-Support leider nicht unterstützt wird. Die GWS hilft Ihnen auf Anfrage bei der Installation und Konfiguration, wird aber keinen Support auf dieses Produkt gewähren können.

Für Windows 98 und NT müssen die Updates manuell heruntergeladen und installiert werden. Gleiches gilt für die Versorgung der PCs in den Zweigstellen. Hier muss der Systemkoordinator eine CD mit den aktuellen Sicherheitsupdates erstellen und diese z.B. 1x monatlich in den Zweigstellen einspielen.

Die Aktualisierung der Server darf nicht automatisch erfolgen, da ansonsten die Gefahr eines automatischen Neustarts während der Geschäftszeit gegeben ist. Zum Aktualisieren der Server kann an der Konsole die Windowsupdate-Seite aufgerufen werden. Einige Grundregeln zur Sicherheit sind unter <http://www.gws.ms/sicherheit> zusammengestellt.

## Datensicherung

Bei Auslieferung des gevis Servers (erster Domänencontroller) ist die Datensicherungssoftware „Symantec (ehem. Veritas) Backup Exec“ in Verbindung mit einem Bandlaufwerk vorkonfiguriert. Im Rahmen der Installation wird durch die GWS ein Sicherungsauftrag konfiguriert, der täglich die Inhalte der wichtigsten Server und die von gevis komplett auf ein Band schreiben kann.

Das Wechseln der Bänder, das Austauschen aller Bandmedien einmal pro Jahr, das wöchentliche Verwenden eines Reinigungsbandes und ggf. Austausch, wenn verbraucht, sowie die Kontrolle der erfolgreichen Datensicherung sind Aufgaben des Systemkoordinators.

Zur Gewährleistung der Sicherheit wird die regelmäßige Probe-Rücksicherung von Datenordnern in ein temporäres Verzeichnis empfohlen.

Weitere Aufgaben sind die ordnungsgemäße und feuer- und entwendungssichere Lagerung der Bänder.

## Firewall

Es ist allgemein bekannt, dass keine Firewall gegen Schadprogramme schützt, die ein Benutzer beim Surfen oder beim Empfangen von eMails einschleust. Eine Firewall schützt gegen direkte Angriffe von Hackern aus dem Netz und regelt die Zugangsberechtigungen zum Internet von innen. Sie erlaubt nur bestimmte Dienste. In Netzwerken erfolgt der Internetzugang über das Produkt w.safe, das Firewall-System der GWS. Die GWS-Firewall wird von der GWS gepflegt und gewartet.

Der Systemkoordinator kümmert sich um die Beauftragung und Bereitstellung eines Internetzugangs (ISDN oder xDSL)

## Virenschutz

Für Kunden, die ihre Internet-Domains und den Mailverkehr über die GWS abwickeln, betreibt die GWS einen zentralen eMail-Virenschanner/Spamfilter auf Basis von Kaspersky Antivirus. Unabhängig davon ist zusätzlich immer ein lokaler Virenschutz für die Server und Arbeitsplätze vor Ort notwendig. Der Systemkoordinator kann von uns den Virenschutz „Kaspersky Antivirus“ für Server und Arbeitsplätze erwerben und lizenzieren. Aufgrund der ständigen Mutationen von Schadprogrammen wird aber auch ein aktuelles Virenschutzprogramm keinen 100%igen Schutz bieten.

Die Aufgabe des Systemkoordinators ist es, auf allen Systemen in seinem Netzwerk für aktuelle Virus-Signaturen zu sorgen. Bei Bedarf kann das Kaspersky Administrationskit installiert werden, das automatisch neue Virus-Signaturen im Netzwerk verteilt.

Arbeitsplätze mit vertaulichen Daten müssen regelmäßig auf Befehl durch Trojanischen Pferde/Würmer untersucht werden. Ergänzend zum Virenschanner eignet sich dazu beispielsweise „SpyBot Search&Destroy“

## First Level Support

Der Systemkoordinator ist der erste Ansprechpartner seiner/ihrer Kollegen bei IT-Problemen. Dazu gehören das Beheben von Druckerstaus, kleineren Netzwerkstörungen, das Erkennen und Beseitigen von Bedienerfehlern. Gleichwohl ist der Systemkoordinator die Schnittstelle zum KSC. Schnelle Hilfe ist nur möglich, wenn die übermittelte Diagnose/Problembeschreibung qualitativ hochwertig ist.

## Organisation

Der Systemkoordinator ist verantwortlich für den rechtskonformen Einsatz von Software und die korrekte Lizenzierung. Er bewahrt die Lizenzen an einem sicheren Ort auf. Durch organisatorische Maßnahmen und geeignete Betriebsvereinbarungen wird das Risiko „Störungen durch Benutzer“ verkleinert. (Benutzer werden angewiesen, nicht jeden eMail-

Anhang zu öffnen etc.) Solche Maßnahmen müssen vom Systemkoordinator eingeleitet oder beauftragt werden.

Der Systemkoordinator ist mit exponierten Rechten ausgestattet und muss daher besondere Sorgfalt im Umgang mit den Daten wahren, um nicht mit den Regelungen des Datenschutzgesetzes (BDSG) in Konflikt zu geraten. Details sind im entsprechenden Gesetzestext nachzulesen.

Der Systemkoordinator arbeitet eng mit dem für das Unternehmen vorgeschriebenen Datenschutzbeauftragten zusammen und liefert diesem die nötigen Prüfunterlagen.

## Rechtliche Bedingungen

Unsere Referate, Artikel, Anleitungen und CDs sind so produziert, dass Ihre Systemkoordinatoren, die das Systemkoordinator 3-Seminar besucht haben, sinnvoll damit umgehen können.

Bei unseren Hinweisen für die Systemkoordinatoren handelt es sich um Empfehlungen, für die die GWS keinerlei Haftung übernimmt. Für die Umsetzung der Datensicherheit, die Einhaltung des Datenschutzgesetzes und sonstiger gesetzlicher und betrieblicher Bestimmungen, ist das jeweilige Unternehmen allein verantwortlich.

Bitte haben Sie Verständnis dafür, dass unser KSC nur Unterstützung für GWS-eigene Produkte sicherstellen kann und eine detaillierte Unterstützung für Patches/ServicePacks fremder Hersteller nicht zum Supportangebot der GWS gehören.

Die Angaben, die auf unseren Webseiten oder in Informationsschriften zur Verfügung gestellt werden, dienen ausschließlich der allgemeinen Information und dienen nicht der Beratung von Kunden im konkreten Einzelfall. Der Autor hat diese Informationen gewissenhaft zusammengestellt, übernimmt jedoch keine Haftung für Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, die sich auf Schäden materieller oder ideeller Art beziehen, welche durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind ausgeschlossen. Das Einspielen der Sicherheitsupdates und Service-Packs geschieht allein auf eigenes Risiko. Eine Beseitigung von dadurch entstandenen Schäden durch die GWS ist kostenpflichtig.