

## Informationen zum Datenschutz

Aus Sicherheitsgründen ermöglichen die meisten Netzwerkverwalter externen Benutzern nur ungern den Zugriff auf ihr System über einen WAN-Anschluß. Beim Anschluß an das SAP-Servicenetz behalten Sie die volle Kontrolle über die Verbindung. Der Zugriff von SAP auf Ihr System ist begrenzt, und Sie können alle Aktivitäten der SAP in Ihrem System verfolgen.

- ❑ Sie allein kontrollieren die Netzwerkverbindung, denn sie bauen die Verbindung auf und beenden sie wieder.
- ❑ Ihre Firmendaten sind den EarlyWatch-Experten nicht zugänglich. Benutzerkennung und Paßwort des EarlyWatch erlauben lediglich den Zugriff auf die Datenbank mit den Leistungsdaten sowie auf die Überprüfungstools.
- ❑ Der Zugriff auf Ihr Netzwerk kann mit Hilfe von Routern, wie z. B. dem SAProuter, weiter eingeschränkt werden.
- ❑ Sie können die Tätigkeit des SAP-Experten über den Echo-Modus verfolgen.

**Schutz vor unberechtigtem Zugriff**

Das EarlyWatch-Team nimmt telefonisch Kontakt mit Ihnen auf, wenn die Verbindung zum EarlyWatch Servicezentrum aufgebaut werden soll. Des weiteren werden Sie telefonisch über den Abschluß der EarlyWatch-Session benachrichtigt, damit Sie die Verbindung beenden können. Sie allein entscheiden über die Verbindung und können diese jederzeit unterbrechen.

**Aufbau einer Verbindung für die EarlyWatch-Session**

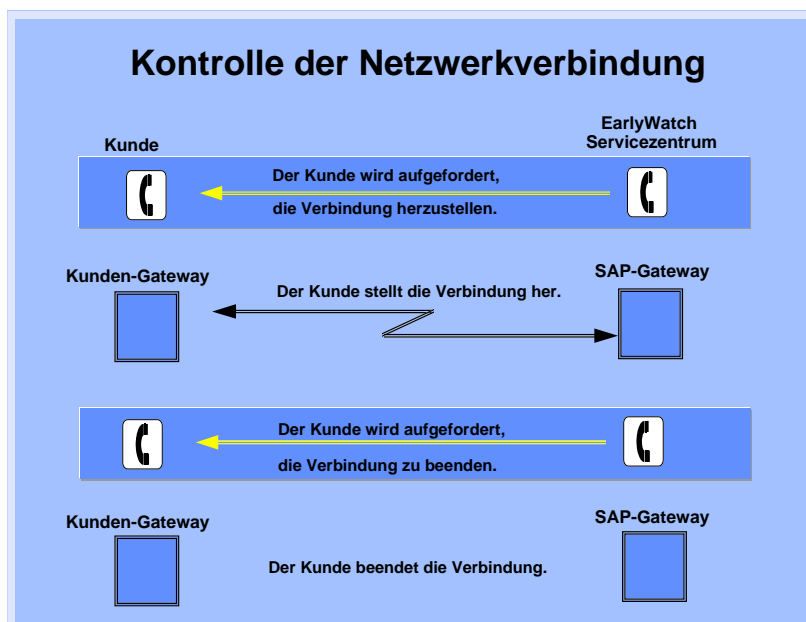


Abb. 3-1: Aufbau und Beendigung der Verbindung für die EarlyWatch-Session

### EarlyWatch-Benutzererkennung und Mandant 066

Grundsätzlich wird der Zugriff auf das System über die EarlyWatch-Benutzererkennung und das zugehörige Paßwort kontrolliert, die in jedem R/3-System angelegt sind. SAP empfiehlt, nach der Session das Paßwort zu ändern, wodurch der Benutzer gelöscht wird.

Die EarlyWatch-Session wird immer mit der Benutzererkennung „Early-Watch“ und dem Mandanten 066 durchgeführt. Mandant 066 ist so eingerichtet, daß der Benutzer „earlywatch“ keinen Zugriff auf Firmendaten hat. Nur die zur Systemanalyse erforderlichen Tools können mit dieser Kennung aufgerufen werden.

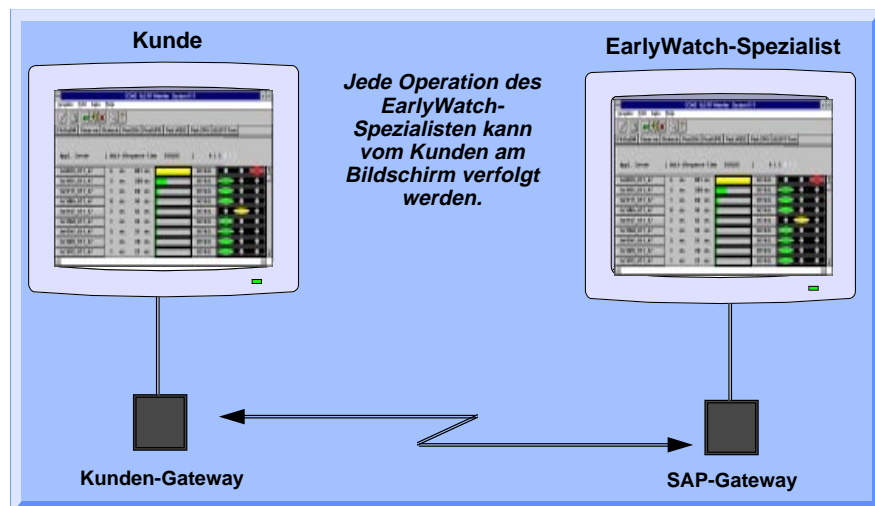
Sie können die Berechtigungen des Benutzers „earlywatch“ jederzeit überprüfen. Sie kontrollieren die EarlyWatch-Benutzererkennung, den Mandanten 066 und das Paßwort und können den Zugang für diese Kennung jederzeit sperren oder freigeben.

### Der SAP-Echo-Modus

Über den SAP-Echo-Modus können Sie sich in die EarlyWatch-Session einschalten und auf Ihrem Bildschirm die Analysen verfolgen, die der Early-Watch-Spezialist durchführt.

Während einer EarlyWatch-Session kann der SAP-EarlyWatch-Spezialist den Echo-Modus aktivieren.

Ab Release 3.0 wird der SAP-Echo-Modus für alle Plattformen verfügbar sein.



**Abb. 3-2: Kontrolle des EarlyWatch-Spezialisten im Echo-Modus**

Sobald der Echo-Modus aktiviert wird, öffnet sich auf Ihrem Bildschirm ein weiteres R/3-Fenster, in dem der Bildschirm des EarlyWatch-Spezialisten angezeigt wird. Damit können Sie alle Aktionen und Bildschirmanzeigen des EarlyWatch-Spezialisten verfolgen.

### Der SAProuter

Der SAProuter ist ein SAP-Programm, das als Zwischenglied in einer Netzwerkverbindung zwischen R/3-Systemen dient. Mit dem SAProuter haben Sie die vollständige Kontrolle über die Zugriffsmöglichkeiten auf Ihr R/3-System.

Über den SAProuter können Sie von einem bestimmten Punkt in Ihrem Netzwerk aus auf einen bestimmten Server zugreifen. Der Zugriff kann durch Übertragungstabellen (Route Transmission Tables) und SAP-Paßwörter geregelt werden. Verbindungen können nur hergestellt werden, wenn die betreffenden IP-Adressen in den Tabellen aufgeführt sind. Auf diese Weise kann der Systemverwalter den unberechtigten Zugriff auf vertrauliche Daten oder Systeme mit eingeschränktem Zugriff noch zusätzlich verhindern.

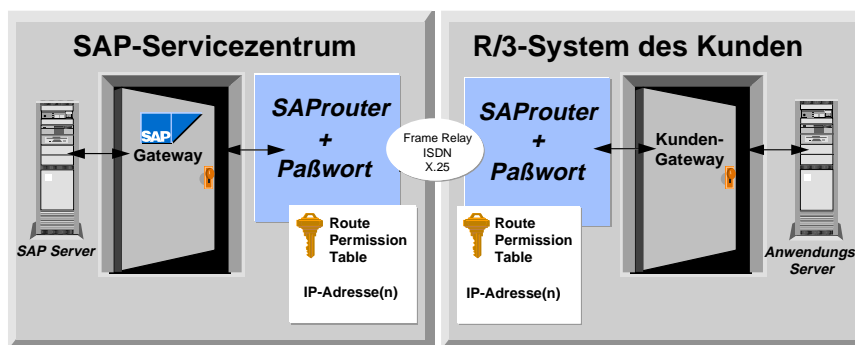


Abb. 3-3: Datenschutz mit der SAProuter-Software

Bei einer Verbindung zwischen Ihrem Netzwerk und dem SAP-Servicenetz kennt der SAProuter nur die IP-Adresse Ihres Computers. In der Gegenrichtung kennt Ihr Netzwerk nur die IP-Adresse des SAP-Systems mit dem SAProuter. So ist sichergestellt, daß kein unberechtigter Zugriff von einem Netzwerk auf das andere möglich ist.

Wenn Ihr Netzwerk über einen Hardware-Router an das SAP-Servicenetz angeschlossen ist, besteht darüber hinaus meist auch die Möglichkeit, über Zugriffslisten (Access Lists) den Zugang auf bestimmte Anwendungen zu beschränken. Diese Beschränkung existiert zusätzlich zum oben beschriebenen SAProuter und ist auch nicht bei allen Hardware-Routern möglich.

Wie wird Ihr System vor unberechtigtem Zugriff geschützt?

- Die Netzwerkverbindung unterliegt immer Ihrer Kontrolle. Sie bauen die Verbindung auf und wieder ab.
- Ihre Daten sind für den EarlyWatch-Spezialisten nicht zugänglich, da er mit der EarlyWatch-Benutzerkennung und dem zugehörigen Paßwort nur auf die Datenbank mit den Leistungsdaten und die Überprüfungstools zugreifen kann.
- Sie können über den Echo-Modus die Aktionen des SAP-Spezialisten verfolgen.

# 3

## Informationen zum Datenschutz

- Über Router-Software wie den SAprouter kann der Zugriff auf Ihr Netzwerk weiter eingeschränkt werden.