CeBIT 2003

»|secaron

Sicherheit in SAP R/3 Systemen
Chancen und Risiken

Dr. Klaus H. Schmidt, secaron AG
schmidt@secaron.com

- **Ausgangssituation**
- **Risiken**
- **Sicherheitsservices im R/3 Umfeld**
- **Beispiele**
- **Chancen zur Kosteneinsparung**
- **Vorgehensweise**
- **Fazit**

Der Geschäftszweck

»|secaron

Die secaron AG steht Ihnen als kompetenter Partner in allen Fragen der IT-Sicherheit zur Verfügung:

- *IT-Sicherheitsmanagement und IT-Risikomanagement*
- *IT-Sicherheitskonzepte und IT-Sicherheitslösungen*
- *IT-Sicherheitsaudits und -Zertifizierungen*

Ausgangssituation: Marktanforderungen

»|secaron

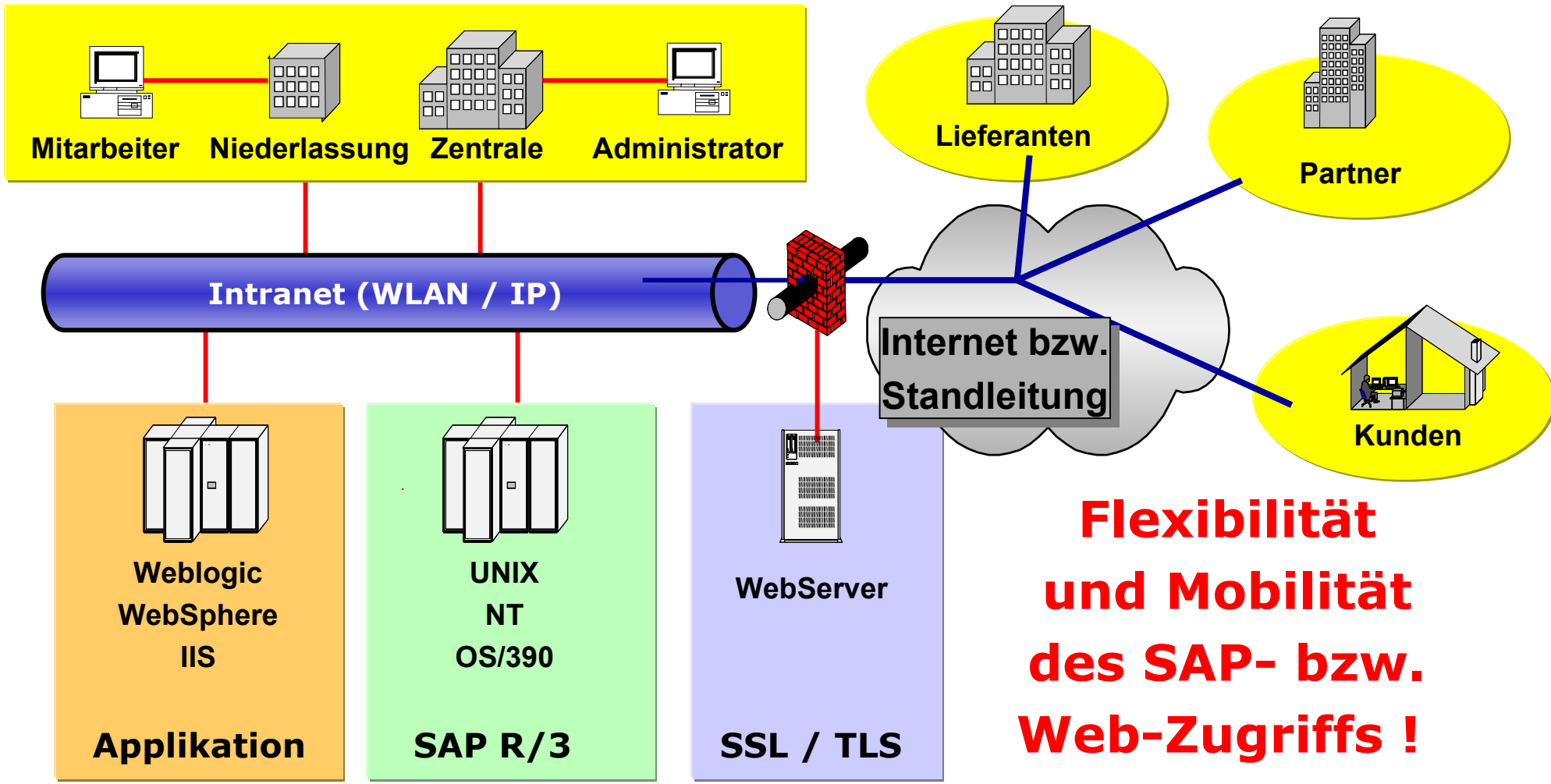
„Collaborative Business" stellt neue Anforderungen:

- Zugriff auf die Systeme durch Kunden, Partner, Lieferanten und Mitarbeiter
- Online-Zugriffe für „Just-in-Time" Geschäftsabwicklung
- Kooperationen auf virtuellen Markplätzen
- Kommunikation mit Behörden über elektronischen Bürgerservice

Grundlage dafür sind:

- Einhaltung der gesetzlichen Rahmenbedingungen (z.B. Datenschutz)
- Solide Vertrauensbasis
- Zuverlässige Authentifizierungsverfahren
- Benutzerfreundliche und sichere Single-Sign-On Mechanismen (erhöhtes Risiko durch Kumulationseffekt !)
- Digitale Signaturen zum Beweis der Authentizität und Integrität der Daten

Ausgangssituation: Systemarchitektur



Flexibilität und Mobilität des SAP- bzw. Web-Zugriffs !

Ausgangssituation:
Kritische Schwachstellen in SAP R/3 Landschaften

»|secaron

- **Fachliche Module (z.B. HR):**
  Höchste Schutzbedarfsklasse aufgrund gesetzlicher Vorschriften
- **Absicherung Plattform: Betriebssystem und Datenbank**
- **Absicherung Web-Schnittstellen: ITS, WAS, WebServer**
- **Eigenentwicklungen: Berechtigungsabfragen**
- **Fernwartungszugänge**
- **Transport von (kritischen) Berechtigungen ins Produktivsystem**

Ausgangssituation: Wirtschaftliche Rahmenbedingungen

»|secaron

Kundenservice und Kosteneinsparung stehen im Vordergrund

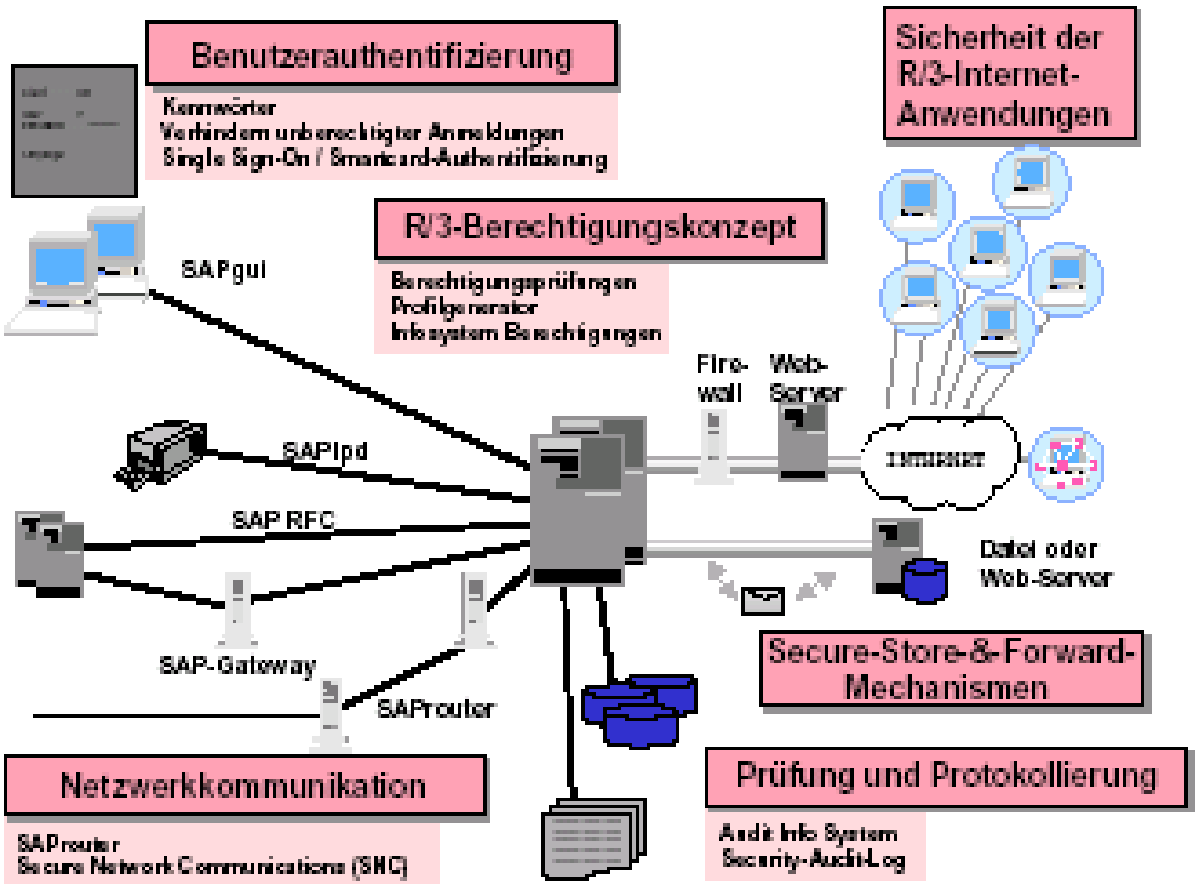
Heterogene IT-Landschaften herrschen vor

Die Folgen aufgrund steigender Komplexität sind oft katastrophal:

- Massiv steigende Betriebskosten der IT
- Wenig kostengünstige Möglichkeiten zur Korrektur
- Erhöhtes Sicherheitsrisiko: Beispiel HR-Daten !

Aber: SAP bietet als zentrales ERP-System ein erhebliches Potenzial für Synergieeffekte !

SAP R/3 Sicherheitsservices



Quelle: SAP Sicherheitsleitfaden

SAP R/3 Sicherheitsservices

»|secaron

- **Benutzerauthentifizierung:**
  Kennwörter, Single-Sign-ON, starke Authentifizierung

- **Berechtigungskonzept:**
  Berechtigungsmodell, Profilgenerator, Infosystem Berechtigungen

- **Netzwerkkommunikation**
  SAP Router, Secure Network Communications (SNC), SSL/TLS

- **Secure-Store&Forward Mechanismen (SSF)**
  für Verschlüsselung und digitale Signatur

- **Prüfung und Protokollierung:**
  Audit Info System (AIS), Security-Audit-Log

Ergänzende Sicherungsmechanismen

»|secaron

- **Remote Access (RAS) Virtual Private Network (VPN),**
  z.B. mit IPSec: Fernwartung, Anbindung Töchter/Niederlassungen

- **Firewalls:**
  in Verbindung mit SAP-Router

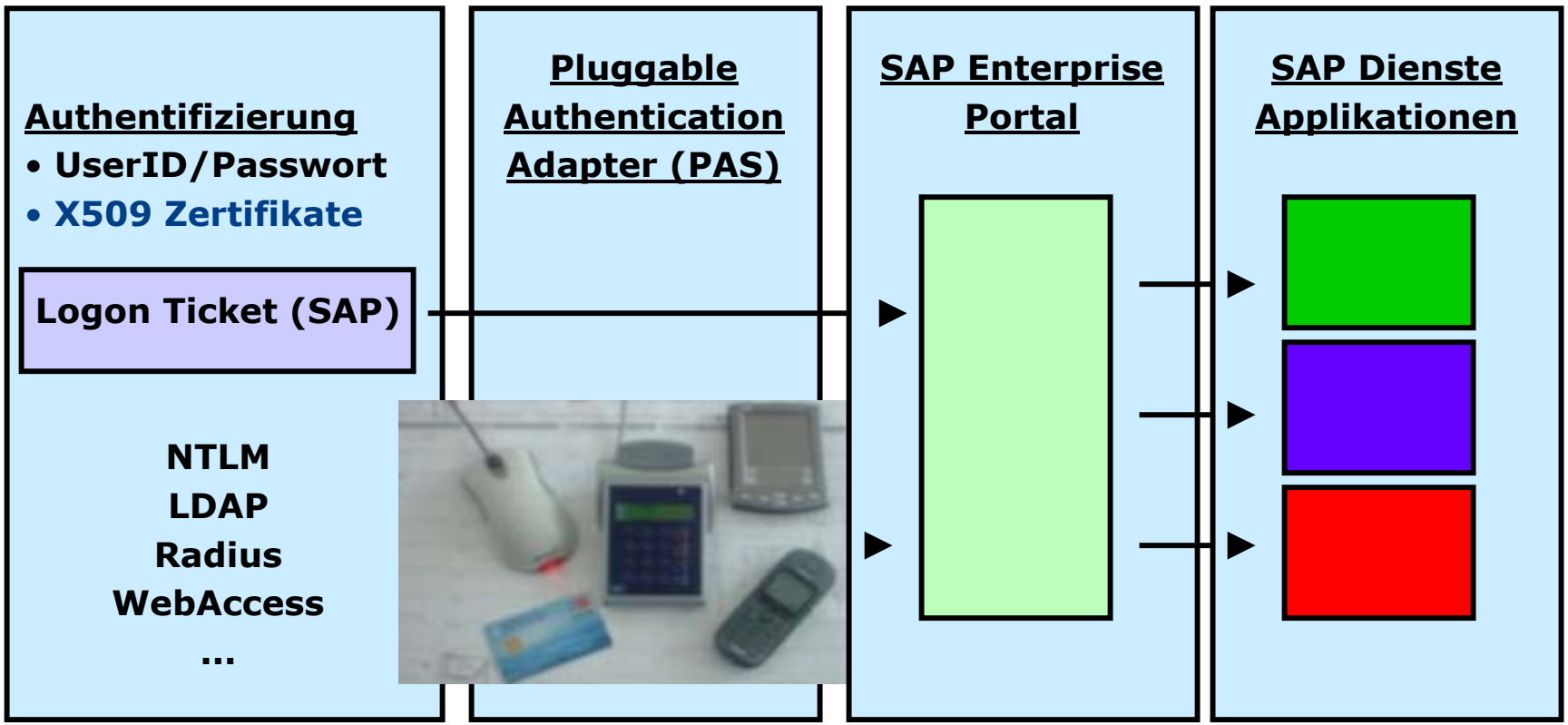
- **Plattformsicherheit:**
  Gehärtete Betriebssysteme und Datenbanken

- **WebServer Sicherheit:**
  Internet Transaction Server (ITS), Web Application Server (WAS)

- **Prozesse und Tools zur Überprüfung kritischer Berechtigungen**

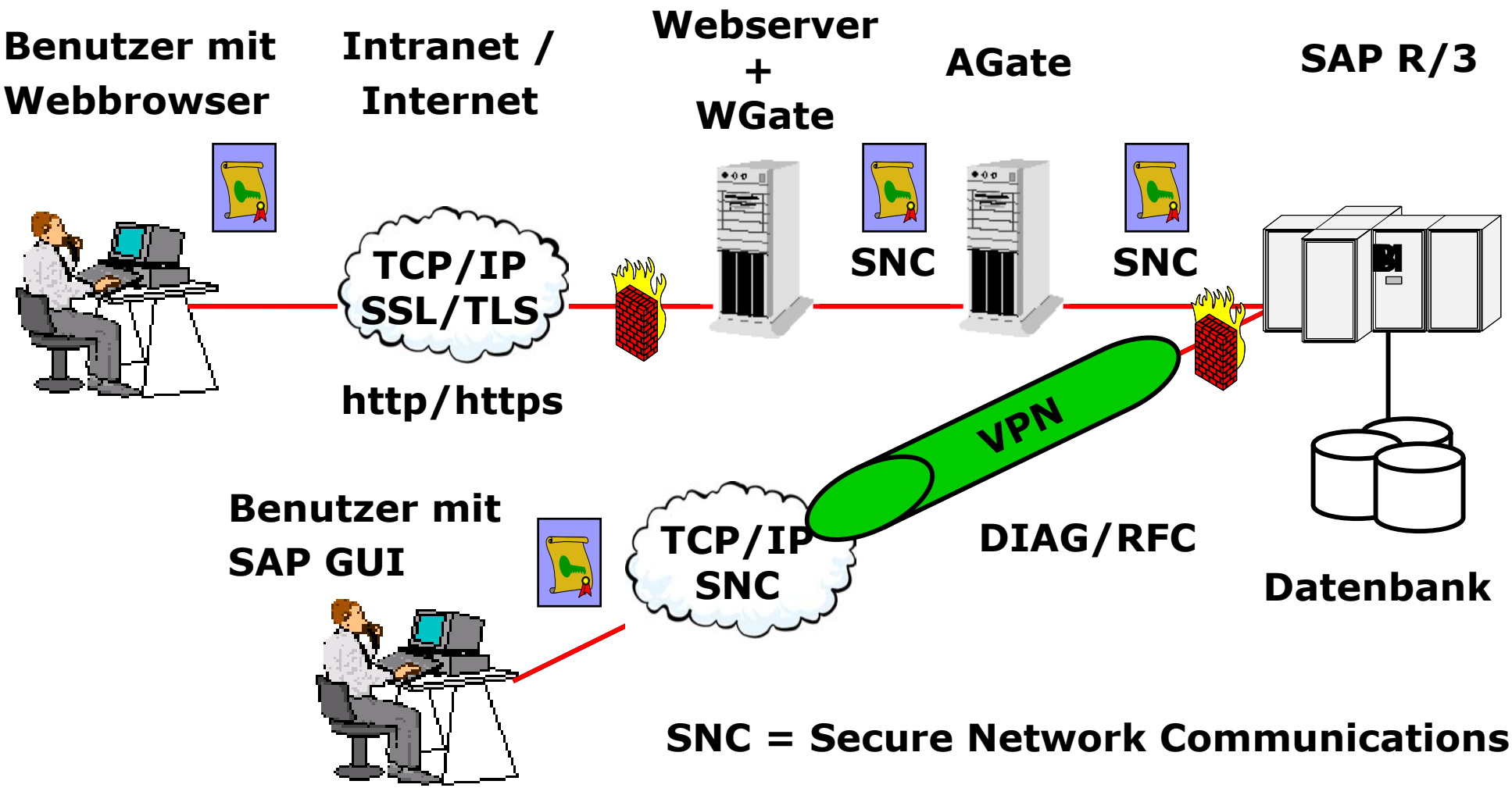
Beispiel 1: Authentifizierung

»|secaron



1. Nach der Authentifizierung wird ein SAP-Logon Ticket für ausgestellt
2. Externe (Non-SAP) Nutzung möglich: Single-Sign-On (SSO).

Beispiel 2: Systemabsicherung mit SNC

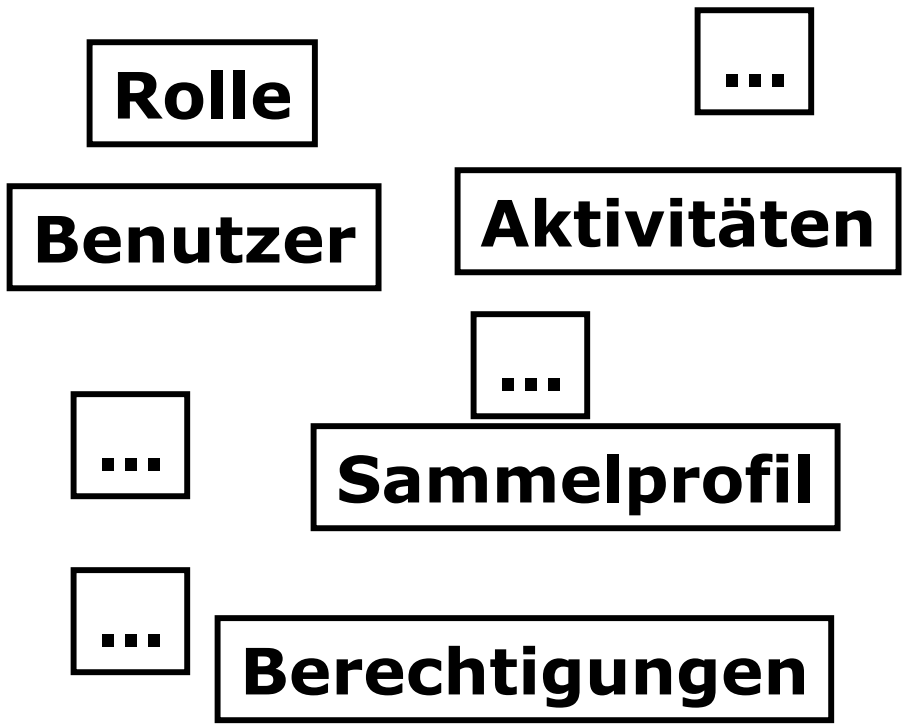


Beispiel 3: Überprüfung kritischer Berechtigungen I

»|secaron

Komplexes Berechtigungsmodell:

Welche Berechtigungen hat nun ein Benutzer wirklich?

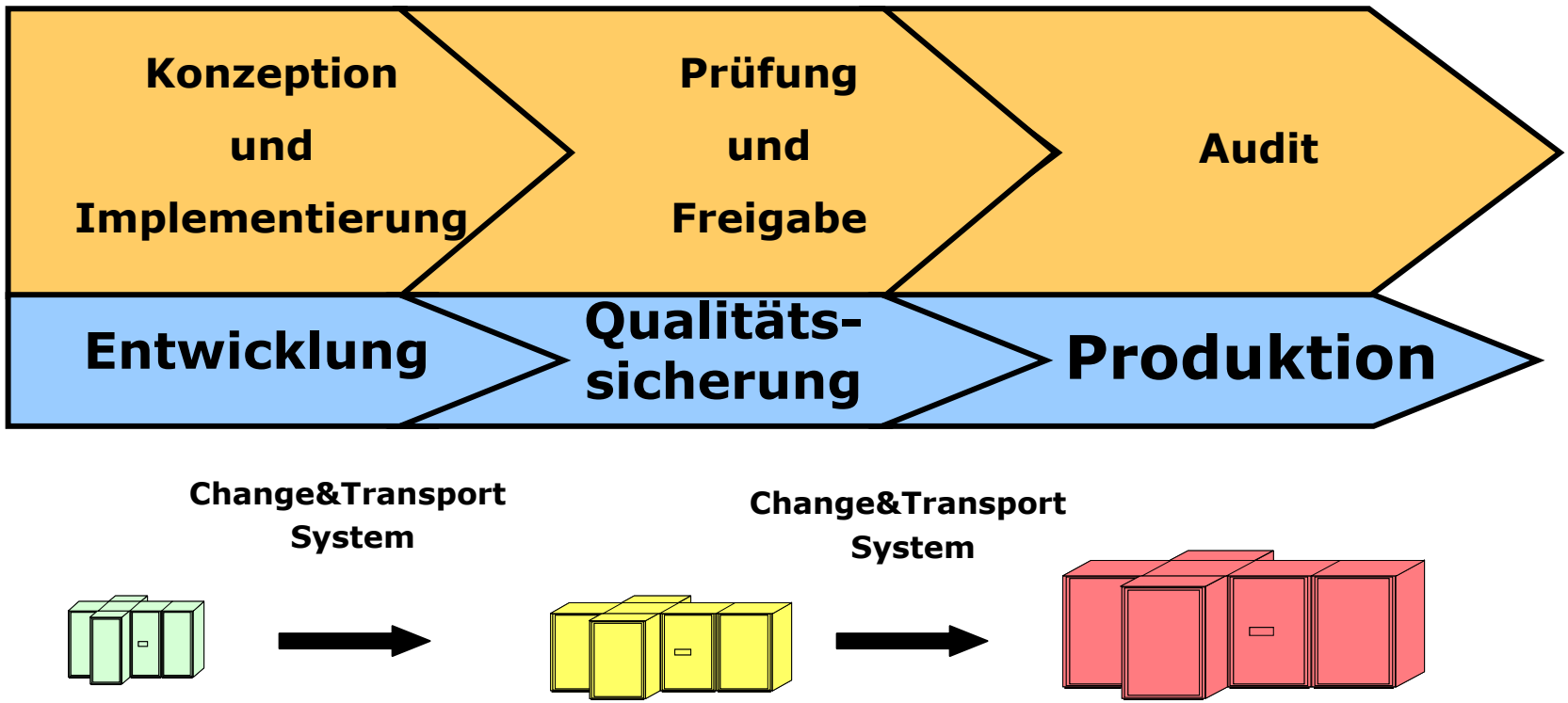


Kontroll und Funktions-trennungsprinzip:

Hat ein Benutzer kritische Rechte?

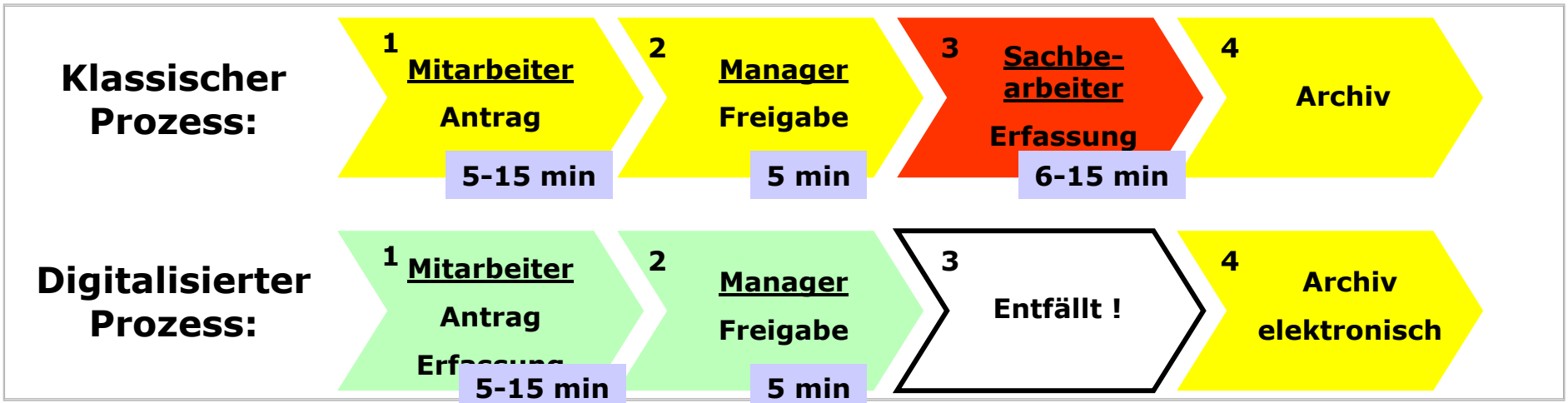
	Fachbe-nutzer 1	Fachbe-nutzer 2	Revisor
Fachbe-nutzer 1		X	X
Fachbe-nutzer 2	X		X
Revisor	X	X	X

Beispiel 3: Überprüfung kritischer Berechtigungen II



Chancen: Kosteneinsparung im Employee Self Service

»|secaron



Beispielprozesse (mit hoher Stückzahl):

- Arbeitszeitänderung, insbesondere Nachmeldung
- Urlaubsantrag
- Reiseabrechnung

Prozessoptimierung:

- Direkte, elektronische Erfassung (Mitarbeiter)
- Freigabe durch digitale Signatur (Mitarbeiter und Manager)

Chancen Kosteneinsparung im Employee Self Service

»|secaron

Nutzenrechnung (konservative Betrachtung):

Zeitersparnis: 6-15 Minuten / Vorfall
Tagessatz: 800 €
Kos

Anz
Ko

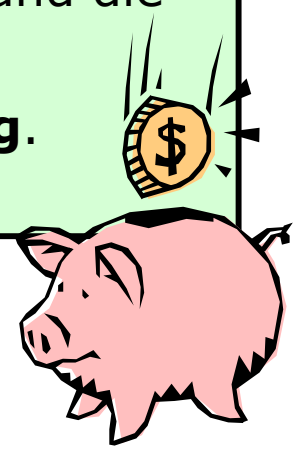
Ers

Zusätzlicher Nutzen:

Die **Sicherheitstechnik** ist gleichzeitig

Voraussetzung und **Werkzeug** für neues Prozessdesign und die

damit verbundene Möglichkeit zur **Kosteneinsparung**.



Beschleunigung und hohe Verfügbarkeit der Prozesse
Fehlerbereinigung (weitere Einsparungsmöglichkeit)
Erfüllung von Datenschutzanforderungen (HR/Personalprozesse !)

Vorgehensweise im Projekt

»|secaron

1. **Durchführung Schutzbedarfsanalyse**

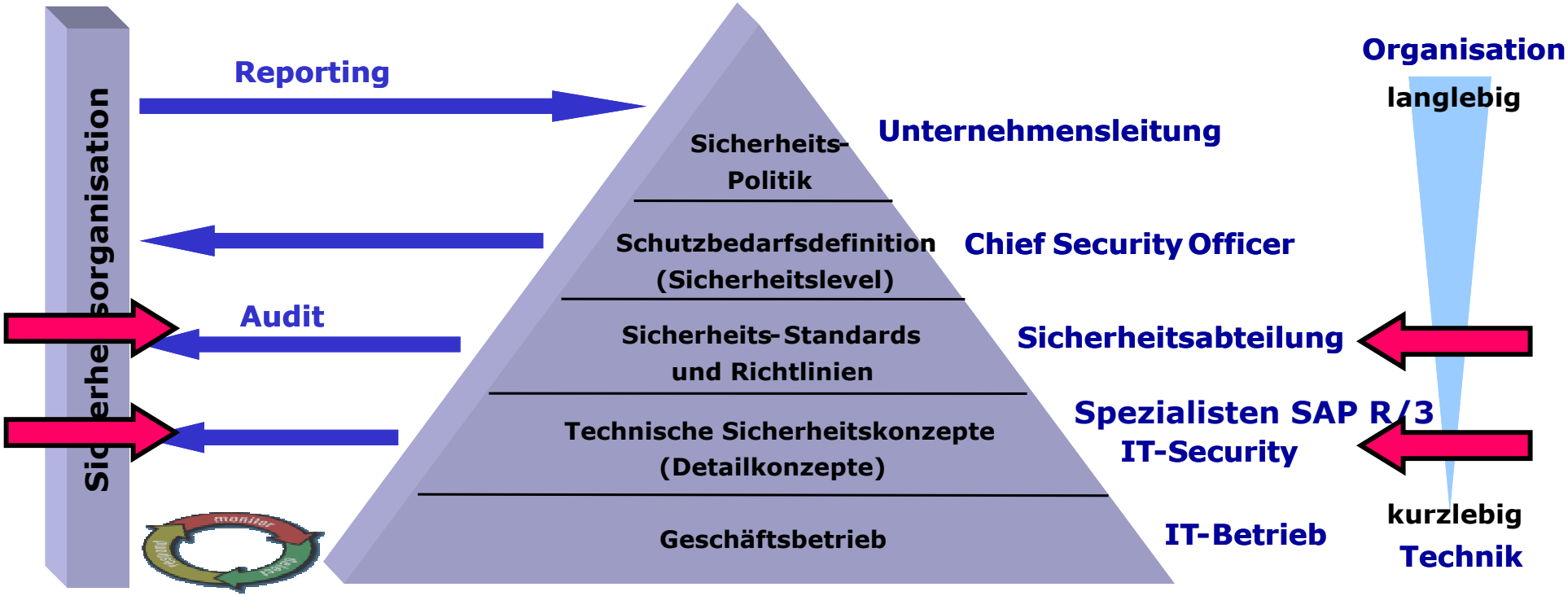
2. **Erstellung Sicherheitsrichtlinien und –konzepten**

3. **Implementierung der SAP R/3 Sicherheitsservices und Integration herkömmlicher IT-Sicherheitsmaßnahmen**

4. **Durchführung von Audits und Penetrationen der technischen und organisatorischen Sicherheitsmaßnahmen**

Vertrauen auch Sie auf unsere Erfahrung, unser Know-how und unsere effiziente und kundenorientierte Projektabwicklung!

Ziel: Einbindung von SAP R/3 ins unternehmensweite IT-Sicherheitsmanagement

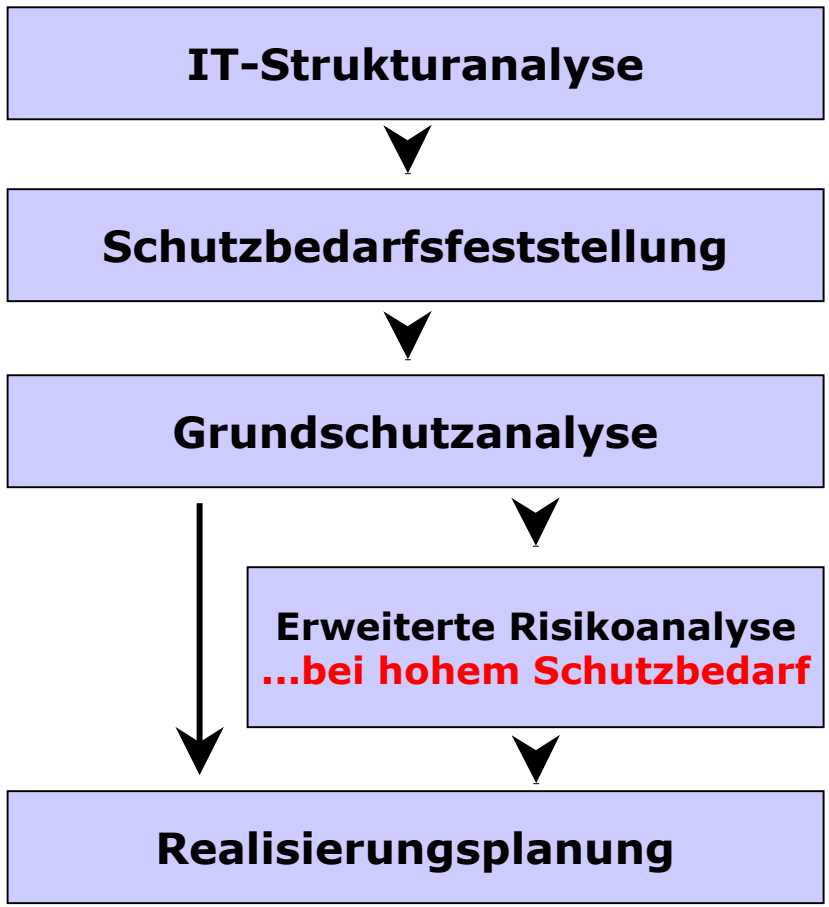


Vorgehensweise zu sicheren (SAP R/3) Systemen

»|secaron

Erstellung des IT-Sicherheitskonzepts

BSI Bundesamt für Sicherheit in der Informationstechnik



- Erfassung aller IT-Systeme
- Bildung logischer Gruppen

Einordnung in Schutzklassen
("niedrig", ..., "sehr hoch")

- Qualitatives Vorgehen
- Zuordnung IT-System – Schutzmaßnahme
- Ausreichend für den mittleren Schutzbedarf

- Quantitatives Vorgehen
- Festlegung erweiterter Schutzmaßnahmen
- Für Daten, Anwendungen & Systeme mit hohem Schutzbedarf

- Wirtschaftliche Bewertung
- Konsolidierung / Priorisierung

Fazit

- **Gehen Sie IT-Risiken bewusst an: 100% Sicherheit gibt es nicht**
- **IT-Sicherheit ist Chefsache:**
  Die Geschäftsleitung trägt die Gesamtverantwortung
- **Delegieren Sie Verantwortung:**
  IT-Sicherheit erfordert viele Köpfe und Hände
- **Klassifizieren Sie IT-Anwendungen, IT-Systeme und Daten**
  IST-Analyse und Schutzbedarfsfeststellung als ersten Schritt
- **Verschaffen Sie sich einen Überblick über den Status Quo**
  Modellierung und SOLL-IST Analyse als konsequente Fortsetzung
- **Überprüfen Sie den laufenden Betrieb**
  Modellierung nach IT-Grundschutzhandbuch liefert Checkliste
- **Bestimmen Sie Ihr individuelles Restrisiko**
  Schließen Sie den Sicherheitskreis durch ein umfassendes und schlagkräftiges Sicherheits-Management

Fazit

»|secaron

Setzen Sie Ihren Fokus auf Ihr SAP R/3 System !

SAP R/3 ist

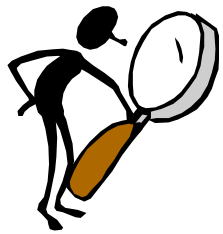
- **„Security-Enabled“: d.h. Sicherheit modular implementierbar**
- **„Ready-for-Business“: d.h. Geschäftsprozesse vorhanden**

Hohes Kosteneinsparungspotential z.B. durch Einsatz

der digitalen Signatur vorhanden: Beispiel liefert die SAP selbst !

Die secaron AG auf der CeBIT 2003

»|secaron



Halle 17 Stand C31-22

Demos und Beispielrechnungen für Kosteneinsparung durch

- ✓ **Content Security**
- ✓ **IPSec Anbindungen.**
- ✓ **Wireless LAN**
- ✓ **Stimmauthentifizierung.**
- ✓ **Windows 2000 + .net Security**
- ✓ **digitale Signatur.**

Dr. Klaus H. Schmidt

secaron AG

www.secaron.com
schmidt@secaron.com

Herzlichen Dank für Ihre Aufmerksamkeit !

Kontakt

»|secaron

secaron AG
Ludwigstrasse 55
85399 Hallbergmoos
Am Flughafen München
Deutschland
Tel.: +49 811 95 94 – 0
Fax.: +49 811 95 94 – 220
info@secaron.com
www.secaron.de

secaron S.A.R.L.
12, route du Vin
L-6794 Grevenmacher

Luxembourg
Tel.: +352 267469 30
Fax.: +352 267469 20
info@secaron.com
www.secaron.lu