Sind Sicherheit und Internet Banking vereinbar?

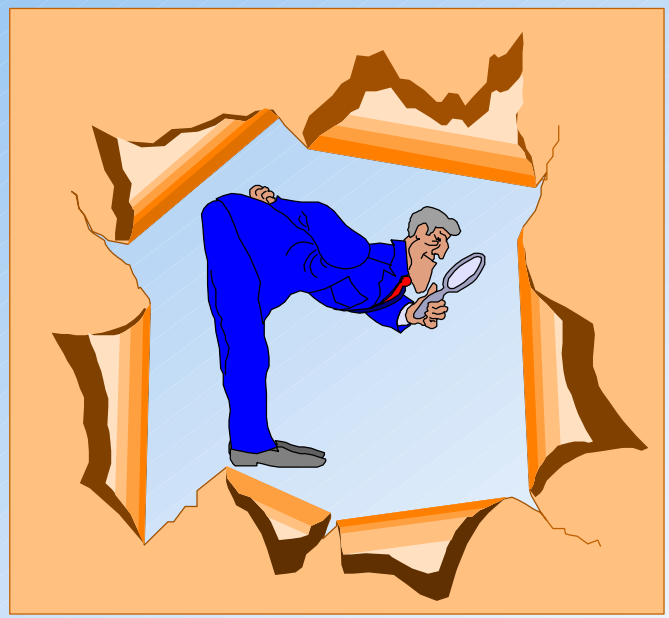
Forum

ecommerce und Vertrauen

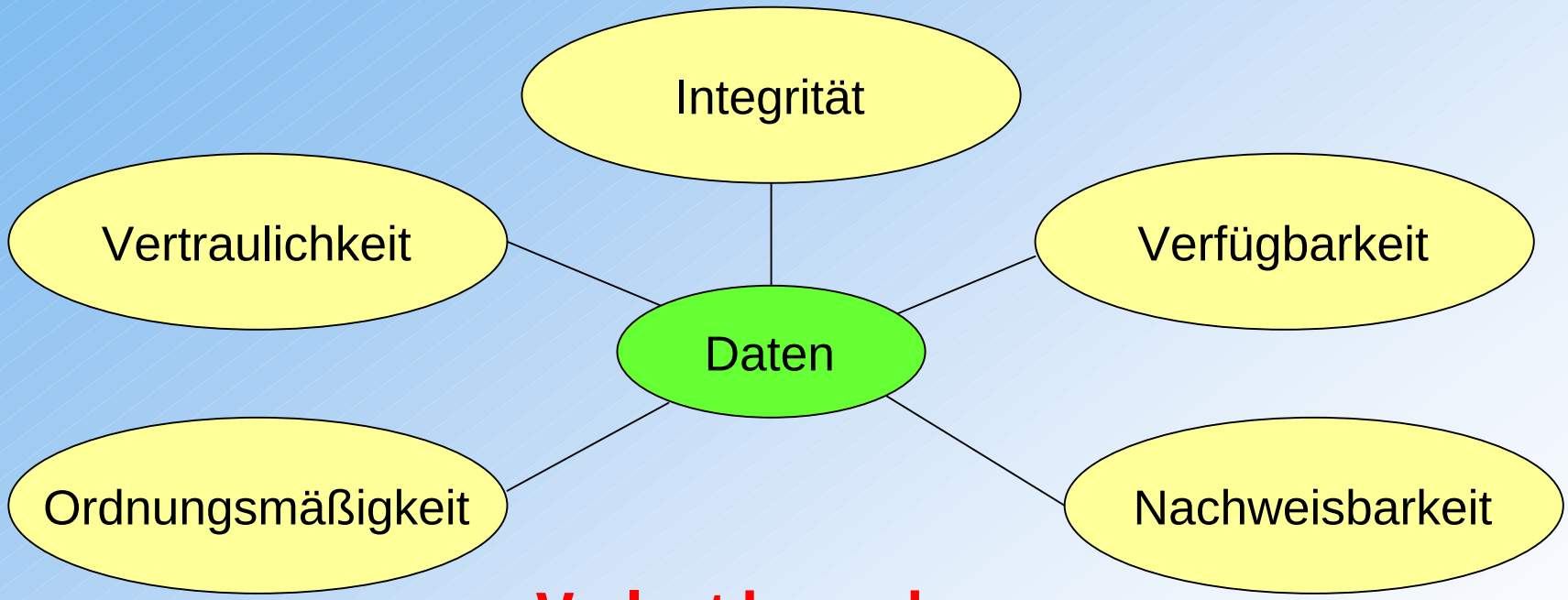
25. September 2002

Manfred Scholz, CISA
Manfred.Scholz@sec4you.com

Internet Banking aus der Sicht eines Prüfers

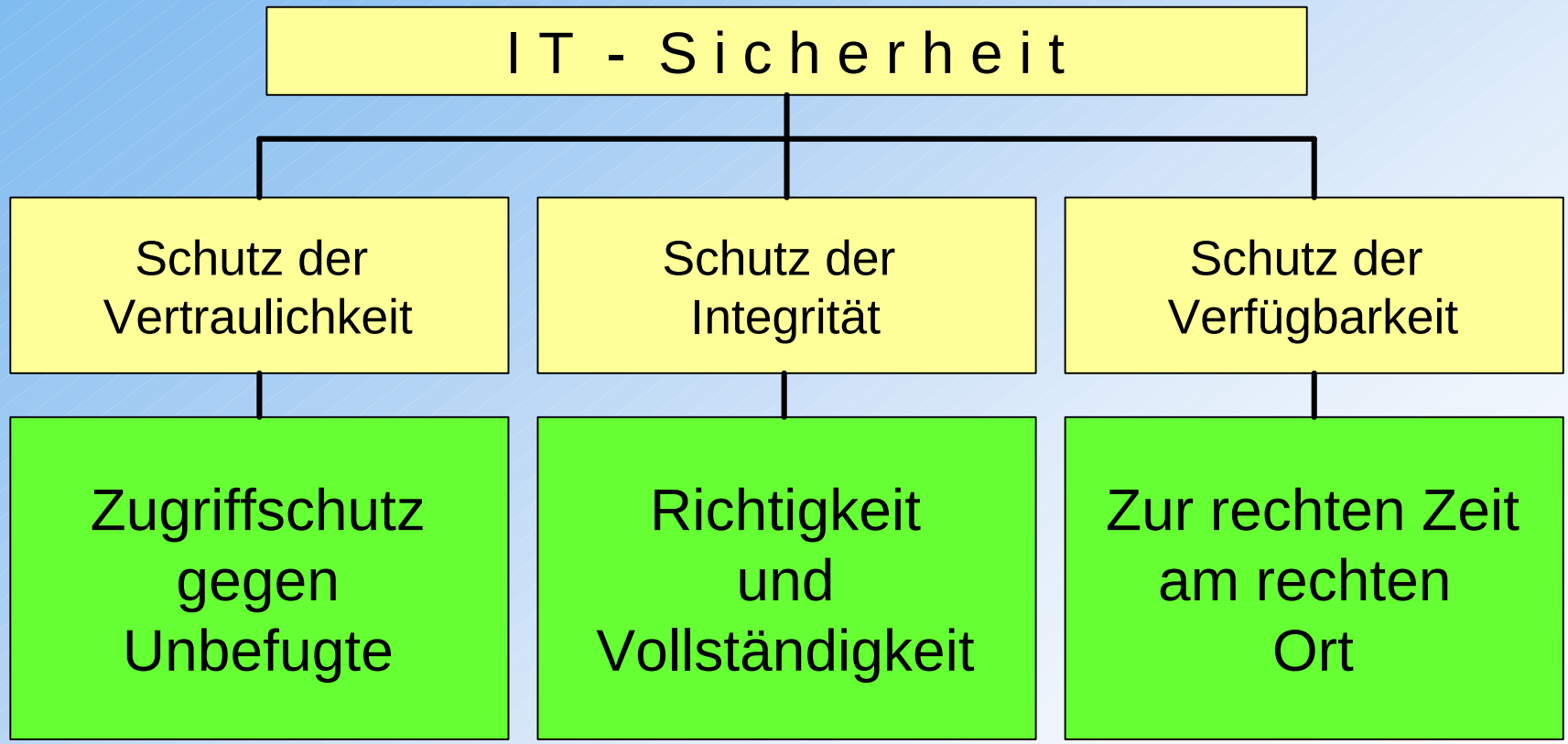


Anforderungen an die Datenverarbeitung

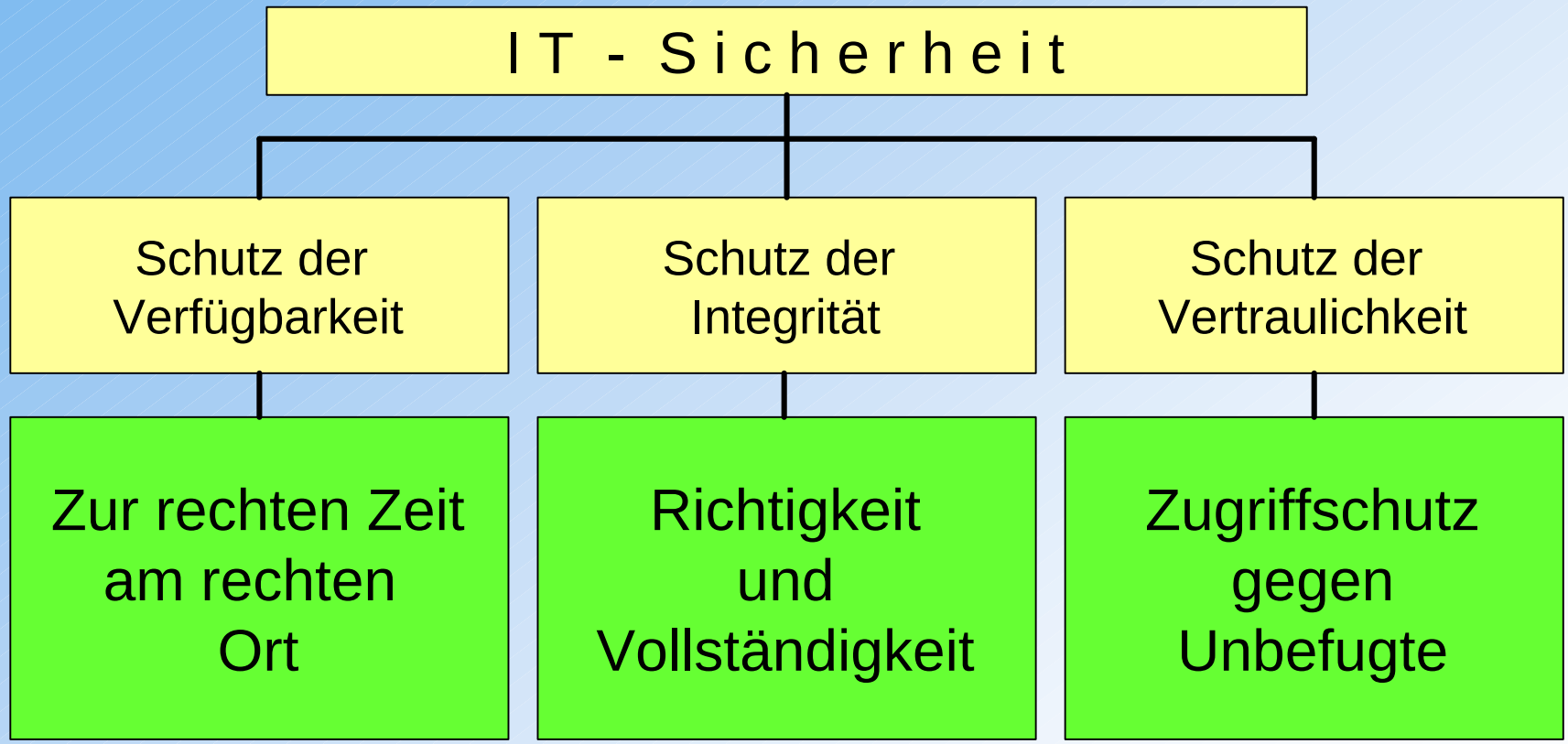


Verlust kann den Fortbestand des Unternehmens gefährden!

Anforderungen aus Sicht der IT-Revision



Anforderungen aus Sicht der IT-Abteilungen



Information Systems Audit and Control Association

ISACA

- Berufsverband der Spezialisten für IT- Revision
- Führend in IT governance, control und assurance
- 1969 gegründet
- weltweit, ca. 22.000 Mitglieder in ca. 100 Ländern
- definiert Standards im IT-Prüfungsbereich
- www.isaca.org
- Zertifizierungen für Auditoren

Information Systems Audit and Control Association

Control Objectives for Information and Related Technology

COBIT

- International anerkannter Standard zur Prüfung von IT-Systemen
- Synthese von 36 nationalen und internationalen Standards
- Definierte Kontrollziele für IT Prozesse
- Steuerung, Messung oder Prüfung von IT-Prozessen
- Daimler/Chrysler, Philips, Steyr Fahrzeugtechnik
- Ausgangsbasis für IT-Prüfungen des Bundes-rechnungshofes

Information Systems Audit and Control Association

Control Objectives for Information and Related Technology

Eingeflossene Standards:

- Technisch: ISO, EDIFACT, uva.
- Geschäftspraktiken: EU, OECD, ISACA, uva.
- Qualifikationskriterien: ITSEC, TCSEC, ISO 9000, CC, SPICE, uva.
- Berufsstandards: COSO, IFAC, AICPA, IIA, GAO, uva.
- Industriepraktiken: ESF 14, IBAG, NIST, DTI, uva.
- Neue industriespez. Anforderungen

Information Systems Audit and Control Association

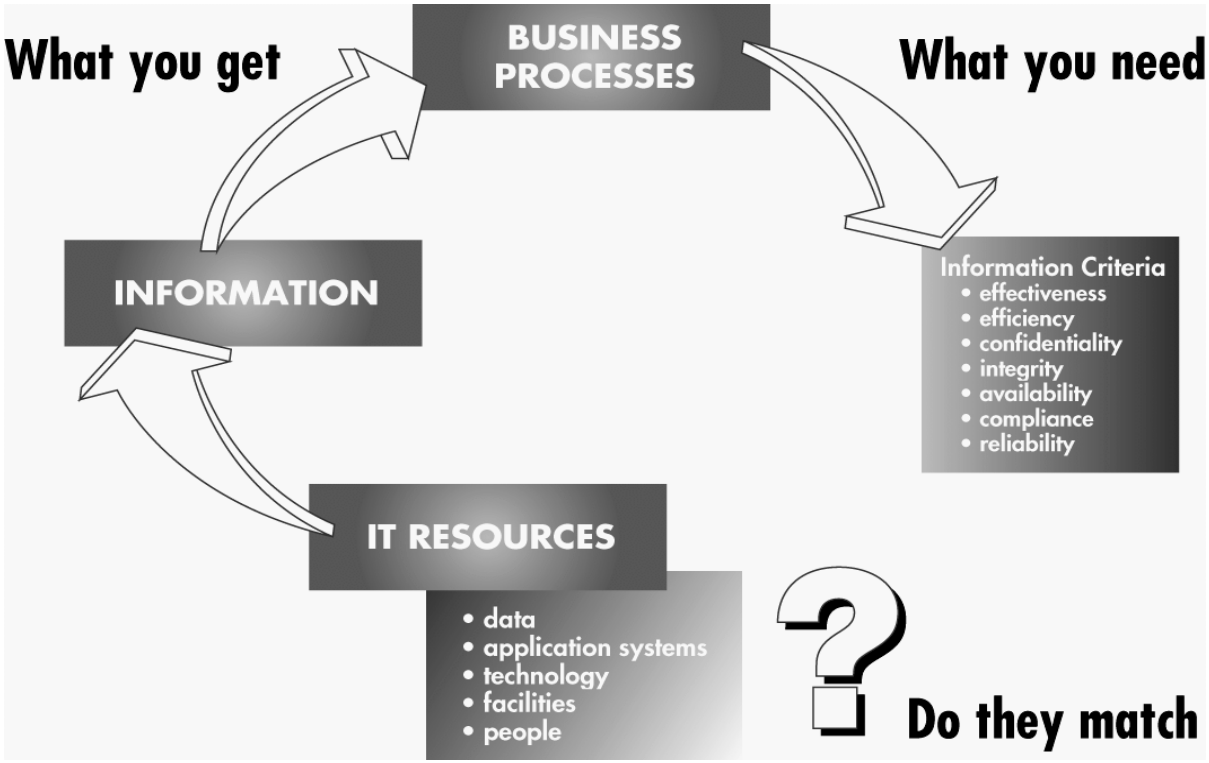
COBIT

Untersuchung der META Group

- In 2003/04 setzen mehr als 30-40% der Global 2000 Unternehmen COBIT ein
- Klare Empfehlung an die CIOs COBIT als Prozess-modell einzusetzen
- Mitarbeiter müssen entsprechend geschult werden

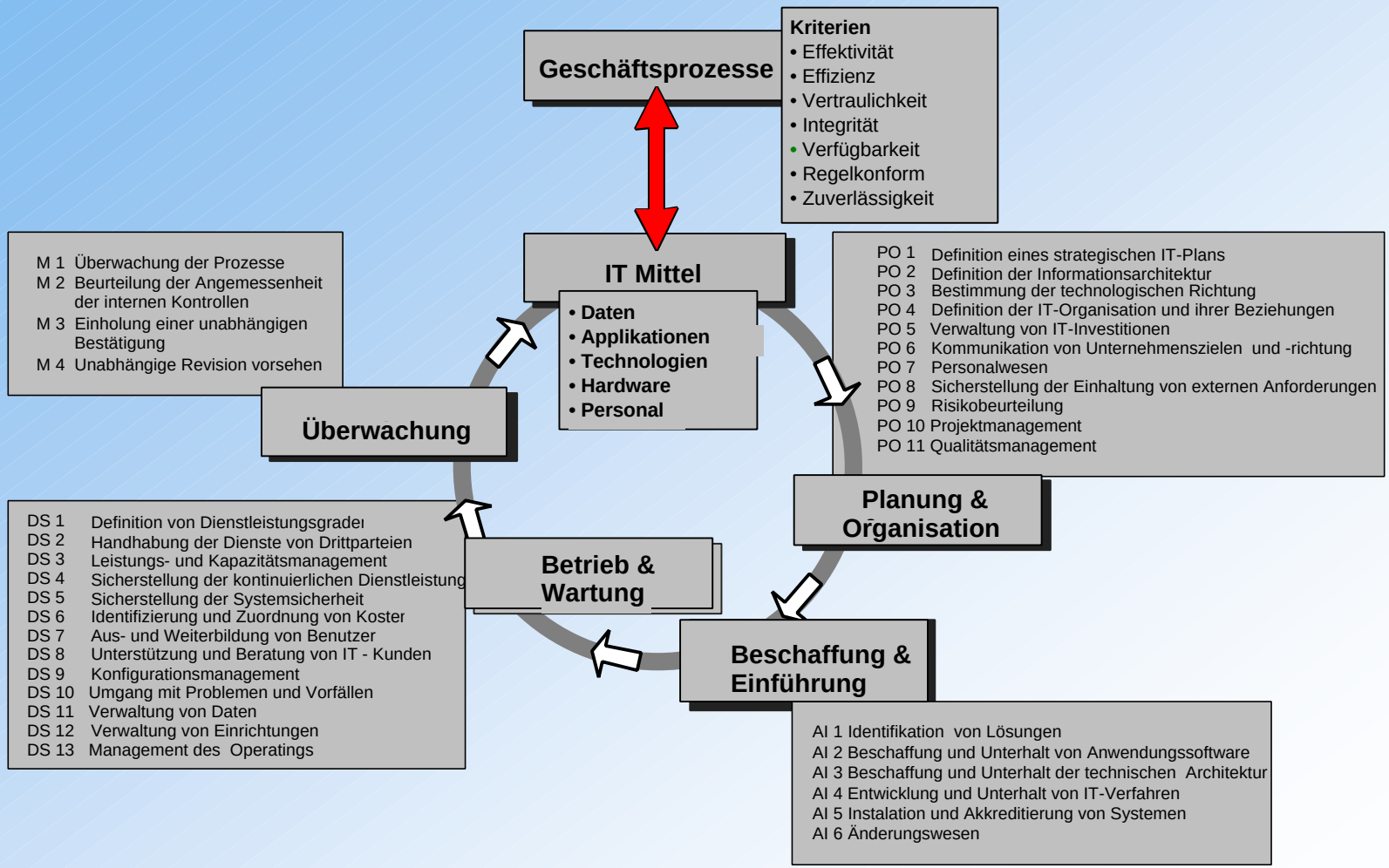
Information Systems Audit and Control Association

COBIT

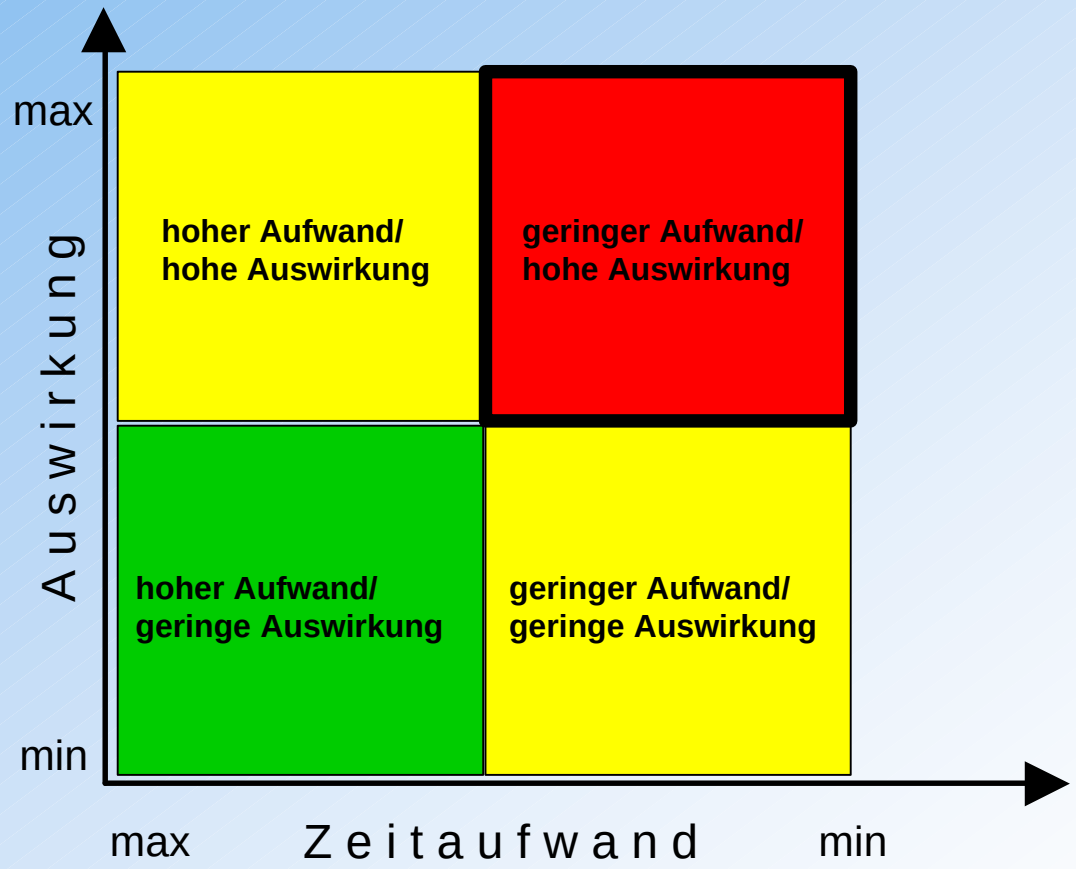


Information Systems Audit and Control Association

COBIT

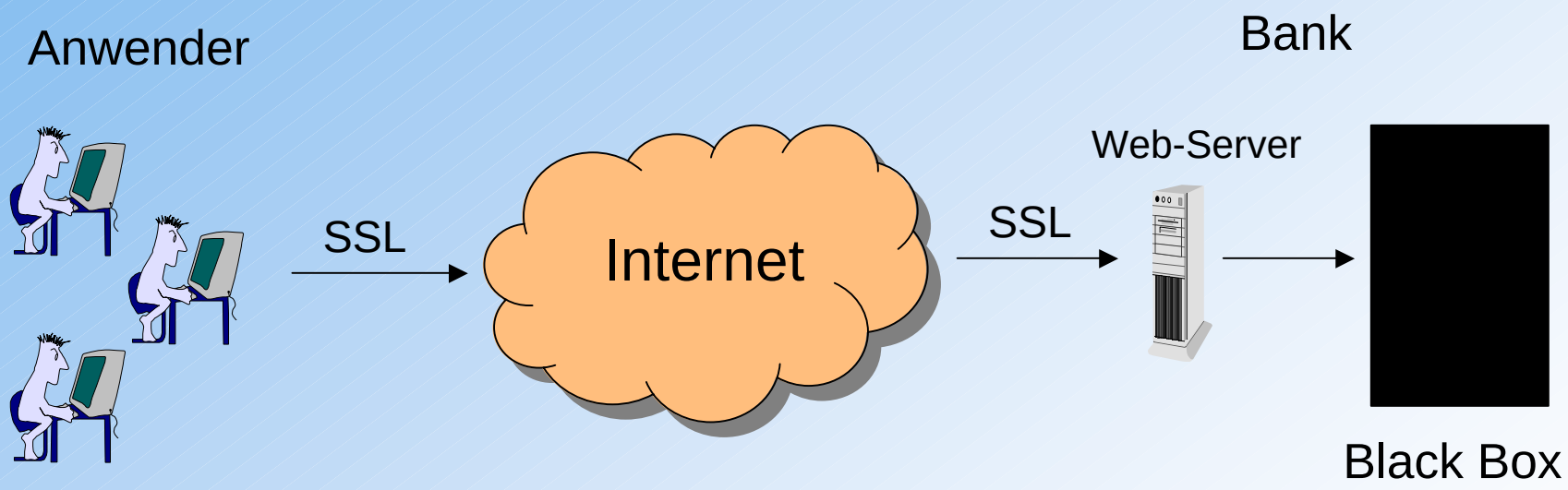


Risikomatrix



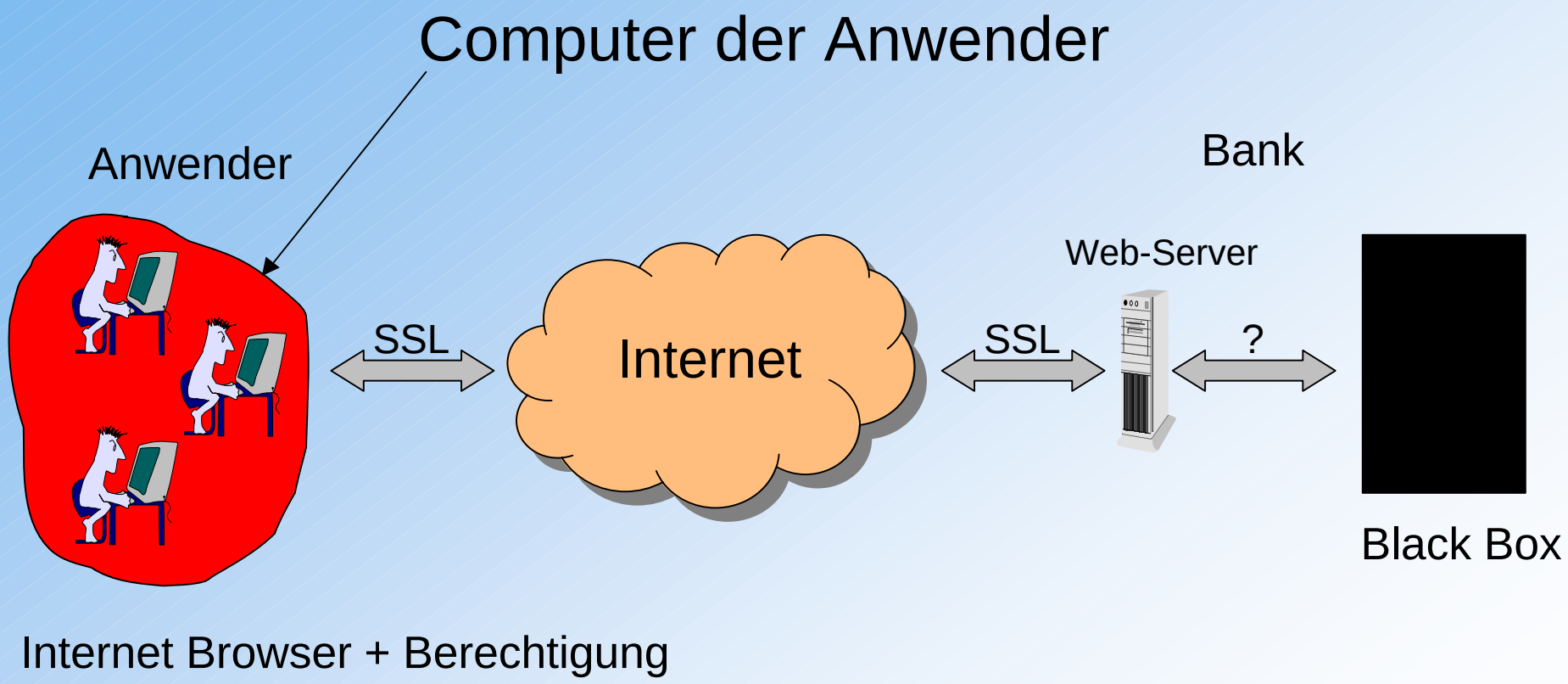
Was ist Internet Banking?

Webapplikation



Internet Browser + Berechtigung

Hauptproblem von Internet Banking



Hauptprobleme von Internet Banking

Potentielle Risikofaktoren

- Hard- und Software der Anwender außerhalb des direkten Einflußbereiches
- Hohe Eigenverantwortung der Anwender erforderlich
- Internet Banking soll überall möglich sein (Unternehmen, Internet-Cafe, usw.)
- Schäden durch Imageverlust meist größer als durch direkten Mißbrauch
- IB darf nicht isoliert betrachtet werden
- Ausrichtung (Anpassung) auf die Geschäftsrisiken notwendig
- uva.

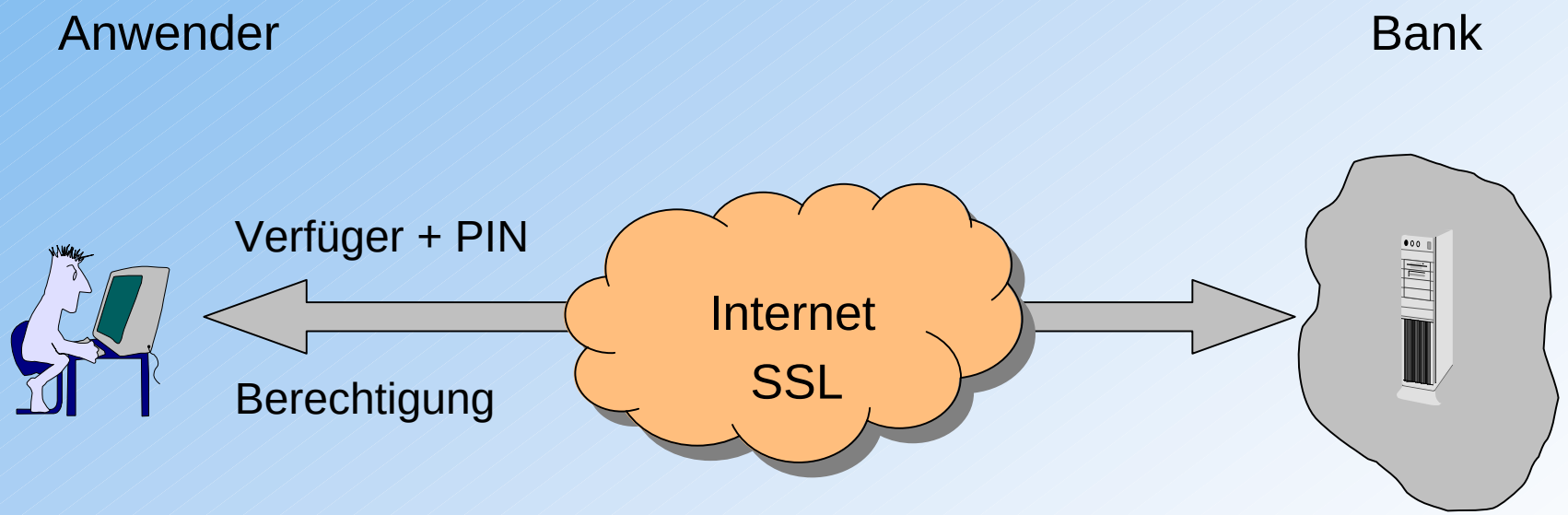
Anwendung von COBIT

DS 5 – Sicherstellen der Systemsicherheit

5.1 Handhabung von Sicherheitsmaßnahmen
5.2 Identifikation, Authentisierung und Zugriff
5.3 Sicherheit des Direktzugriffs auf Daten
5.4 Verwaltung der Benutzerkonten
5.5 Überprüfung der Benutzerkonten durch das Management
5.6 Überprüfung der Benutzerkonten durch die Benutzer
5.7 Sicherheitsüberwachung
5.8 Datenklassifikation
5.9 Zentrale Verwaltung von Identifikation und Zugriffsrechten
5.10 Rapportierung von Verstößen und Sicherheitsaktivitäten
5.11 Umgang mit Zwischenfällen
5.12 Re-Akkreditierung
5.13 Vertrauenswürdigkeit der Gegenpartei
5.14 Genehmigung von Transaktionen
5.15 Nicht-Abstreitbarkeit
5.16 Vertrauenswürdiger Pfad
5.17 Schutz von Sicherheitsfunktionen
5.18 Verwaltung kryptographischer Schlüssel
5.19 Prävention, Aufdeckung und Korrektur bei bösartiger Software
5.20 Firewall-Architekturen und Verbindungen mit öffentlichen Netzwerken
5.21 Schutz von elektronischen Werten

Identifikation, Authentisierung und Zugriff (DS 5.2)

PIN/TAN Verfahren



Identifikation, Authentisierung und Zugriff (DS 5.2)

Sicherheitsmaßnahmen

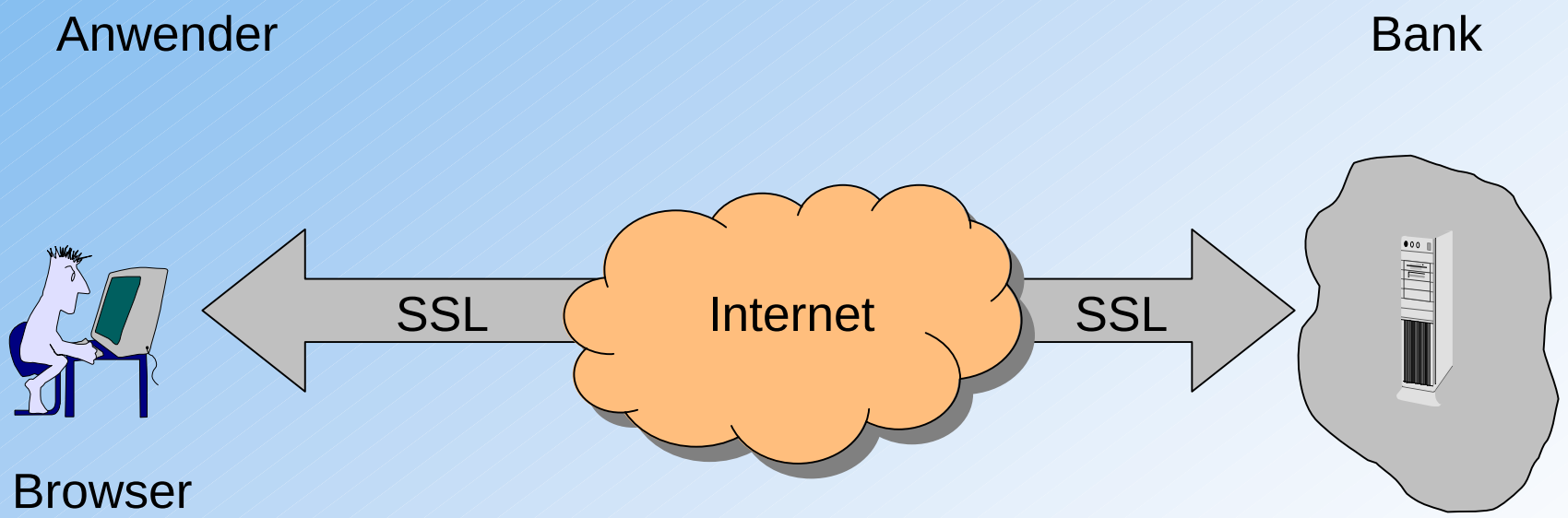
- Mindestlänge der PIN
- Beschaffenheit des Verfügers
- Sperrung des Zugangs nach 3 (?) erfolglosen Anmeldeversuchen
- Regelmäßige Änderung der PIN (Erzwungen !)
- Unterscheidung zwischen Groß- und Kleinschreibung
- Qualitätskontrolle der Beschaffenheit des PIN
- Historie der bereits verwendeten PIN‘s
- Prozess zur Entsperrung von Zugängen
- uva.

ACHTUNG

Sämtliche Maßnahmen helfen nicht gegen
Passwörter schlechter Qualität!

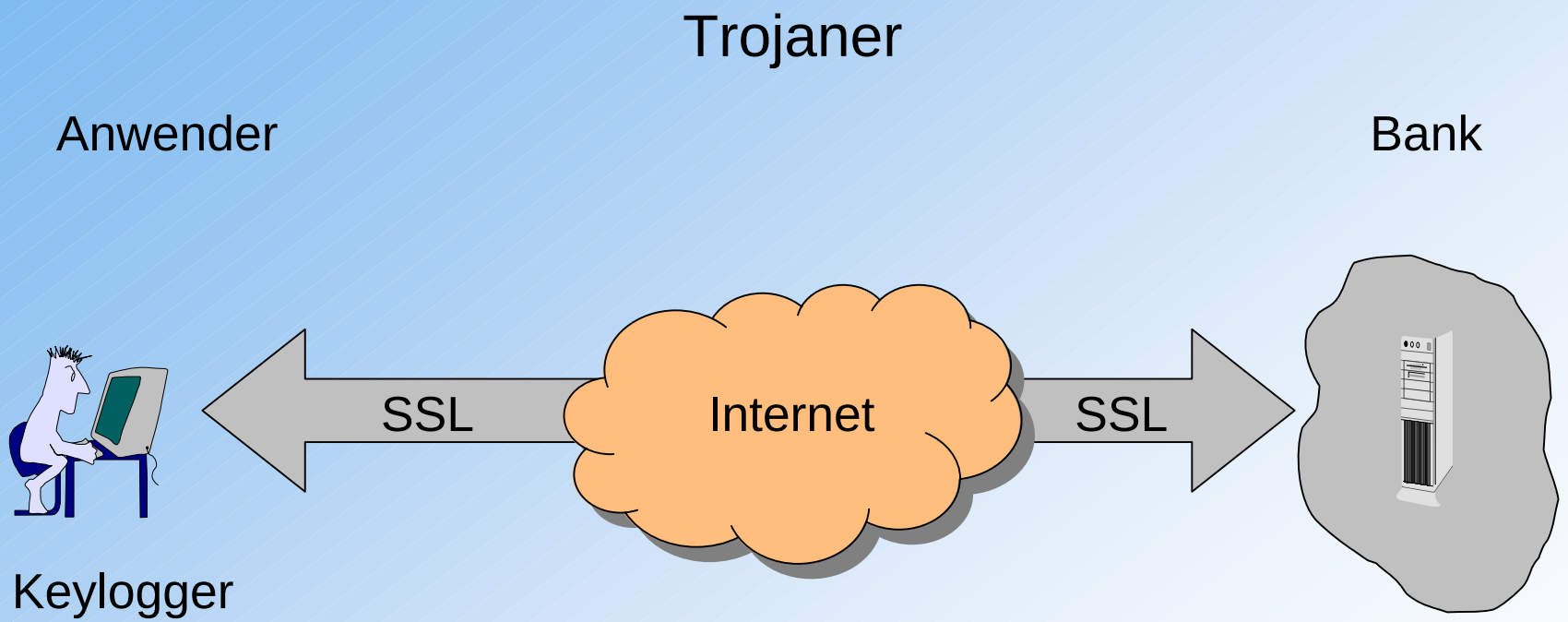
Typische Schwachstellen einer Webapplikation

Caching



Zwischenspeicherung von verschlüsselten Inhalten am PC
(UNVERSCHLÜSSELT !!!)

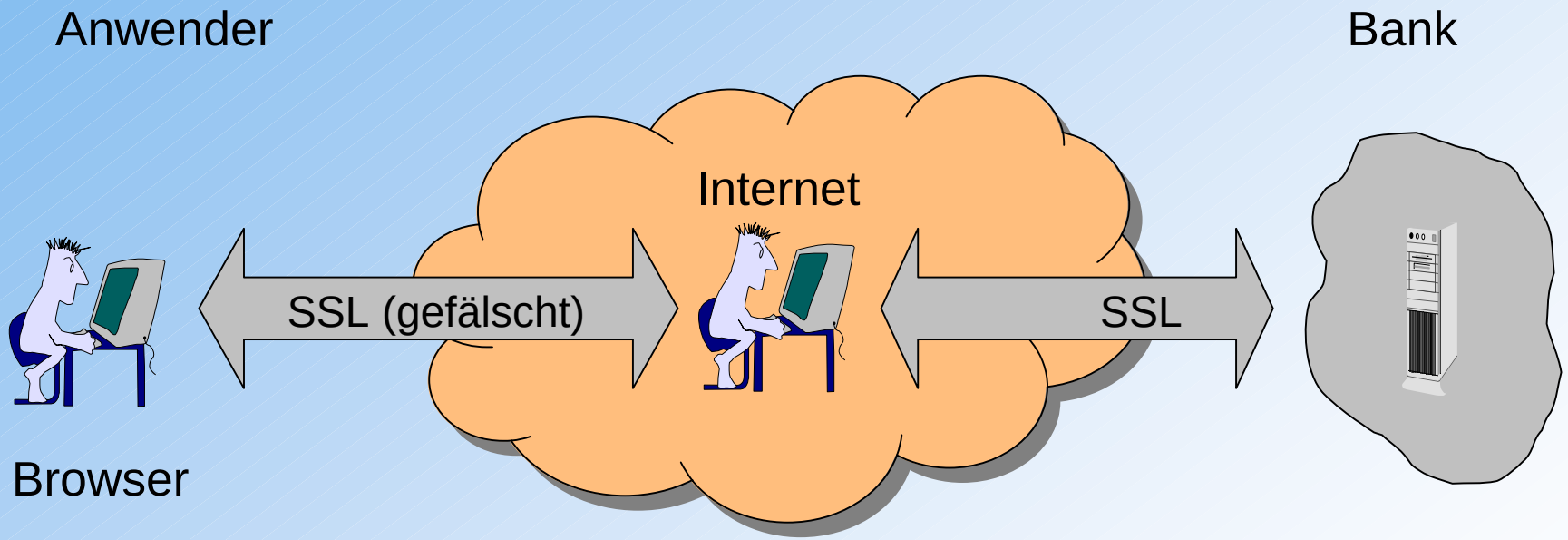
Typische Schwachstellen einer Webapplikation



Alle Tastatureingaben des Anwenders werden mitprotokolliert.

Typische Schwachstellen einer Webapplikation

Anwendung von SSL-Proxies



Die gesamte Kommunikation des Anwenders kann
im KLARTEXT mitprotokolliert werden.

Maßnahmen

- Ausrichtung an den Geschäftsprozess sicherstellen
- Risiko- und Bedrohungsanalyse
- Sicherheitskonzept
- Kombination aus organisatorischen und technischen Maßnahmen
- Aufklärung und Sensibilisierung der Anwender
- Durchführung von Audits in regelmäßigen Abständen
- Externe Unterstützung in Anspruch nehmen

Fragen?

Danke für die Aufmerksamkeit

Manfred Scholz
In der Fischerzeile 13/10
2100 Korneuburg
Tel.: +43 (0)2262/ 728 57
Email: office@sec4you.com