

# Stand der Sicherheit der in der Schweiz eingesetzten SAP-Systeme

... eine Studie der

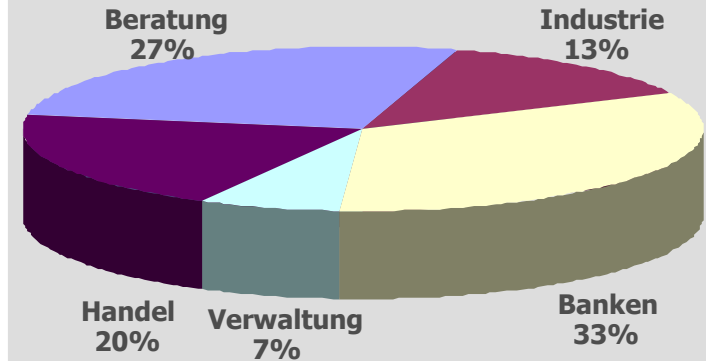


Basierend auf den Ergebnissen der Arbeitsgruppe Sicherheit in SAP-Systemen, durchgeführt und aufbereitet von Jörg Altmeier im April 2004

- Arbeitsgruppe
- Ziele, Vorgehen
- Teilnehmer, Voraussetzungen
- Ergebnisübersicht
- Branchenunterschiede
- Verbesserungsbereiche
- Einschätzung
- Diskussion

- Gegründet im März 2003
- Organisation:  
regelmässige Meetings und Vorträge
- Zusammenarbeit:
  - Security Team der SAP AG
  - Deutsche SAP Anwender Gruppe (DSAG)
  - Arbeitskreis Revision und Datenschutz
  - IGSAP des ISACA Switzerland Chapter
- Ziele:
  - Erarbeiten von Entscheidungshilfen zu allen Fragen der SAP-Sicherheit
  - koordinierte Kommunikation, dadurch
  - höheres Gewicht gegenüber SAP AG

## 17 aktive Mitarbeitende



### **Roadmap:**

#### **(1) Grundschutz-Checkliste**

Q2/2003: Themenabstimmung

Q3/2003: Erarbeitung Selfassessment

Q4/2003: Umsetzung (Pilot)

Q1/2004: Erfahrungsbericht/Survey








#### **(2) Umsetzungsempfehlungen**

ab Q2/2004

#### **(3) Vorgehensempfehlungen**

ab Q4/2004

# Mitglieder der Arbeitsgruppe

<p>Name: <b>Priska Altorfer</b> Funktion: <b>Chairman</b></p>  <p>Firma: <b>Wikima4</b> E-Mail: <a href="mailto:priska.altorfer@wikima4.com">priska.altorfer@wikima4.com</a></p>	<p>Name: <b>Jörg Altmeier (Leiter)</b> Funktion: <b>Managing Director</b></p>  <p>Firma: <b>Wikima4</b> E-Mail: <a href="mailto:joerg.altmeier@wikima4.com">joerg.altmeier@wikima4.com</a></p>	<p>Name: <b>Jürg Bärtschi</b> Funktion: <b>Consultant/ Partner</b></p>  <p>Firma: <b>CCE AG</b> E-Mail: <a href="mailto:juerg.baertschi@cce-ag.ch">juerg.baertschi@cce-ag.ch</a></p>
<p>Name: <b>Patrick Bockel</b></p> <p>Funktion: <b>Leiter Projekte SAP</b> Firma: <b>AddOn AG</b> E-Mail: <a href="mailto:patrick.bockel@addon-ag.ch">patrick.bockel@addon-ag.ch</a></p>	<p>Name: <b>Simone Bonanni</b></p>  <p>Funktion: <b>Leiter IT - Sicherheit / T</b> Firma: <b>Zuger Kantonalbank</b> E-Mail: <a href="mailto:simone.bonanni@zugerkb.ch">simone.bonanni@zugerkb.ch</a></p>	<p>Name: <b>Monika Galli</b> Funktion: <b>Revisionsexpertin</b> <b>CISM, CISA</b></p>  <p>Firma: <b>Eidg. Finanzkontrolle</b> E-Mail: <a href="mailto:monika.galli@efk.admin.ch">monika.galli@efk.admin.ch</a></p>
<p>Name: <b>Rudolf Gisler</b> Funktion: <b>IT-Application Security Officer</b></p>  <p>Firma: <b>MGB</b> E-Mail: <a href="mailto:rudolf.gisler@mgb.ch">rudolf.gisler@mgb.ch</a></p>	<p>Name: <b>Hanspeter Mäder</b> Funktion: <b>Manager</b></p>  <p>Firma: <b>Abraxas Informatik AG</b> E-Mail: <a href="mailto:hp.maeder@bluewin.ch">hp.maeder@bluewin.ch</a></p>	<p>Name: <b>Andrea Schäfer</b></p> <p>Funktion: Firma: <b>Bell AG</b> E-Mail: <a href="mailto:SchaeferA@bell.ch">SchaeferA@bell.ch</a></p>
<p>Name: <b>Rolf Wälti</b></p> <p>Funktion: Firma: <b>RTC AG</b> E-Mail: <a href="mailto:rolf.waelti@rtc.ch">rolf.waelti@rtc.ch</a></p>		

# Vorgehen der Studie

- Einladung potentieller Kandidaten durch direktes Anschreiben, Veröffentlichungen in der Fachpresse sowie auf bekannten Internet-Portalen.
- Durchführen eines von Assessoren strukturiert geführten Interviews (3 - 8 Stunden) auf Basis von 48 Prüf-Statements.
- Für jede Prüffrage wurden von den Interviewpartnern Punkte von 0-100 für den Ist wie für den Sollzustand vergeben.
- Die Ergebnisse wurden für jedes teilnehmende Unternehmen in einem individuellen Management-Bericht zusammengestellt, die aggregierten Ergebnisse bilden die Grundlage der vorliegenden Studie.

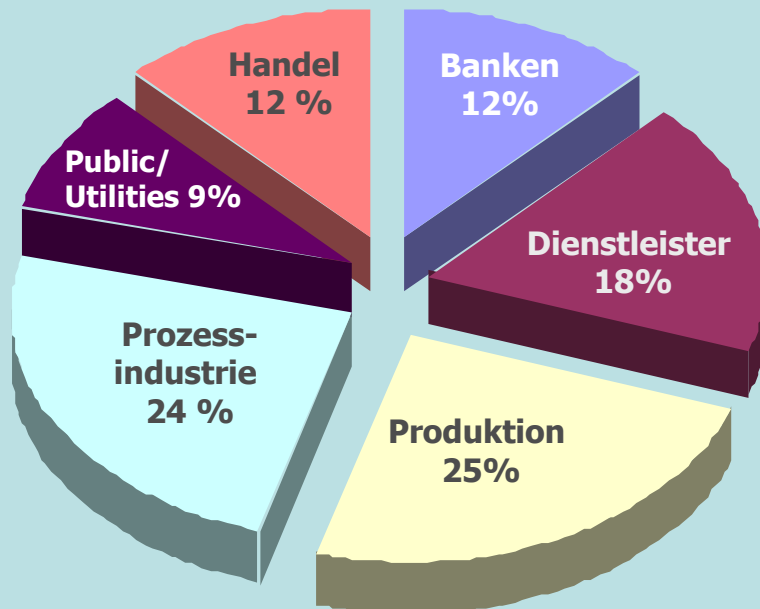
# Ziele der Studie

- Ermittlung des Status Quo der Sicherheit von SAP-Systemen in Unternehmen.
- Ermittlung des State-of-the-art der Sicherheit von SAP-Systemen in Unternehmen.
- Identifizierung von dringenden und empfohlenen Verbesserungsbereichen.
- Grundlage für zukünftige Schwerpunktsetzungen in der Arbeitsgruppe Sicherheit in SAP-Systemen und für Empfehlungen hin zum State-of-the-art.
- Erhöhung der Awareness im Bereich SAP-Sicherheit.

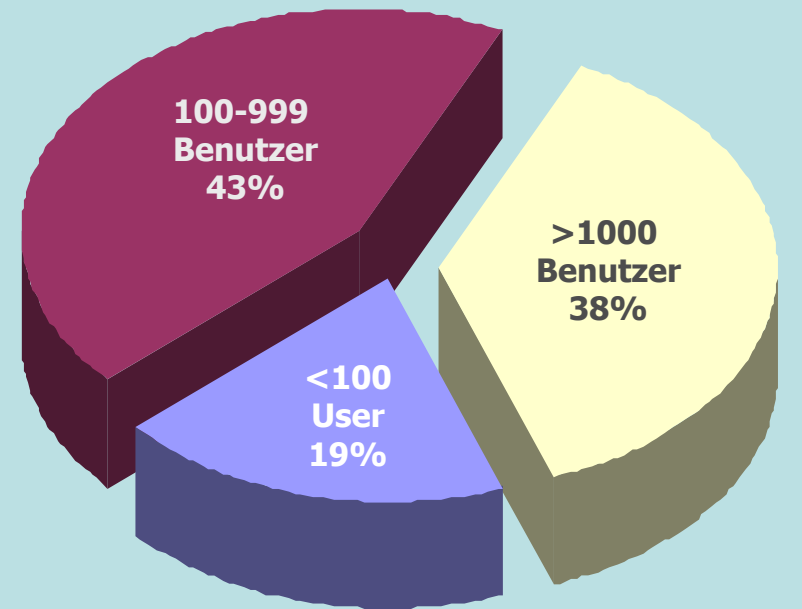
# Teilnehmer der Studie

- > 35 Unternehmen
- > 100 Interviewpartner
- > 46'000 Benutzer

## Aufteilung nach Branchen



## Aufteilung nach Grössen



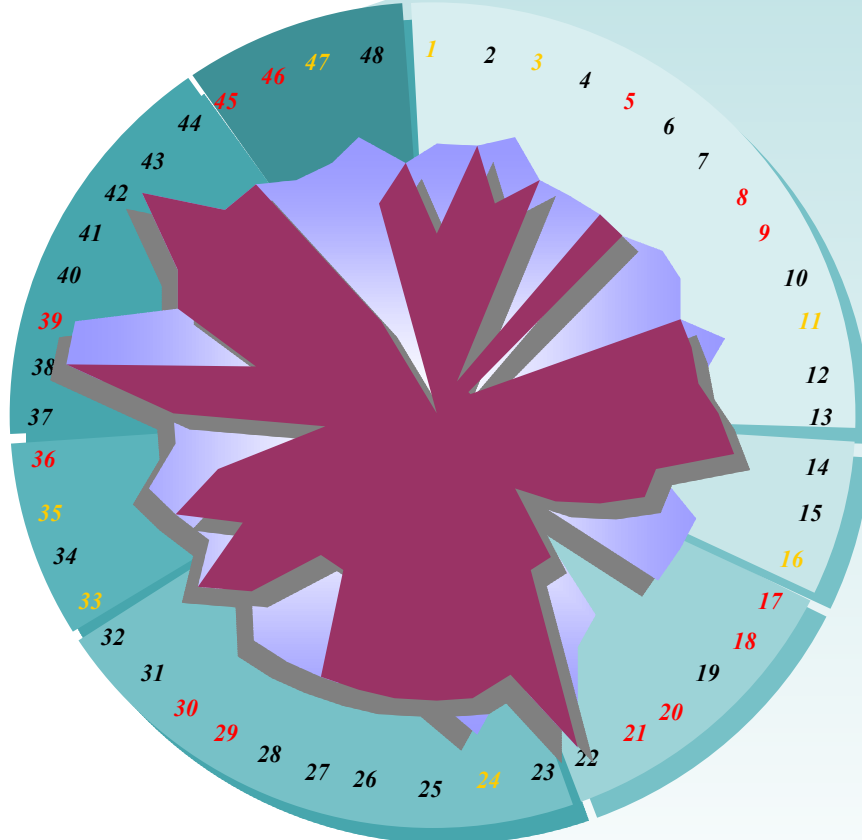
# Voraussetzungen für eine Teilnahme

- Produktives SAP-System mit Kerngeschäftsprozessen.
- Einverständnis zur Prüfung und Einsicht.
- Die benötigten Interviewpartner werden freigestellt (Zeitraumen 1/2 - 1 Tag).
- Ergebnisse dürfen (anonymisiert) weiterverwendet werden.

- Das Assessment basierte auf der Selbsteinschätzung der jeweiligen Interviewpartner.
- Eine Überprüfung der Richtigkeit der Aussagen durch die Assessoren konnte aufgrund der Grösse des Untersuchungsbereichs und der knappen Zeit nicht erfolgen.
- Gesamt-Studie stellt die subjektive Einschätzung der Interviewpartner dar. Die Tatsache, dass die Interviews immer von den gleichen Assessoren begleitet und unterstützt wurden, erhöht aber die Validität der Aussagen.

- Die erhobenen Daten und resultierenden Ergebnisse werden ausschliesslich dem geprüften Unternehmen kommuniziert und in keinem Falle an Dritte weitergegeben.
- Es werden keine externe Zugriffe auf die untersuchten SAP-Systeme durchgeführt.
- Zur Aggregierung und Präsentation werden alle Informationen, die einen Rückschluss auf das geprüfte Unternehmen zulassen, anonymisiert.
- Die Assessoren verpflichten sich zur Geheimhaltung.

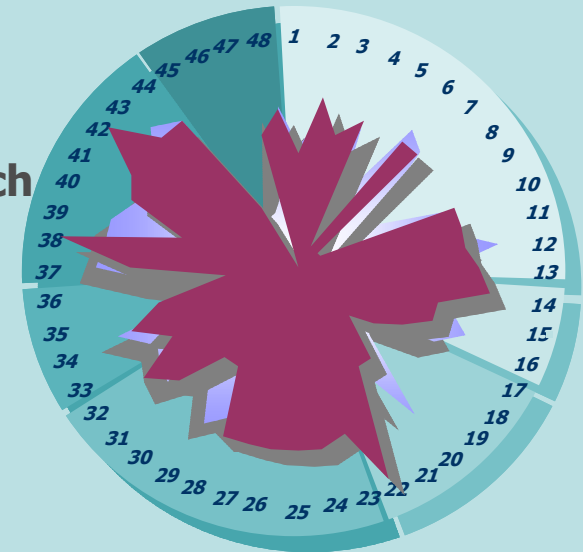
# Auswertung eines Kandidaten (Verbesserungs-Matrix)



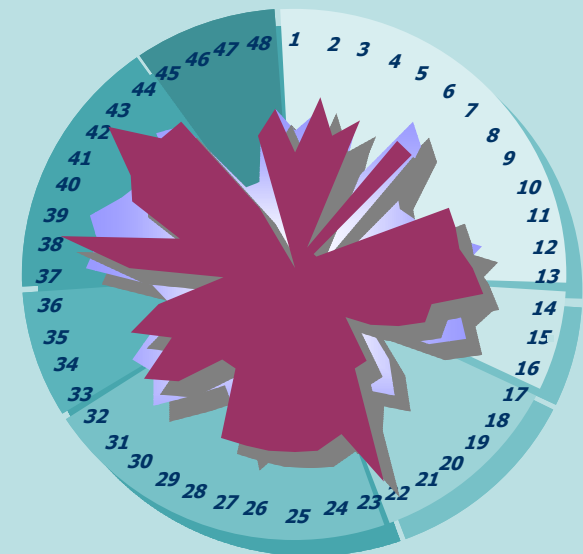
Bereich	Gesamteindruck	Verbesserungspotentiale/ Lücken
Organisation	<p>Generell stark ausgeprägtes Sicherheitsdenken - typisch innerhalb dieser Branche - minimiert das IT-Risiko in grossem Masse. Die Verantwortlichen innerhalb der Informatik haben klare Vorstellungen, wie die erkannten Sicherheitslücken behoben werden können. Pragmatisch orientierte Lösungsansätze können schnell und mit geringem Aufwand die Prozess- und System-Sicherheit verbessern.</p> <p>Gut ausgeprägt sind die geordnete Störfallbehandlung, die Vertragsgestaltung mit Dritten und die Aufgabenverteilung innerhalb der SAP-Organisation. Kleinere Verbesserungspotentiale bestehen im Bereich Notfallkonzept, Risikomanagement und Richtlinien-Überprüfung.</p> <p>Einige organisatorische Anforderungen im Bereich Sicherheitsorganisation und Kommunikation mit SAP AG können nur ungenügend erfüllt werden und sollten als kritisch betrachtet werden. Insbesondere die bestehende Ressourcenknappheit zur Bearbeitung von Sicherheitsbelangen bereitet Sorge.</p>	<p>(5) Kommunikation mit SAP ist auf beiden Seiten ungenügend</p> <p>(8) + (9) Ressourcengaps im Bereich der Sicherheitsorganisation und Kontrolle; mangelnde Awareness beim Management</p> <p>(1) Verfeinerung der Notfallkonzepte und Test ausstehend; Integration der Datenverluste aus SAP-Systemen in bestehende Konzepte</p> <p>(3) Mangelnde Management-Awareness im Bereich Risikomanagement</p> <p>(11) Einhaltung vorgegebener Richtlinien wird nicht systematisch geprüft</p>
Physischer Schutz	<p>Der Physische Schutz zur Absicherung der Infrastruktur und Backup-Daten ist bedarfsgerecht; verbesserungsfähig ist die Absicherung kritischer Drucker im Bereich der Barcode-Etiketten.</p>	<p>(16) Das Drucker-Output-Management weist Sicherheitslücken auf; sensitive Daten werden nicht geschützt.</p>
Netzwerk	<p>Dass SAP-Daten, die unverschlüsselt zwischen Server und Client ausgetauscht werden, verletzlich sind, ist den am Assessment beteiligten Personen bekannt. Aus diesem Grund wurden eine periodischen Überprüfung des Netzwerkes und ein konsequentes Monitoring der Zugriffe aufs SAP-System als dringende Verbesserungsbereiche erkannt. Das derzeit eingesetzte Verschlüsselungsverfahren (VPN-Tunneling) bietet einen teilweisen Schutz, von dem aber nur bestimmte Personenkreise profitieren, nicht aber interne Anwender mit kritischen Aufgaben und Berechtigungen (z.B. Personal und Finanzen).</p>	<p>(17) Penetration-Tests werden nicht periodisch durchgeführt</p> <p>(18) Verschlüsselung von kritischen Daten wird nicht umgesetzt (nur Ansätze zur Netzverschlüsselung)</p> <p>(20) Laptops sind noch mit Modems ausgestattet</p> <p>(21) Zugriff auf SAP-System wird nicht konsequent protokolliert und ausgewertet</p>
Server	<p>Grundsätzlich weist die SAP-Anwendung eine hohe Qualität auf; die Benutzer sind entsprechend zufrieden. Die angegebenen kritischen Bereiche sind den Verantwortlichen in Ausmass und Wirkung bekannt.</p>	<p>(29) Authority Checks sind nicht in jeder Anwendung vorhanden</p> <p>(30) zu viele Personen haben zu viele Rechte in der Produktionsumgebung</p> <p>(24) Auswertungen im SAP sollen verbessert werden</p>
Clients	<p>Mitarbeiter und Management sind sich der Verletzbarkeit des SAP-Systems (noch) nicht genügend bewusst. Das ausserhalb SAP-Systeme überdurchschnittliche Sicherheitsniveau lässt aber vermuten, dass geeignete Massnahmen zur Verbesserung der Awareness rasch zu Verbesserungen führen werden.</p>	<p>(36) Sensible Daten werden beim Ausdruck nicht spezifisch geschützt</p> <p>(33 + 35) Awareness bei den Benutzern ist zu verbessern</p>
Berechtigungen	<p>Das Konzept für Benutzer-Berechtigungen ist gut ausgelegt; Verfahren sind etabliert, die einen Missbrauch minimieren helfen. Dringender Handlungsbedarf besteht bei Systembenutzern, die von aussen auf das SAP-System zugreifen.</p>	<p>(39) Benutzer-Berechtigungs-Konzept System-Benutzer ist nur ansatzweise vorhanden</p>
Protokollierung	<p>Das SAP-System stellt im Standard Hilfsmittel zur Verfügung, die ein proaktives Monitoring der sicherheitskritischen Systemereignisse ermöglichen. Diese Möglichkeiten werden bislang nur ungenügend genutzt. Es wurde aber erkannt, dass Fachabteilungen, einen zusätzlichen Nutzen durch den Einsatz der Protokollierung erfahren können.</p>	<p>(45 + 46) Audit Information System (AIS) ist implementiert, wird aber nicht genutzt</p> <p>(47) System-Protokollierung ist nur ansatzweise eingeschaltet</p>

# Auswertung eines Kandidaten (Benchmarks)

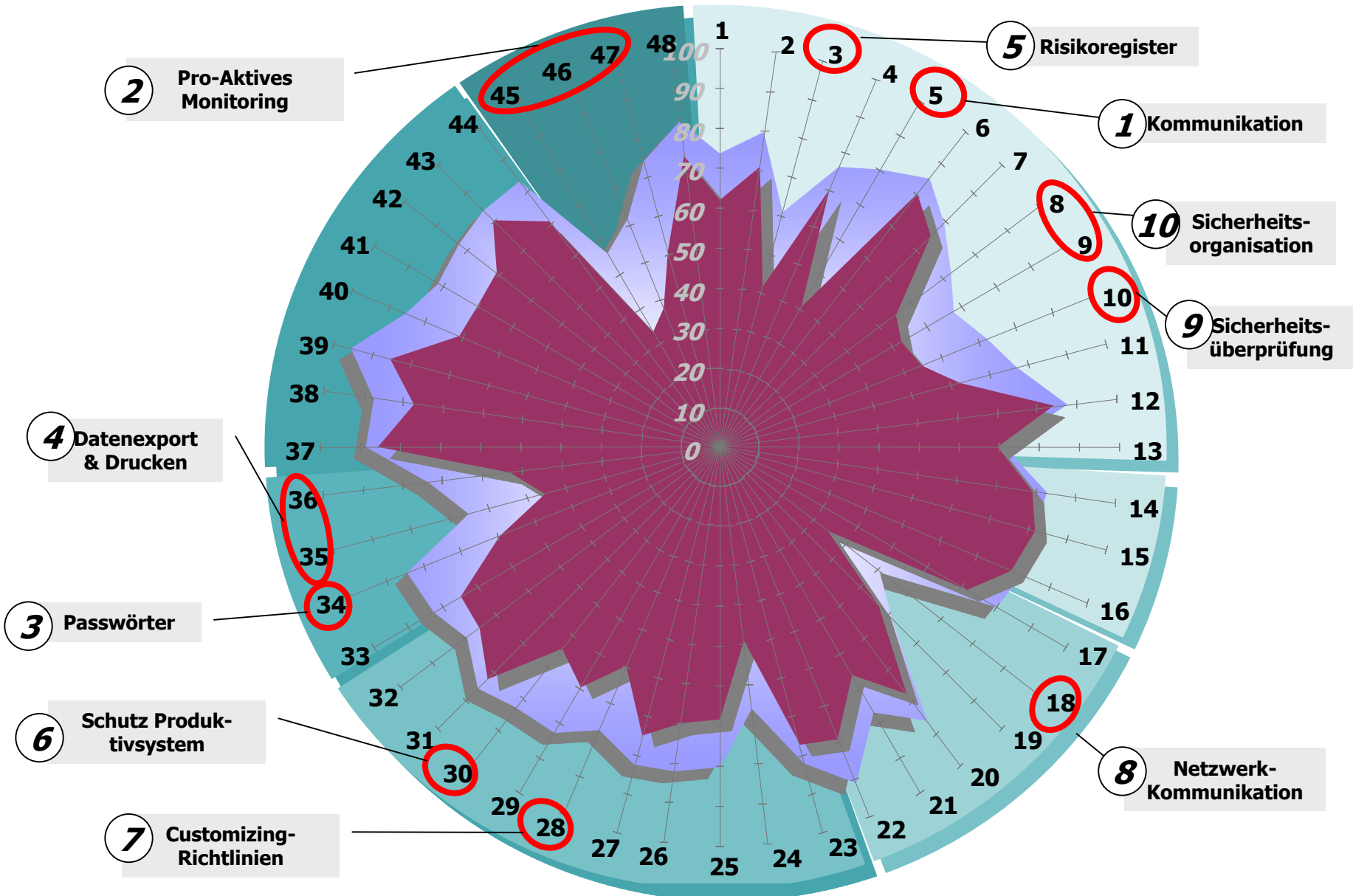
## Branchenvergleich



## Gesamtvergleich



# Erkannte Verbesserungsbereiche (Top 10)



# Branchenvergleich



***Prozess-  
industrie***



***Produktion***



***Dienstleister***



***Banken***



***Handel***



***Utilities/  
Public***

*In den Top 10 keine  
signifikanten Bewertungs-  
Unterschiede zwischen  
den Branchen!*

Gesamt-  
durchschnitt

## Verbesserungsbereich: Kommunikation

- 7 von 10 befragten Unternehmen bewerten die bestehende Kommunikation zu Themen der SAP-Sicherheit als ungenügend.
- Von SAP AG wird eine pro-aktive Informationspolitik (Bringschuld) erwartet, die auf das kundenbezogene Umfeld abgestimmt ist; SAP Security Newsletter wird positiv bewertet.
- Kommunikation zur SAP AG bzw. zum Outsourcing-Partner, periodische Berichterstattung an die Geschäftsleitung zu Neuerungen im Bereich der SAP-Sicherheit und Mitarbeit in Arbeits- und Benutzergruppen soll institutionalisiert werden (Holschuld).

- Das SAP-System stellt Hilfsmittel zur Verfügung, die ein proaktives Monitoring der sicherheitskritischen Systemereignisse ermöglichen. Diese Möglichkeiten sind bislang wenig bekannt und werden nur ungenügend genutzt.
- Es wurde erkannt, dass Unternehmen einen zusätzlichen Nutzen durch den Einsatz der System-Protokollierung erfahren können.
- Das angebotene Audit Information System (AIS) sollte von SAP AG im Bereich Security Incident weiter entwickelt werden.

- In 5 von 10 befragten Unternehmen werden die Benutzer mit zu vielen Authentifizierungs-Mechanismen (> 3) konfrontiert und sind mit dem Merken von verschiedenen Passwörtern überlastet.
- Genutzte Passwörter sind oft nicht qualifiziert und es kann nicht sichergestellt werden, dass sie sicher verwahrt werden.
- Zahl der Passwörter sollte mit geeigneten Mitteln reduziert, die Qualität erhöht werden. Dabei stehen neben Mechanismen eines dedizierten Single Sign-On die Bereitstellung einer bedarfsgerechten Passwort-Policy im Vordergrund.

- In 5 von 10 Unternehmen findet sich ein zu sorgloser Umgang mit elektronischen Dokumenten aus dem SAP und beim Druckprozess. Es werden Daten in externe Applikationen exportiert, ohne dass sie durch geeignete Sicherungsmechanismen oder eine entsprechende Verfahrensvorschrift geschützt werden.
- Es sollten Richtlinien zum Datenexport in Office-Applikationen und zum (lokalen) Drucken besonders sensibler Daten erstellt werden. Mit Hilfe geeigneter Massnahmen sollte die Awareness bezüglich sensibler Daten erhöht werden.

- In den befragten Unternehmen existieren Risikoabschätzung und Schadensregister meist nur in rudimentärer Form und sind ausschliesslich systembezogen. Die (geldmässige) Folgenabschätzung eines Prozess-Unterbruchs durch Umfeldfaktoren ist nicht möglich.
- Es sollte ein Risikoregister bis auf Ebene Geschäftsprozess-Schritte erstellt werden. Dies erlaubt es, die Risiken eines Geschäftsprozesses zu bewerten und eventuelle Schäden zu quantifizieren. Insbesondere wird anhand einer bedarfsgerechten Risikoanalyse die Berechnung eines Return on Security Investment ermöglicht (ROSI).

- In zahlreichen befragten Unternehmen haben zu viele Personen Entwicklungs-Rechte in der kritischen Produktivumgebung. Die Gefahr, dass eine fahrlässige Fehleingabe oder eine böswillige Manipulation zu nicht abschätzbaren Schäden führt, wird unterschätzt.
- Die Produktivsysteme sollten gegen jede Art der Veränderung gesperrt sein. Dazu gehören neben entsprechenden Einstellungen auch der vollständige Verzicht auf zu weit gehende Entwicklungs-Rechte.
- Die Reduktion der SAP\_ALL- bzw. artverwandten Berechtigungen schützt auch die betroffenen Personen.

## Verbesserungsbereich: Customizing-Richtlinien

- In vielen Unternehmen sind Dokumentations-Qualität und Einhaltung vorgegebener Richtlinien beim Customizing ungenügend.
- Die mangelhafte Qualität der Dokumentation resultiert aus Altlasten, die noch nicht aufgearbeitet sind oder aus der Tatsache, dass die Einführung gerade erst abgeschlossen wurde.
- Es sollten Mechanismen eingesetzt werden, die die Dokumentation der Customizing-Einstellungen sowie Einhaltung der Vorgaben überprüfen und erzwingen helfen. Insbesondere sind genügend Ressourcen zur Altlastenbereinigung bereit zu stellen. Damit könnte dem nächsten Release-Wechsel gelassener entgegen gesehen werden.

- Dass SAP-Daten, die unverschlüsselt zwischen Server und Client ausgetauscht werden, verletzlich sind, ist den meisten befragten Personen bekannt.
- Die eingesetzten Verfahren des VPN-Tunneling bieten einen teilweisen Schutz, von dem bestimmte Personenkreise profitieren, nicht aber interne Anwender mit kritischen Aufgaben und Berechtigungen.
- Kritische Daten und Prozesse sollten mit Secure Network Communication (SNC), ausgehende Belege möglichst mit Hilfe digitaler Signaturen geschützt werden.

- In vielen befragten Unternehmen wird keine tiefere Überprüfung von im SAP-Bereich arbeitenden Personen mit sicherheitskritischen Aufgaben bei Einstellung durchgeführt.
- Eine periodische Überprüfung auch langjähriger Mitarbeiter ist in den seltensten Fällen institutionalisiert und gilt als „Führungsaufgabe“.
- Bei Einstellung sollten Referenzauskünfte eingeholt werden; Führungskräfte sollten pro-aktiv bei der „Beobachtung“ von Fachkräften des Personalwesens unterstützt werden.

- In vielen Unternehmen ist (noch) niemand dediziert für die Sicherheit der SAP-Systeme zuständig; die Verantwortung wird von Stellen (mit) übernommen. Oftmals besteht daher ein Ressourcen- bzw. Know-how-Problem.
- Eine unabhängige Kontrollinstanz, die die Sicherheitsmassnahmen überprüft, fehlt meist oder ist zu wenig über die speziellen Erfordernisse der SAP-Systeme informiert.
- Unternehmen sollten für die SAP-Sicherheits-Verantwortung und die unabhängige Kontrollinstanz Personen oder Teams definieren und mit genügend Ressourcen, Know-how und Entscheidungskompetenzen ausstatten.

- Assessments haben bei zahlreichen Teilnehmern die intensive Auseinandersetzung mit der Sicherheit von SAP-Systemen erst ausgelöst.
- Verantwortliche haben klare Vorstellungen, wie die erkannten Sicherheitslücken behoben werden können.
- Pragmatisch orientierte Lösungsansätze können schnell und mit geringem Aufwand die Prozess- und System-Sicherheit verbessern.
- Stand der Sicherheit der in der Schweiz eingesetzten SAP-Systeme ist hoch, die selbst gesteckten Ziele auf einem erfreulichen Niveau.

Herzlichen Dank!

Präsentation ist auf der  
Webseite der fgsec abrufbar  
[www.fgsec.ch](http://www.fgsec.ch).

Weitere Informationen zur  
Studie und zur Arbeitsgruppe  
Sicherheit in SAP-Systemen  
sind erhältlich bei:

Jörg Altmeier  
Leiter AGSAP

Managing Director  
wikima4 AG

[joerg.altmeier@wikima4.com](mailto:joerg.altmeier@wikima4.com)

[www.wikima4.com](http://www.wikima4.com)

