

Informationssicherheit – Wunsch und Wirklichkeit

...vom schrittweisen Start zur
Erfüllung komplexer Standards

Prof. Dr. Rudolf Hackenberg
Hochschule Regensburg
rudolf.hackenberg@informatik.fh-regensburg.de

- Ausgangslage
 - Motivation
 - Erkenntnisse
 - Praxis
- Studie IT Security Awareness
 - Einordnung, Umfeld und Ziele
 - Ergebnisse
 - Handlungsbedarf
- Anwenderzentrum IT Security
 - Mission
 - Mehrwert
 - Netzwerk
 - Finanzierung

Globalisierung der Märkte

Abhängigkeit von IT/ TK

Komplexität der Systeme

„Time to Market“

Umgang mit neuen Technologien

Wirtschaftsspionage

Rechtliche Rahmenbedingungen

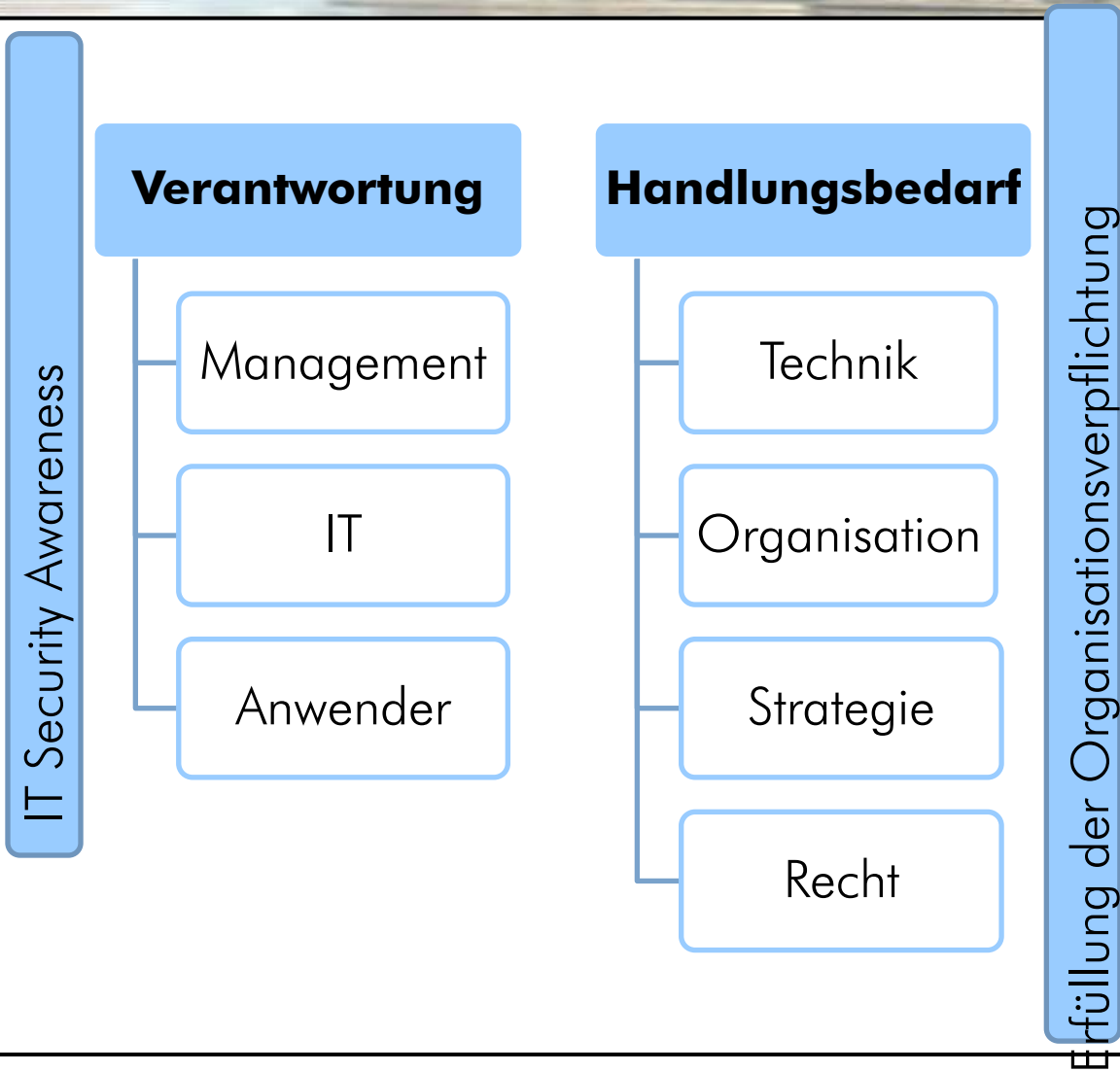
„Handy“

„Beta Tester“

„E-Mail“

Konsequenzen

Herausforderungen

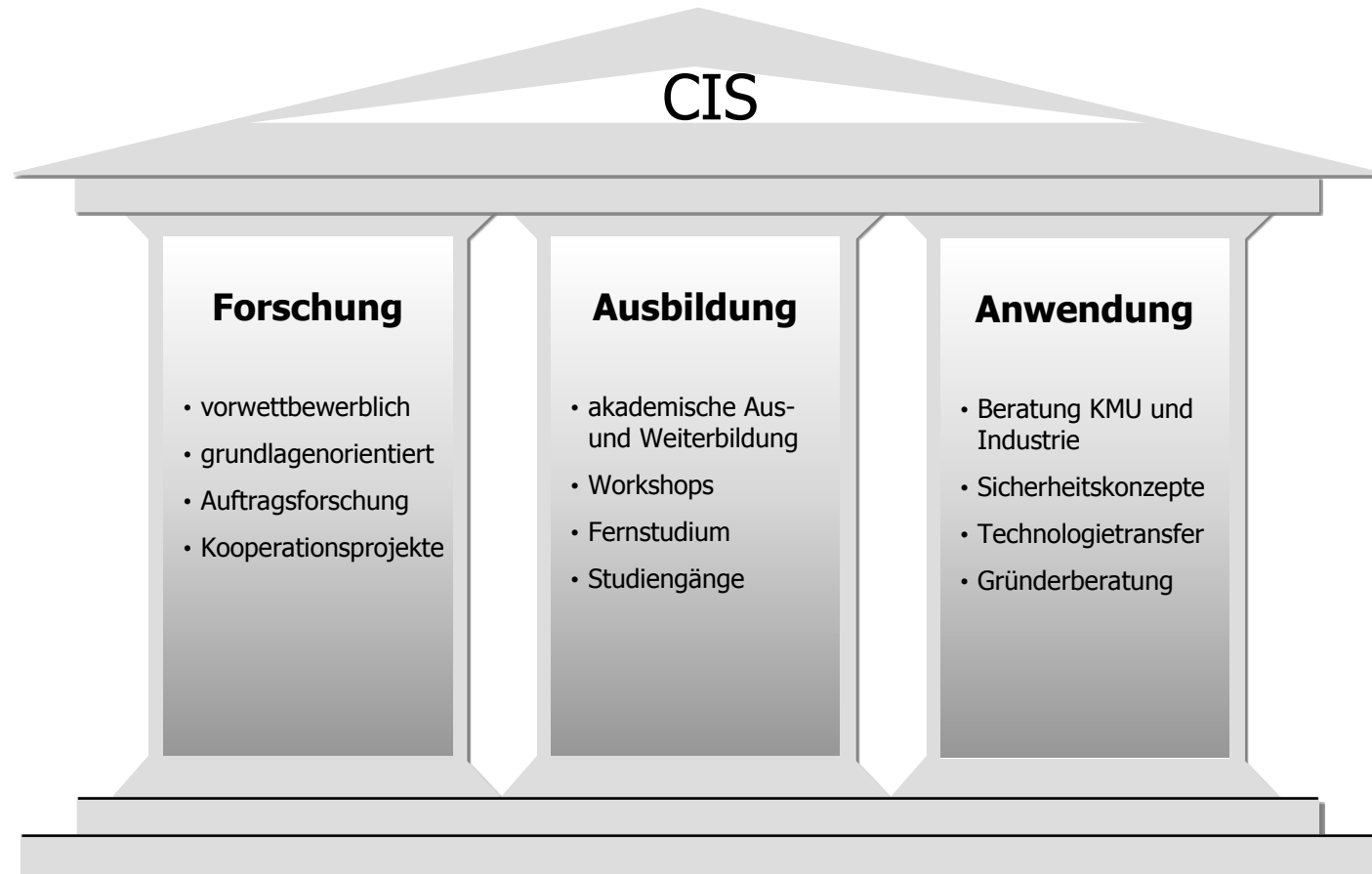


- BSI Lagebericht 2007
 - „...Ursache f.d. mangelnde Investition in IT-Sicherheit ist auf der Ebene der Geschäftsleitung und des Managements anzusiedeln...“
- BSI Vize Michael Hange 2008
 - „Bei vielen Verantwortlichen...ist das Sicherheitsbewusstsein heute noch nicht ausreichend ausgeprägt.“
- ICM Research Jan. 2009
 - 45% der KMUs glauben aus mangelndem Bekanntheitsgrad nicht ins Visier von Hackern zu kommen ... speichern jedoch für Angreifer interessante, weil sensible Kundeninformationen
- Ponemon Institute Jan. 2009
 - mehr als 50% der Mitarbeiter hatten beim Ausscheiden unbemerkt Daten mitgehen lassen ... weil Schutz fehlte.



IT Security Awareness Studie

- Unternehmen kommunizieren regelmäßig Unsicherheit bzgl. der Umsetzung von IT-Security in bestimmten Bereichen
- Sie fragen nach Leitfäden und „Best-Practise“
- Studie hinsichtlich IT-Security Awareness, um den aktuellen Status der Umsetzung zu ermitteln - bei:
 - Unternehmensleitung
 - IT-Leitung
 - User



CIS – Center for Information Security
Regensburger Hochschul-Kompetenz

„Anwendersäule“ Hochschule Regensburg

Anwendung

- Beratung KMU und Industrie
- Sicherheitskonzepte
- Technologietransfer
- Gründerberatung

Anwenderzentrum IT Security
Prof. Dr. Hackenberg

Biometrie
Prof. Dr. Hook

Datenschutz
Prof. Dr. Kulla

Funktionale Sicherheit,
Prof. Dr. Mottok

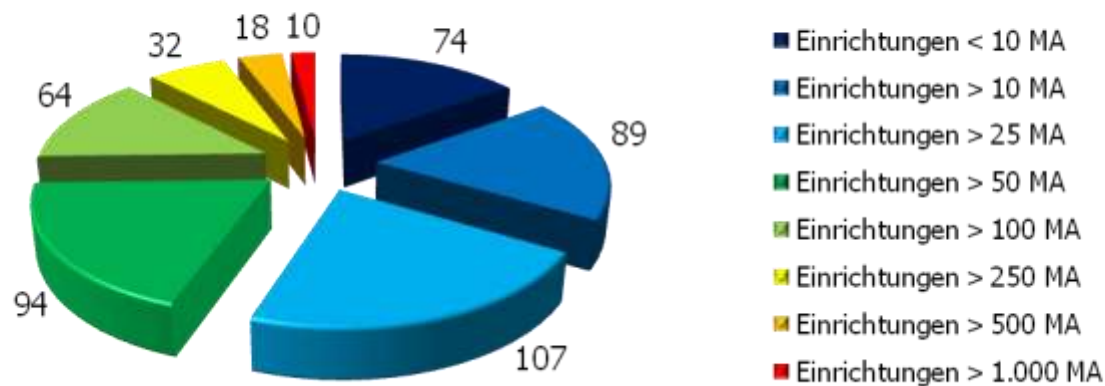
Kryptographie
Prof. Dr. Pohl



Rahmen der Studie

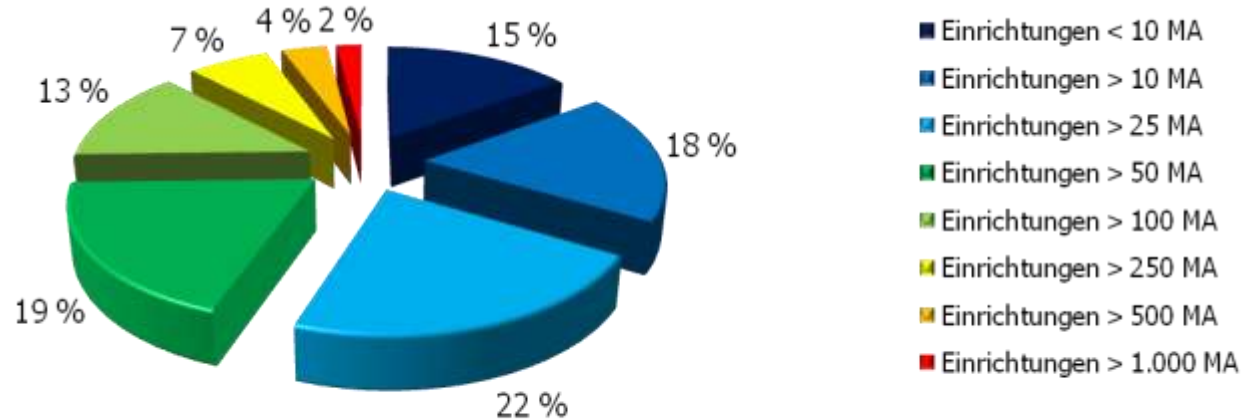
- Unternehmen und Behörden in Deutschland
- in Zusammenarbeit: HS Regensburg und A.P.E. ICT-Group
- geplantes Ende: Q3 2009

Anzahl der teilgenommenen Unternehmen und Behörden nach Mitarbeiterzahl



Interesse und Beteiligung an der Studie

- 64 % der beteiligten Einrichtungen < als 100 Mitarbeiter



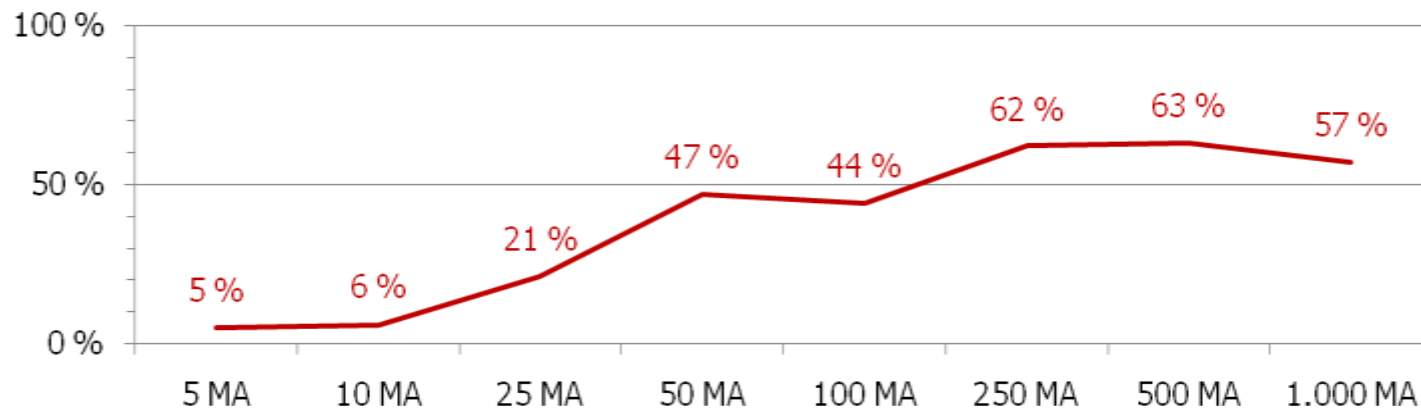
Auszug

- Ist Ihnen die rechtliche Lage bei Unterlassung der technischen und organisatorischen Einführung und dem Betrieb einer adäquaten IT-Sicherheitslösung bewusst?
- Welche Bereiche der IT sind in Ihrem Unternehmen bei einem Ausfall als kritisch einzustufen?
- Sind Ihnen die möglichen Kosten bei einem solchen Ausfall bekannt?
- Sind die Zuständigkeiten in Ihrem Unternehmen geklärt?

Auszug

- Sind Ihnen die Anforderungen Ihrer Geschäftspartner hinsichtlich IT-Sicherheit bekannt?
- Sind die Verträge mit Mitarbeitern, Kunden und Lieferanten hinsichtlich IT-Sicherheit geregelt?
- Ist die private Nutzung von Internet und E-Mail am Arbeitsplatz geregelt?
- Findet eine Klassifikation von Informationen und Bestimmung des Schutzbedarfs statt?
- Finden in Ihrem Unternehmen Weiterbildungen der Mitarbeiter hinsichtlich Awareness statt?

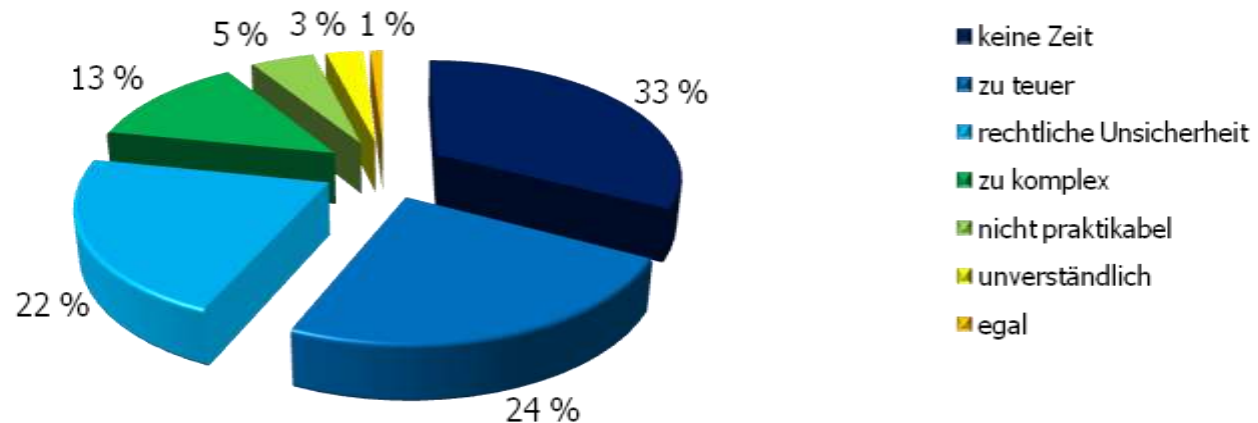
Umsetzung Organisationsverpflichtung



Tendenzen:

- In allen Unternehmensgrößen trifft man auf Unsicherheit bzgl. rechtlicher Grundlagen
- Erst durch die Orientierung an Standards (BSI, ISO) ist ein signifikanter Anstieg von Awareness und der OV-Umsetzung zu verzeichnen.

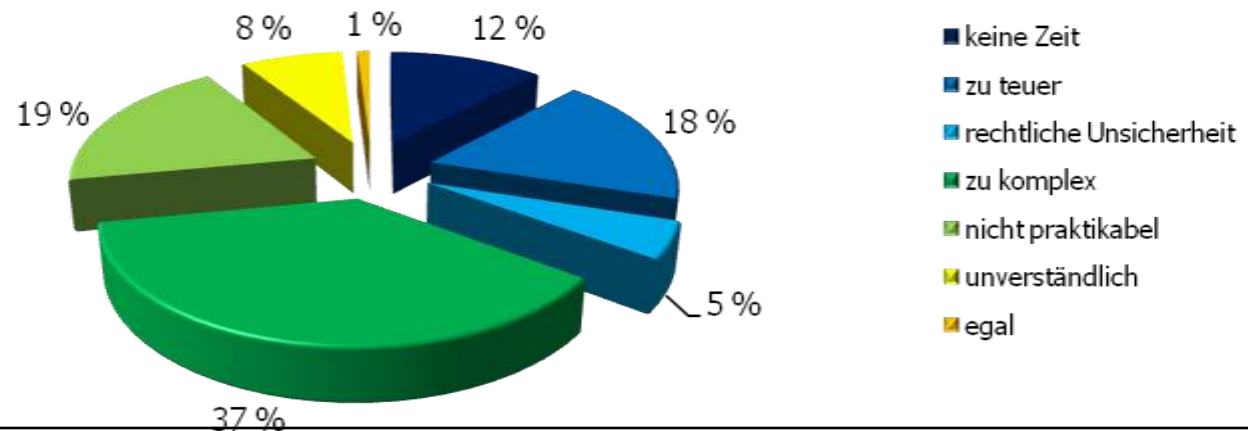
Gründe für Nichtumsetzung (< 100 MA)



Tendenzen:

- Zeit, Kosten und rechtl. Unsicherheit dominieren und verhindern die Umsetzung der OV
- es wird versucht die Verantwortung an IT DL zu delegieren,
- Über 80 % haben das Vorgehen nach BSI oder ISO innerhalb der ersten 2 Monate abgebrochen.

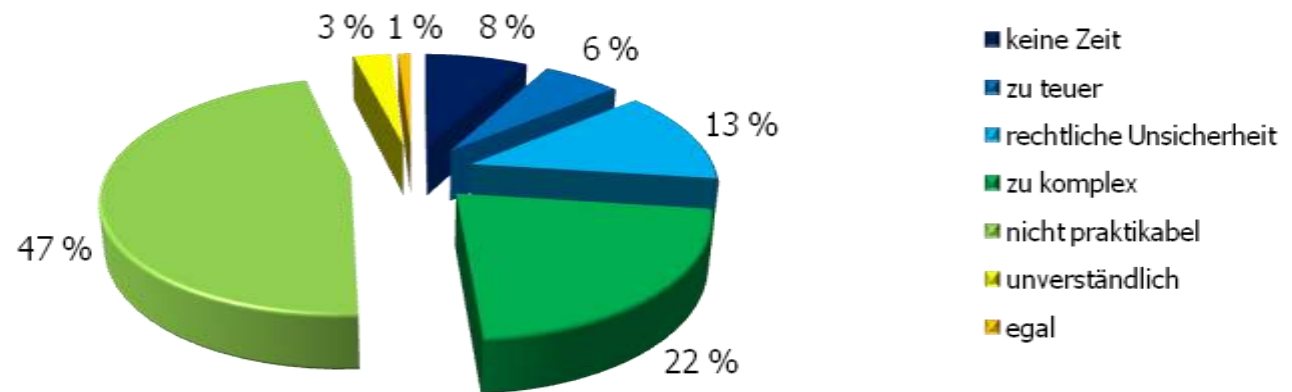
Gründe für Nichtumsetzung (100-500 MA)



Tendenzen:

- Über 50 % der Unternehmen berichten über zu große Komplexität und mangelndem Praxisbezug der rechtlichen, organisatorischen und technischen Vorgaben.
- Erst durch das Einbeziehen externer Berater konnte die Umsetzung vorangebracht werden.

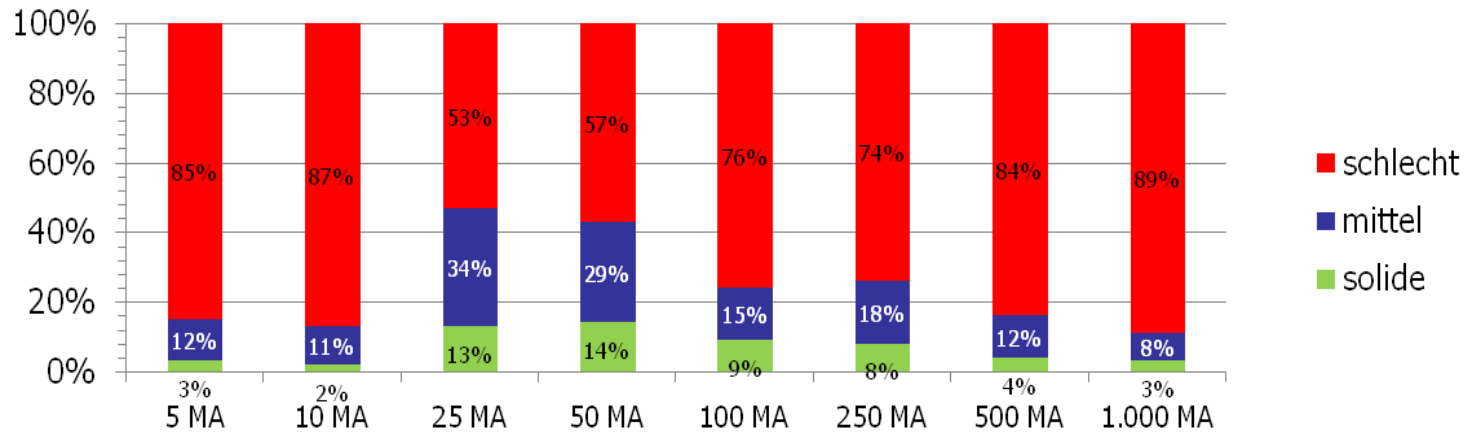
Gründe für Nichtumsetzung (> 500 MA)



Tendenzen:

- Eingeführte Maßnahmen greifen nicht, da sie nicht "gelebt" werden.
- Große Defizite bei der User-Awareness, vor allem hinsichtlich der Akzeptanz der Policies und Richtlinien.
- Über 80 % gaben an, dass die Aufrechterhaltung der Maßnahmen an den Usern scheitere.

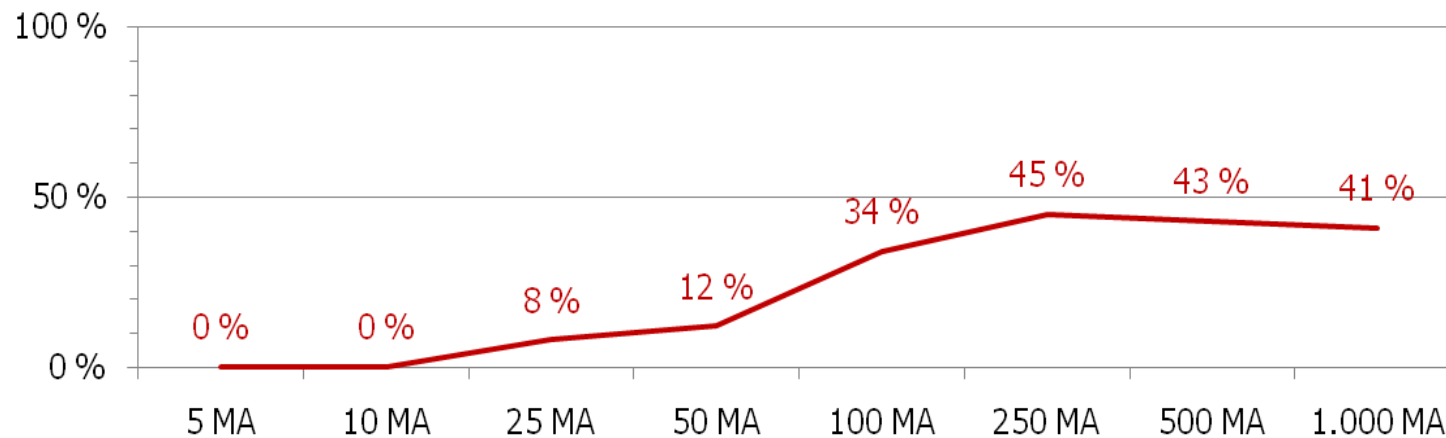
Rechtl. Wissen zu E-Mail und Webnutzung am Arbeitsplatz



Tendenzen:

- Deutliche Unsicherheit bei Unternehmens- und IT-Verantwortlichen
- Massnahmen werden nicht gelebt
- Kurze Halbwertszeit der Maßnahmen und Regelungen (1 - 4 Monate)

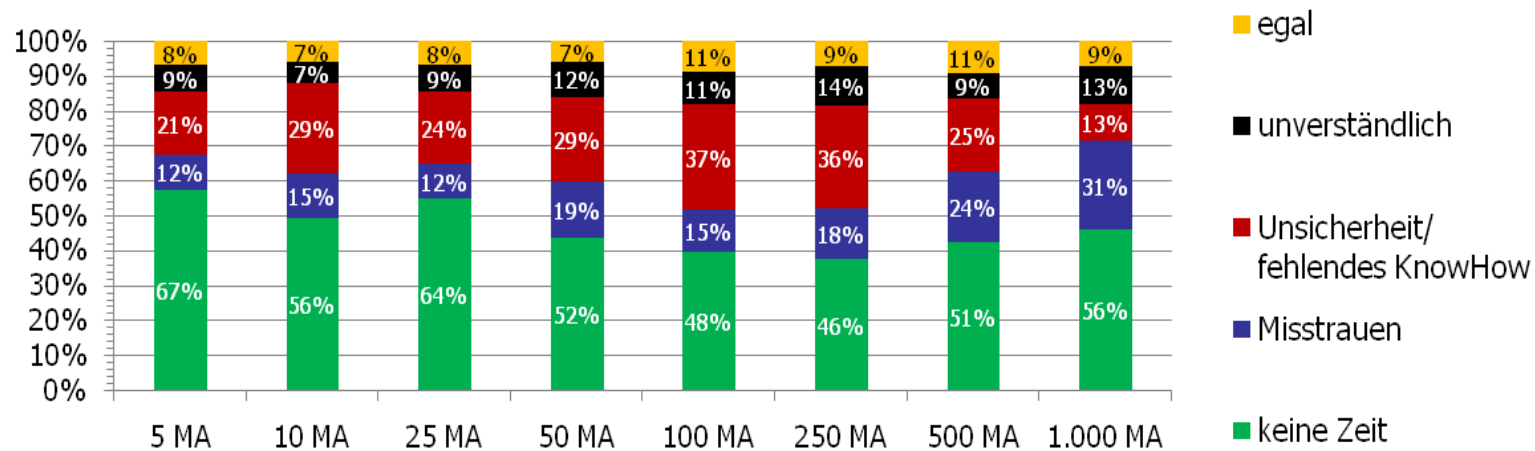
Finden User-Awareness Schulungen statt?



Tendenzen:

- kleinere Unternehmen haben kein umfassendes Schulungskonzept
- in größeren Unternehmen: Wahrnehmung als willkommene Abwechslung
- Ohne klare Richtlinien besteht die Gefahr von Desinteresse

Warum halten sich User nicht an die Vorgaben/Richtlinien?



Tendenzen:

- Mitarbeiter fühlen sich überwacht
- Die User fühlen sich von Vorgaben wie "Öffnen Sie keine unbekanntes E-Mail-Anhänge" für dumm verkauft.
- In konkreten Fällen fühlen sie sich allein gelassen (Hoaxes, Rechner langsam, Programmabstürze, sporadische Probleme, ...)

Zusammenfassung:

- Eingeschränkte Awareness verhindert ganzheitliche Betrachtung von IT Projekten – fixiert auf Kernfunktion.
 - Beispiel Mail-Server
- Mentalität: Ignorieren von Risiken und Delegieren von Verantwortung
 - Belegfrage: Ist ihr mobiles Endgerät verschlüsselt ?
- Mehrwert durch gelebte IT Security (adäquaten Standarts)
 - Kostensenkung durch effiziente und vereinfachte Administration
 - Zugang zu neuen Themen/Märkten durch Glaubwürdigkeit
 - Vermeidung verborgener Kosten

- Die Hemmschwellen für die Einführung von Maßnahmen hinsichtlich der Organisationsverpflichtung abbauen, indem die Brücke zwischen einem schrittweisen Start und den komplexen Standards wie den BSI- und ISO-Vorgaben geschlagen werden kann.
- Klare Definition der Verantwortungsbereiche und Zuständigkeiten:

Management Awareness

Organisatorische, rechtliche und strategische Detaillierung

IT-Management Awareness

Rechtliche und technische Detaillierung

User Awareness

Security-Awareness unter Einbezug der Mitarbeiter auf Basis klarer Vorgaben aus den Leitungsebenen



Anwenderzentrum IT Security Hochschule Regensburg

- Profil/Rolle
 - unabhängige, marktübergeordnete Ansprechstelle
 - Kompetenz und Innovation
 - Technologie Transfer

- Ziele
 - Hemmschwellen abbauen: schrittweiser Start mit Fahrplan in Richtung komplexer Standards
 - Erstversorgung an Beratung, Lösungen und Veranstaltungen
 - Weiterversorgung durch zertifiziertes Partnernetzwerk
 - Entwicklung neuer Lösungen und Tools im Bereich Awareness

- Kostengünstiger Einstieg für Unternehmen (EU Förderung)
- Nachhaltiger und Standard-konformer Lösungsweg
(Investitionssicherheit)
- Qualitätsgesicherte Lösungen
- Zertifizierte Partner
 - aus dem Umfeld der strategischen Partnerschaft IT Security

Netzwerk / Finanzierung



Universität Regensburg

Re-CIS innerhalb der Wirtschafts-
informatik in der Fakultät für
Wirtschaftswissen-
schaften

Universität Passau

ISL als Einrichtung der Juristischen
und der Fakultät für Informatik
und Mathematik



**Bündelung heterogener
Kompetenzen in
Ostbayern**

A-CIS Anwender-
Zentrum und
funktionale Sicherheit

Fachhochschule Regensburg

IT-Inkubator und
Netzwerk von
regionalen Partnerunternehmen

**Strategische Partnerschaft
IT-Sicherheit**




**Europäischer Fonds für
regionale Entwicklung (EFRE)**



Anwenderzentrum IT Security

- Teilnahme an Studie
- Kontakt
- www.azitsec.de



Vielen Dank für Ihre Aufmerksamkeit