

Strukturierte Informationssicherheit

Was muss getan werden – ein kurzer Überblick.

Donnerstag, 16.Juli 2009

- Einführung -

Informationssicherheit braucht ein Konzept

Regelmäßig anzutreffen: Pseudo-Sicherheit



Beispiel Notebooks: Dran gedacht?

- Notebooks arbeiten ohne schützende Firmen-Firewall.
- Sie werden viel transportiert, sind sehr mobil.
- Sie kommunizieren mit fremden Netzwerken über unsichere Verfahren.
- Die Benutzer haben oft Administrator-Rechte.
- Können ziemlich einfach geklaut oder zerstört werden...
- Werden im Sicherheitskonzept oft vergessen.



Sicherheitskonzept? Welches Sicherheitskonzept?

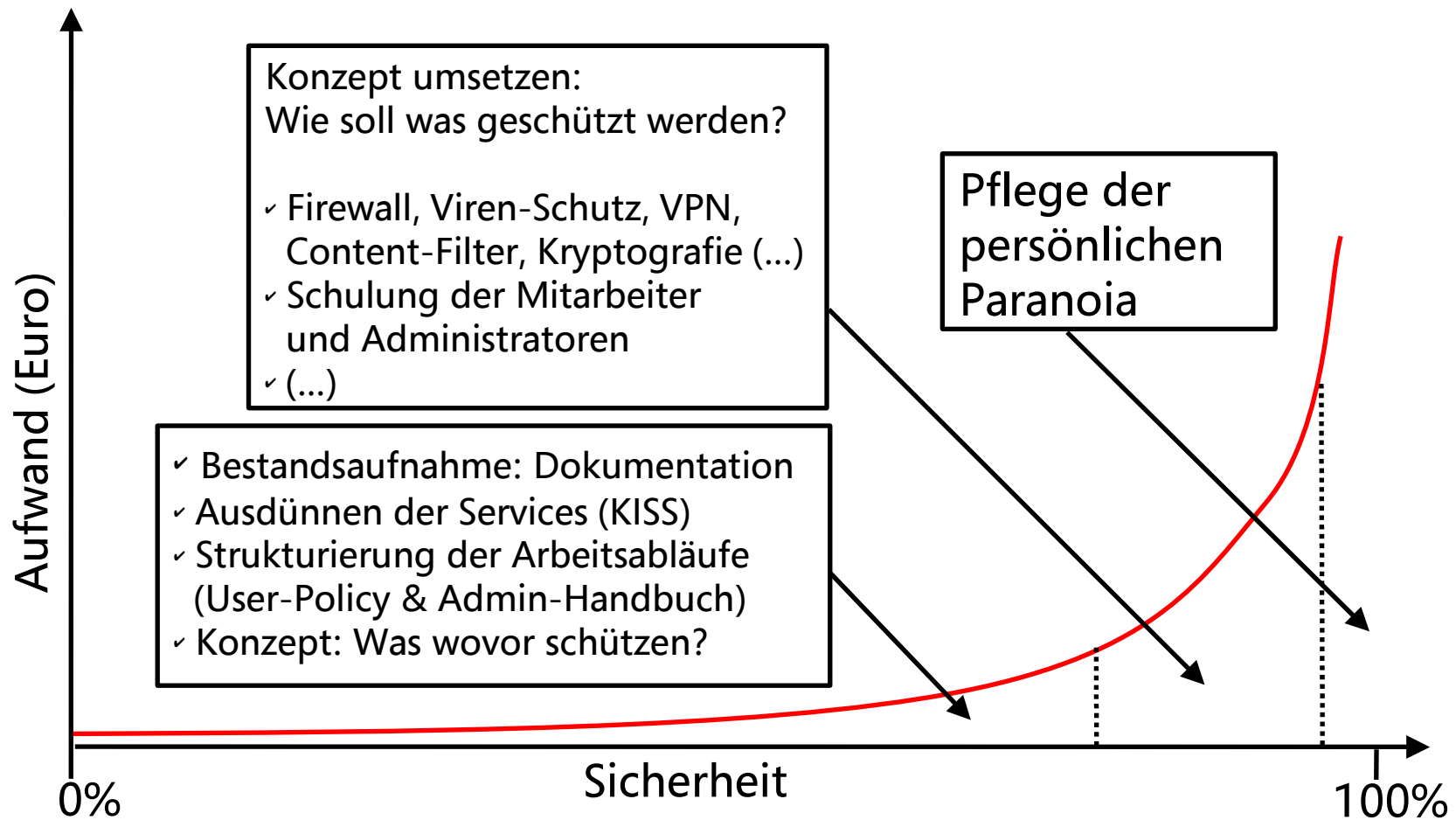
Was ist das Ziel unserer Anstrengungen?

- Erreichen eines angemessenen Sicherheitsniveaus mit möglichst geringem Aufwand!
 - ✓ Effektivität aller Maßnahmen
 - ✓ Verhältnismäßigkeit der Investitionen
 - ✓ Unabhängigkeit von externen Dienstleistern
 - ✓ Einfache Umsetzung
 - ✓ Nachhaltigkeit
 - ✓ Orientierung an Bedürfnissen und Prozessen im Unternehmen - nicht umgekehrt!

Willkommen in der Realität

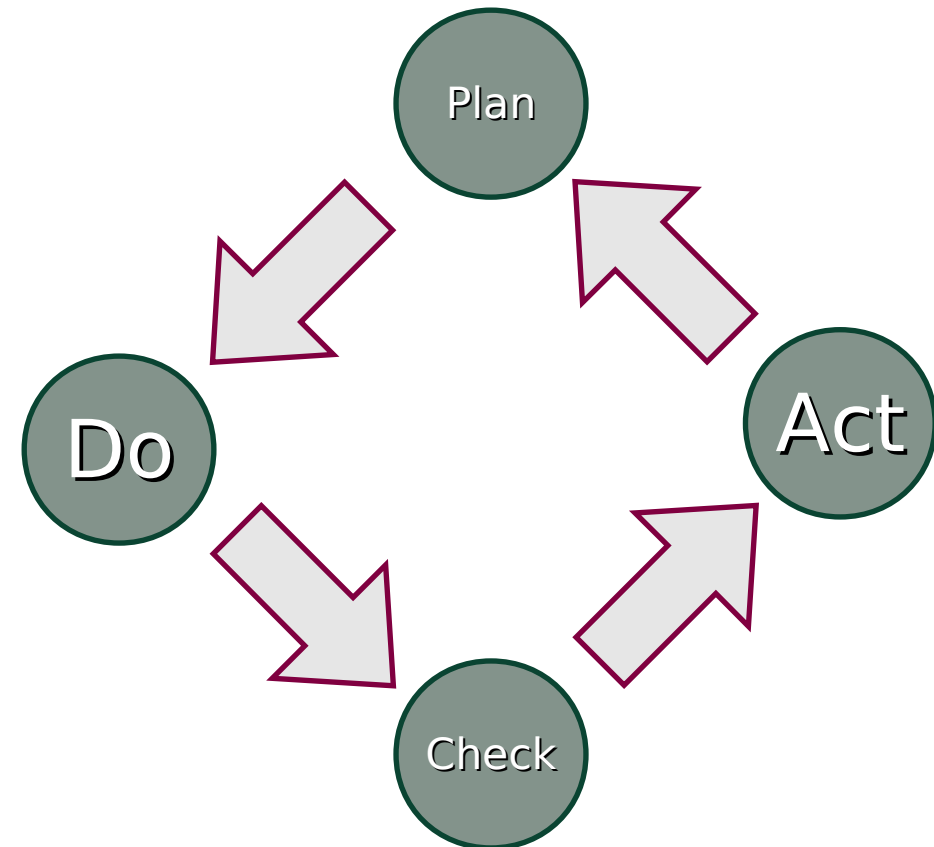
- Informationssicherheit ist mehr als die Installation einer Firewall.
- Informationssicherheit betrifft alle Teile eines Unternehmens.
- Informationssicherheit kann nicht auf den Schultern einiger weniger Personen (den Administratoren bzw. den Sicherheitsbeauftragten) abgeladen werden.

Ziel: So wenig wie möglich, so viel wie nötig!



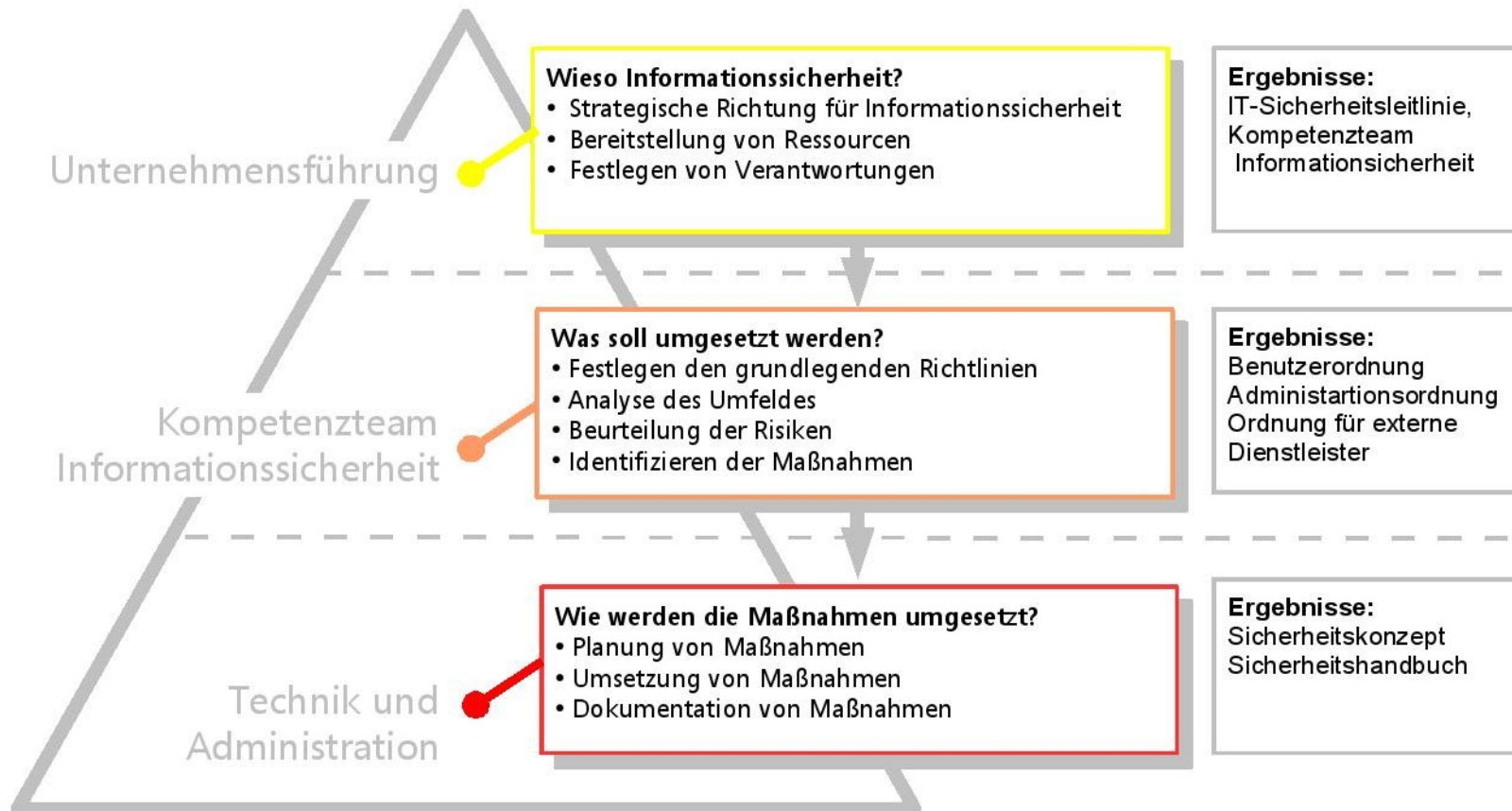
Ziel: Effektivität und Angemessenheit!

- Jede Sicherheitsmaßnahme kostet Geld: Anschaffung, Installation, Betrieb, Updates ...
- Deshalb: So wenig wie möglich und so viel wie unbedingt nötig für Informationssicherheit tun!
- Zielgerichtet planen und umsetzen, überprüfen und anpassen: Ein strukturiertes Vorgehen spart Geld, Zeit und Nerven!



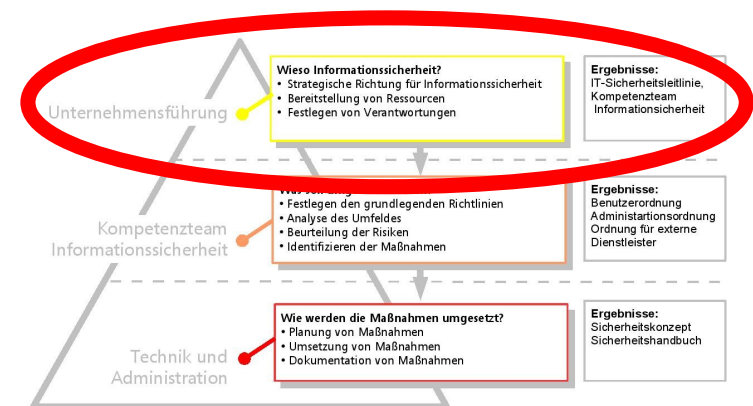
- Strukturierte Sicherheit -
Wie funktioniert es?

Unerlässlich: Top-Down-Vorgehen



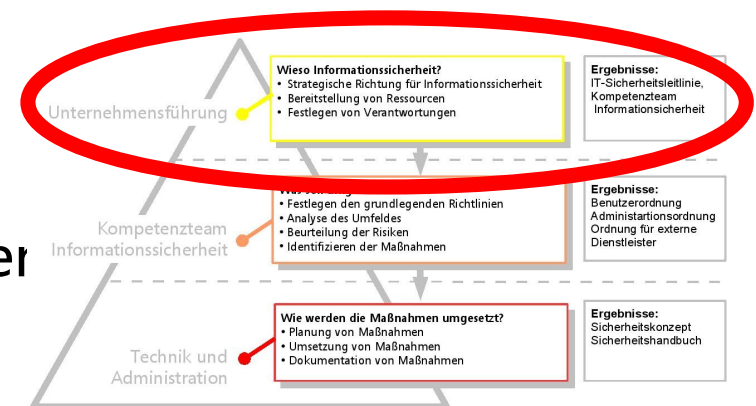
Die Leitungsebene: Vorgaben sind gefordert

- Informationssicherheit hinterlässt Spuren in der Technik und der Organisation. Nicht zuletzt berührt sie Haftungsfragen (Straf- und Zivilrecht). **Deshalb ist Informationssicherheit Chefsache.**
- Die Leitungsebene muss dafür Sorge tragen, dass IT-Security in der Firma verankert wird. Dafür müssen geeignete organisatorische Strukturen etabliert und angemessene Ressourcen eingeplant werden.
- Die Leitungsebene muss eindeutig zur Informationssicherheit Stellung nehmen. Dies geschieht in einer schriftlich fixierten Leitlinie, die das Fundament zur Etablierung einer funktionierenden Informationssicherheit ist.



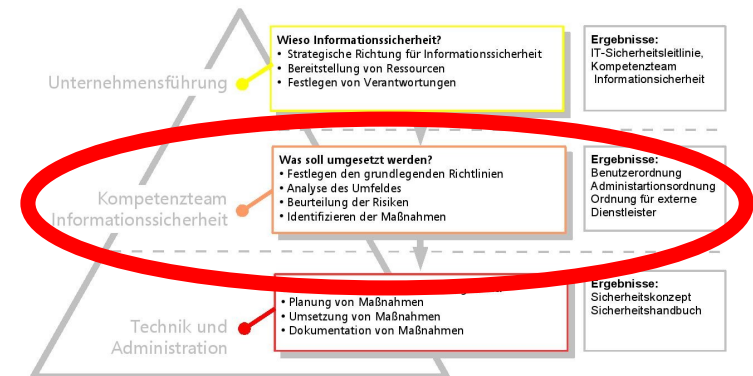
IT-Sicherheitsleitlinie

- Dieses Papier wird vom Vorstand erarbeitet und vom Vorstand veröffentlicht.
- In ihm bringt der Vorstand die Notwendigkeit eines sicheren Umgangs mit Informationen zum Ausdruck, benennt die Ziele der Informationssicherheit und legt konkrete Verantwortlichkeiten fest.
- Inhalt:
Was soll erreicht werden?
Wer ist für was verantwortlich?
- Umfang:
eine bis maximal zwei DIN-A4-Seiter



Kompetenzteam Informationssicherheit

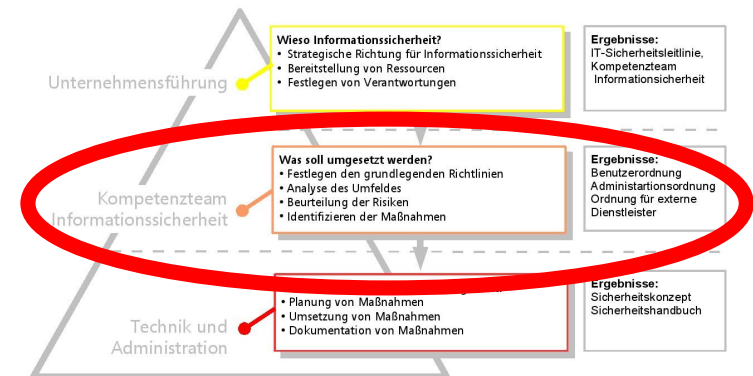
- Das Kompetenzteam Informationssicherheit wird vom Vorstand berufen. Hier sind verschiedene Kompetenzen gebündelt: Vorstand, Administration, Datenschutzbeauftragter, ein Vertreter der Mitarbeiter und ggf. externe Experten
- Das Gremium ist dafür verantwortlich, ein angemessenes Sicherheitskonzept zu erarbeiten und dieses in regelmäßigen Abständen zu überprüfen (Informationssicherheit muss leben!).
- Das Konzept wird u.a. in Form von Policies verabschiedet.



Policies: Grundgesetze für die Firma!

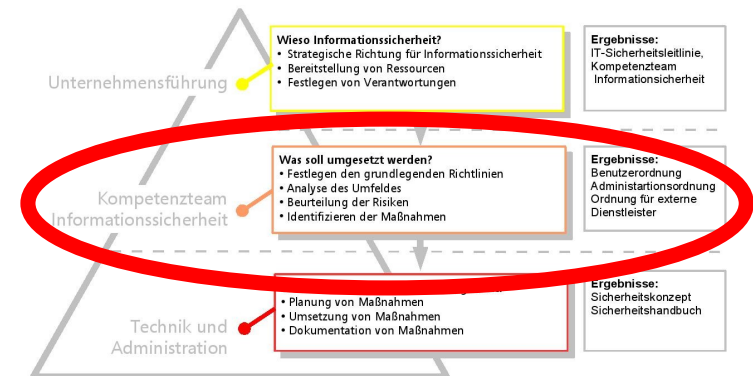
- Die Policies werden vom Kompetenzteam erarbeitet und vom Vorstand gebilligt.
- Sie haben den Charakter eines Grundgesetzes: kurz, knapp, generell gehalten und sehr statisch.
- Die folgenden Policies sollten erarbeitet werden:

- ✓ Benutzerordnung
- ✓ Benutzerordnung für externe Dienstleister
- ✓ Administrationsordnung



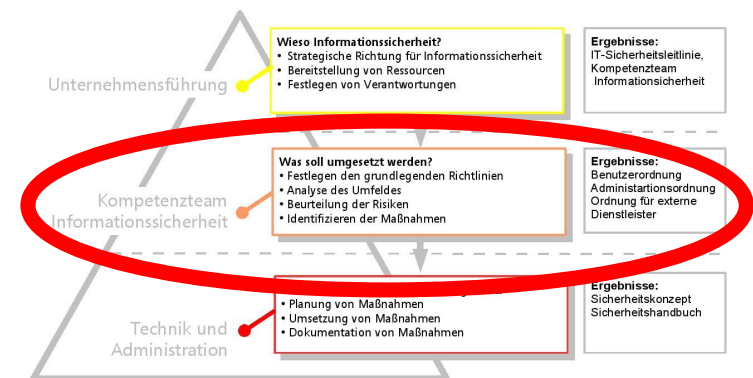
Unabdingbar: die Policy „Benutzerordnung“

- In ihr wird festgelegt, was die Mitarbeiter in der IT-Infrastruktur tun dürfen und was verboten ist.
- Außerdem werden Vorgaben des Datenschutzes (Erhebung personenbezogener Daten durch Server, Firewall etc.!) und des Telemediengesetzes durch die hier getroffenen Regelungen erfüllt.
- Umfang:
maximal fünf DIN-A4-Seiten



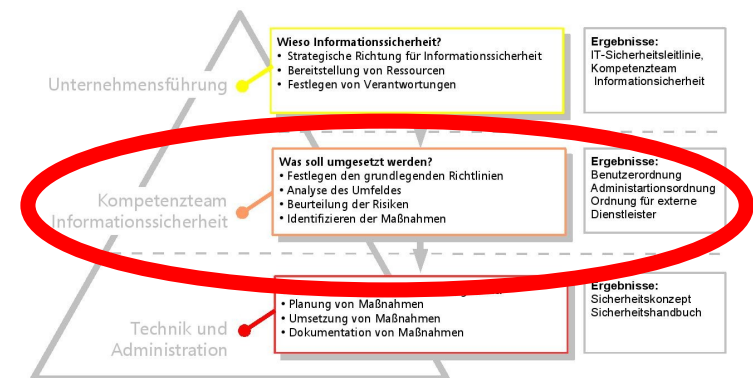
Wichtig: Policy für externe Dienstleister

- Da externe Dienstleister Geräte mit der IT-Infrastruktur koppeln bzw. Geräte in die IT-Infrastruktur einbringen, sollten auch hier verbindliche Vorgaben über diese Geräte und zum Verhalten der Mitarbeiter der Dienstleister getroffen werden.
- Auch hier gilt:
kurz, knapp, generell gehalten
- Umfang:
maximal fünf DIN-A4-Seiten



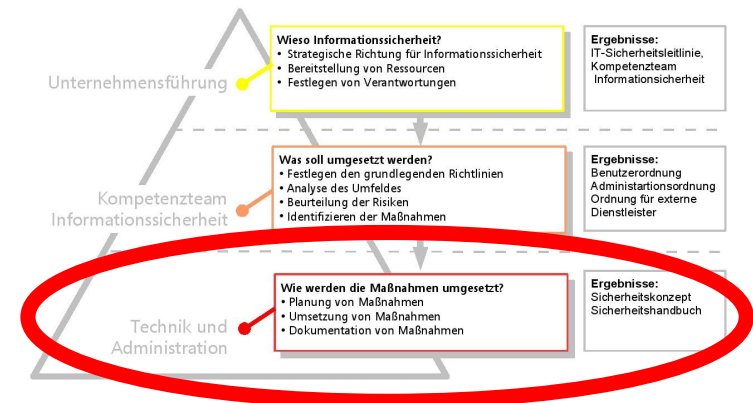
Wichtig: Administrationsordnung

- Die Administrationsordnung wird von den Administratoren erarbeitet und vom Kompetenzteam Informationssicherheit und dem Vorstand gebilligt.
- In ihr werden Vorgaben für das Administrieren der IT-Infrastruktur und der Zusammenarbeit unter den Administratoren getroffen.
- Genau wie die Benutzerordnung ist die Administrationsordnung mit dem Grundgesetz vergleichbar: kurz, knapp, generell gehalten
- Umfang:
maximal fünf DIN-A4-Seiten



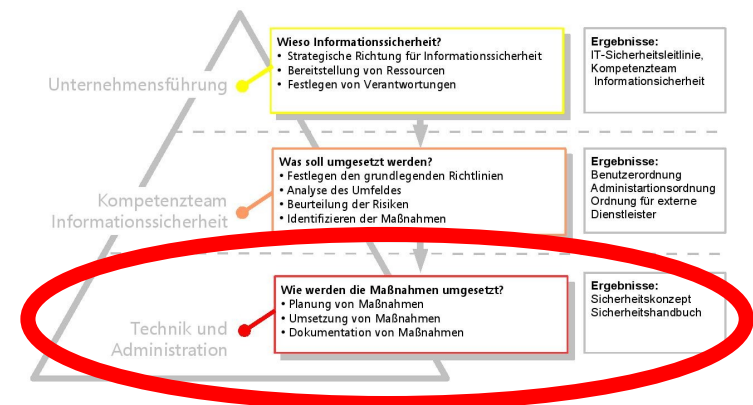
Administration: Umsetzen des Konzepts

- Die Administration muss die Vorgaben zur Informationssicherheit technisch umsetzen, indem sie den Aufbau und die Konfiguration der IT-Infrastruktur entsprechend gestaltet.
- U.a. muss sie für die Benutzer Handlungsanweisungen erarbeiten, die den „richtigen“ Umgang mit der IT-Infrastruktur in konkreten Fällen regelt.
- Diese Anweisungen sollten in einem Sicherheits-Handbuch gesammelt werden.



Flexibel & lebendig: Sicherheitshandbücher

- Benutzer und Administratoren benötigen konkrete Vorgaben, wie wichtige oder kritische Arbeitsschritte durchgeführt werden müssen.
- Diese Handlungsanweisungen werden an (virtuellen) Orten gesammelt:
 - ✓ Sicherheitshandbuch für Benutzer
 - ✓ Sicherheitshandbuch für Administratoren
- Dieses Handbuch ist sehr flexibel: Administratoren entwerfen oder aktualisieren Handlungsanweisungen bei Bedarf, das Kompetenzteam setzt sie in Kraft



- Los geht's! -

Was muss getan werden?

Die Arbeitsschritte in der Übersicht



1. Phase: Aufbauen von Strukturen

Analyse der Strukturen im Unternehmen und Erarbeiten eines geeigneten Vorgehens: „Kennenlernphase“.

KP

Erarbeiten der Unternehmenleitlinie zur Informationssicherheit und Einrichtung eines Kompetenzteams

SL

2. Phase: Definieren von Richtlinien

Erarbeiten der Benutzerordnung

BO

Erarbeiten der Administrationsordnung

AO

Erarbeiten der Benutzerordnung für
externe Dienstleister

BE

3. Phase: Risikobewertung

SA

Strukturierte Analyse des Unternehmens

RA

Identifizieren und bewerten von Risiken
(Risk Assessment)

4. Phase: Planung und Umsetzung

PM

Identifizieren und Planen von
Maßnahmen

UM

Umsetzen der Maßnahmen

5. Phase: Überprüfen und Verbessern

UV

Überprüfen und Verbessern von
Maßnahmen

- Was können wir für Sie tun? -
Kontaktieren Sie uns!

