



Zukunft der Unternehmenssicherheit. Zehn Thesen zur Entwicklung der Informationssicherheit.

Dr. Eberhard von Faber

Dokumentation - keine Vortragsfolien.

Die beim Vortrag verwendeten Folien weichen ab.

These 1

In der Mainframe-Ära bedeutet Security „Abschirmen“. Im Zuge von Client-Server-Architekturen und dem Internet wurde die Verteidigungsstrategie angepasst. Immer mehr Technik für die IT-Sicherheit wurde entwickelt und installiert.

Was kommt 2007+? Alle Technologien bleiben wichtig. Security entwickelt sich jedoch zu einer ganzheitlichen Disziplin und einem strategischen Erfolgsfaktor. Entsprechend ändern sich Aufgabenbereich und Arbeitsweise des Security-Managers.

These 2

Sicherheit ist in aller Munde. Und doch werden die Ausgaben immer stärker hinterfragt. IT-Security braucht seinen eigenen Business-Case.

Was ist notwendig? Die Verantwortlichen müssen u.a. ihre Sicherheitsstrategie genau beschreiben und dann kontinuierlich und fast pedantisch dokumentieren, wie sie Zustand und Fortschritt der IT-Sicherheit messen und bewerten.

Passende Formen von „Outsourcing“ helfen, Komplexität zu beherrschen und Kosten zu senken.

These 3

Es wird immer schwieriger, sichere und unsichere Produkte voneinander zu unterscheiden. Die Sicherheitsstrategie muss versuchen, die für die Abwehr der Massenattacken gebundenen finanziellen und personellen Ressourcen schrittweise freizusetzen, um andere Lücken zu schließen und individualisierte Angriffe abzuwehren.

Sicherheitslücken, Anwendungsbereiche mit höheren Sicherheitsanforderungen werden Sicherheitsstandards und Anforderungen an die Vertrauenswürdigkeit bzw. die Evaluierung durch Dritte definieren wie dies bei Zahlungsverkehrssystemen heute schon gang und gäbe ist.

These 4

Im Zuge der Globalisierung nimmt die Arbeitsteilung zu. Aus Zulieferketten werden Zuliefernetze. Entsprechend verändert sich die Informationstechnologie. Es kommt zur Öffnung der Unternehmens-IT; ehemals wohldefinierte Perimeter verschwinden.

Die Folgen? Erstens wird Multi-Layer- und verteilte Sicherheit weiterhin erforderlich sein. Weder Host- oder End-Punkt-Sicherheit, noch Netzwerksicherheit oder die Anwendungssicherheit wird allein alle Fragen beantworten. Zweitens übernehmen immer mehr (mobile) Endgeräte Funktionen als Sicherheitsanker im unabhängigen Internet. Entsprechend hoch sind die Anforderungen an das Device-Management.

These 5

Unternehmen verfügen über eine große Anzahl von Sicherheitsleistungen. Effektivität hinsichtlich Ressourceneinsatz und Wirtschaftlichkeit erfordert ein systematisches Vorgehen und ebenso umfassende wie schlankes Business- und IT-Architekturen.

Die Aktualisierung von Software sowie die Kontrolle und Anpassung von Konfigurationseinstellungen sind für sich schon eine eigene Disziplin.

Darüber hinaus müssen jedoch Informationen über sicherheitsrelevante Ereignisse gesammelt, möglichst zentral erfasst und bewertet werden. Nur dann können Unternehmen schnell und zweckmäßig reagieren.

These 6

Die Verlässlichkeit IT-gestützter Geschäfts- und Verwaltungsprozesse basiert auf dem kontrollierten Fluss von Information. Die Steuerung erfolgt anhand digitaler Identitäten. Ihre Zuweisung und Verwaltung wird zur alles entscheidenden Aufgabe.

Identitäts- und Zugriffsmanagement ist dabei mehr als ein IT-Projekt, es greift tief in die Unternehmensprozesse ein und gestaltet die Abwehr von Bedrohungen im Vordergrund, sondern die Unterstützung der Nutzer und damit die Erhöhung von Agilität und Produktivität.

Überwachung und Beweissicherung sind weitere wichtige Bestandteile.

These 7

Wissen (Know-how, Know-„Wh“) entscheidet heute den Wettbewerb. Informationssicherheit durch granulare Zugriffskontrolle und Verschlüsselung werden höhere Priorität bekommen müssen. Trotz dem werden Datenverluste Teil des normalen geschäftlichen Alltags bleiben.

Alle Implementierungen müssen mit der Konzeption von Politiken und der Klassifikation von Daten beginnen. Komplexere Lösungen sind eng mit dem Identitätsmanagement verflochten und lassen sich ebenso wenig wie diese allein auf der Ebene der IT lösen.

Langfristig wird sich Enterprise DRM verbreiten, da diese Technologie auch gegen unberechtigte Weitergabe von Informationen schützt.

These 8

Wettbewerbsfähigkeit: Anwenderunternehmen lagern IT-Services an spezialisierte Unternehmen aus, die Skaleneffekte realisieren und damit billiger produzieren können. Gleichzeitig sinken die Kosten für schlechte IT. Die Industrialisierung der IT führt auch zur Standardisierung der Module, aus denen das Kundenprodukt entsteht.

Damit übernimmt der IT-Dienstleister auch einen Teil der Verantwortung für die IT-Sicherheit. Problematisch für die Sicherheitsverantwortlichen bei den Anwendern ist das Vordringen von Konsumententechnologien und Endverbraucherprodukten in geschäftliche Systeme. Die Folge: Sie können nur einen Teil des Systems gestalten und sicher kontrollieren.

These 9

Das Internet ist ein maßgeblicher Wirtschaftsfaktor. Aber nicht allein als Medium. Die Wahrnehmung eines Unternehmens erfolgt primär über das Netz. Ihr folgt die Bewertung – vermutlich ebenfalls im Netz. Das Internet entscheidet damit über die Reputation eines Unternehmens und wird ihr bestimmen der Ursprung. Der Bezug zur Informationssicherheit? Reputation ist nur aufwändig aufzubauen, aber leicht zu verlieren. Unternehmen haben mehr „IT-Sicherheit“ ist neu definiert. Mit mehr als 20 Milliarden sind mehr Geräte als Individuen im Netz. „Trust“ ist neu definiert. Das Informationszeitalter erreicht schließlich sein Endstadium...

Bewiesene Verlässlichkeit ist ein zweiter Einflussfaktor. Regierungen und Verbände erlassen zunehmend Vorschriften zur Informationssicherheit, sie definieren Standards, fordern Kontrollen und verfügen Sanktionen. Die Gesetzgebung erobert die IT.

These 10

Heute gibt es weltweit bereits etwa eine Milliarde PCs. Die Anzahl der „intelligenten“ Geräte dürfte etwa 50 mal größer sein. Mehr und mehr dieser Geräte interagieren mit ihrer Umgebung und werden vernetzt.

Wie könnte die Entwicklung weitergehen? Unternehmen übertragen die IT- und TK-Leistungen mehr und mehr Dienstleistern und nutzen Services im Netz. Schließlich erfolgt die Speicherung und Verarbeitung überwiegend im Netz. Unternehmen haben keine IT-Abteilungen mehr. „IT-Sicherheit“ ist neu definiert. Mit mehr als 20 Milliarden sind mehr Geräte als Individuen im Netz. „Trust“ ist neu definiert. Das Informationszeitalter erreicht schließlich sein Endstadium...



Mehr als Technik!

Veränderungen bei Treibern und Hemmnissen.

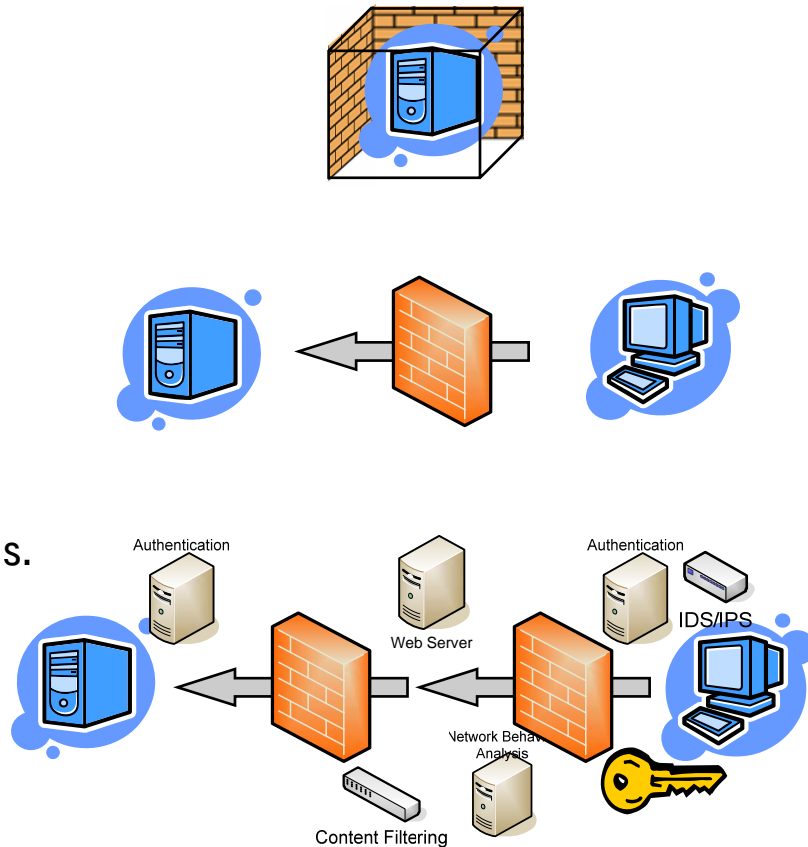
In der Mainframe-Ära bedeutete Security „Abschotten“. Im Zuge von Client-Server-Architekturen und dem Internet wurde die Verteidigungsstrategie angepasst. Immer mehr Technik für die IT-Sicherheit wurde entwickelt und installiert.

Was kommt 2007+? Alle Technologien bleiben wichtig. Security entwickelt sich jedoch zu einer ganzheitlichen Disziplin und einem strategischen Erfolgsfaktor. Entsprechend ändern sich Aufgabenbereich und Arbeitsweise des Security-Managers.

Sicherheit im Wandel. Mehr als Technik!

Wenn wir im Jahre 1997 oder 2002 wären.

- 1980er - Mainframe-Ära.
 - zentralisiert, abgeschirmt, Zeit der „IT-Elite“,
 - Security 1.0
- 1990er – PC, C/S, LANs, ... Internet.
 - Öffnung, wachsende Bedrohungen, Zeit der Verteidigung,
- 2000er – Internet, Globalisierung.
 - Networking, Cyber War, Security-Gurus.
 - DMZ, Firewall, Content Security, Filtering, VPN, Encryption, IDS, IPS, strong authentication, token, crypto ...
 - Security 2.0

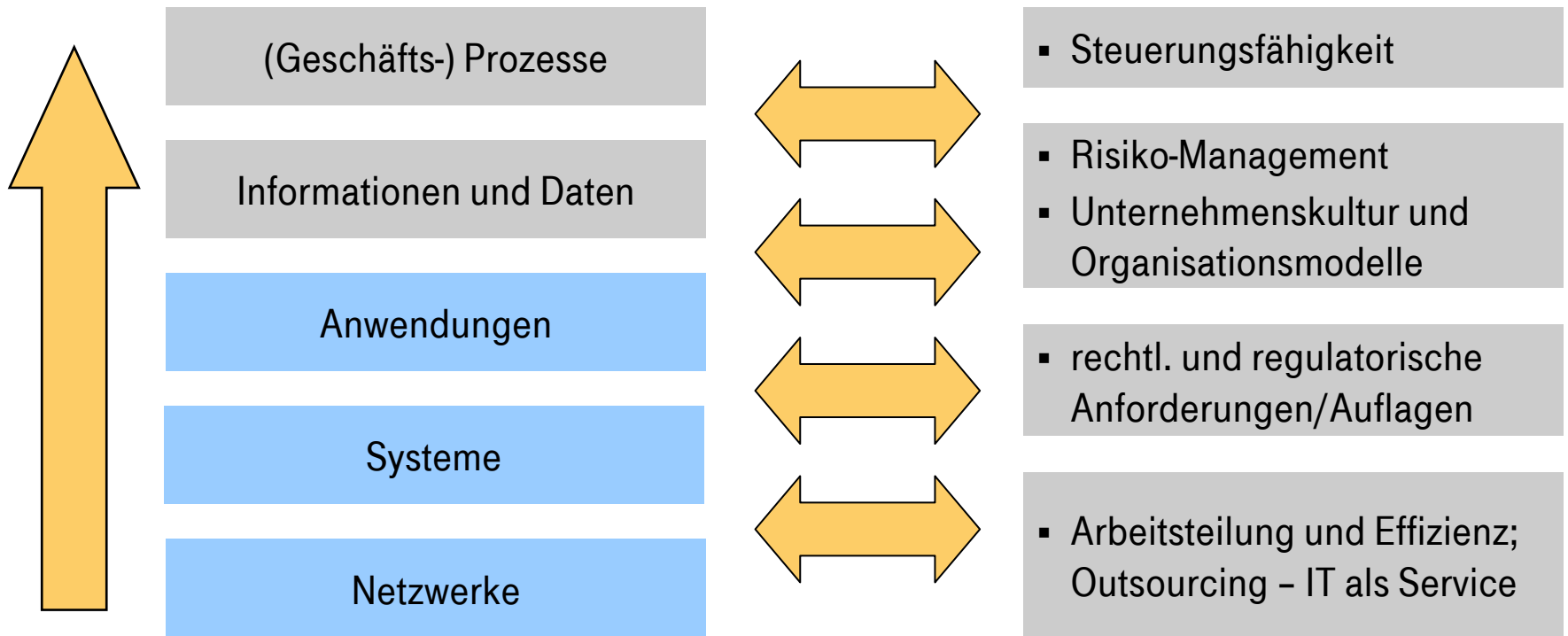


Security 3.0 - willkommen 2007+

Sicherheit im Wandel. Mehr als Technik!

Strategiewandel 2007+.

- Governance, Risks, Compliance and Efficiency.





Prozesse kontrollieren und Kosten senken.

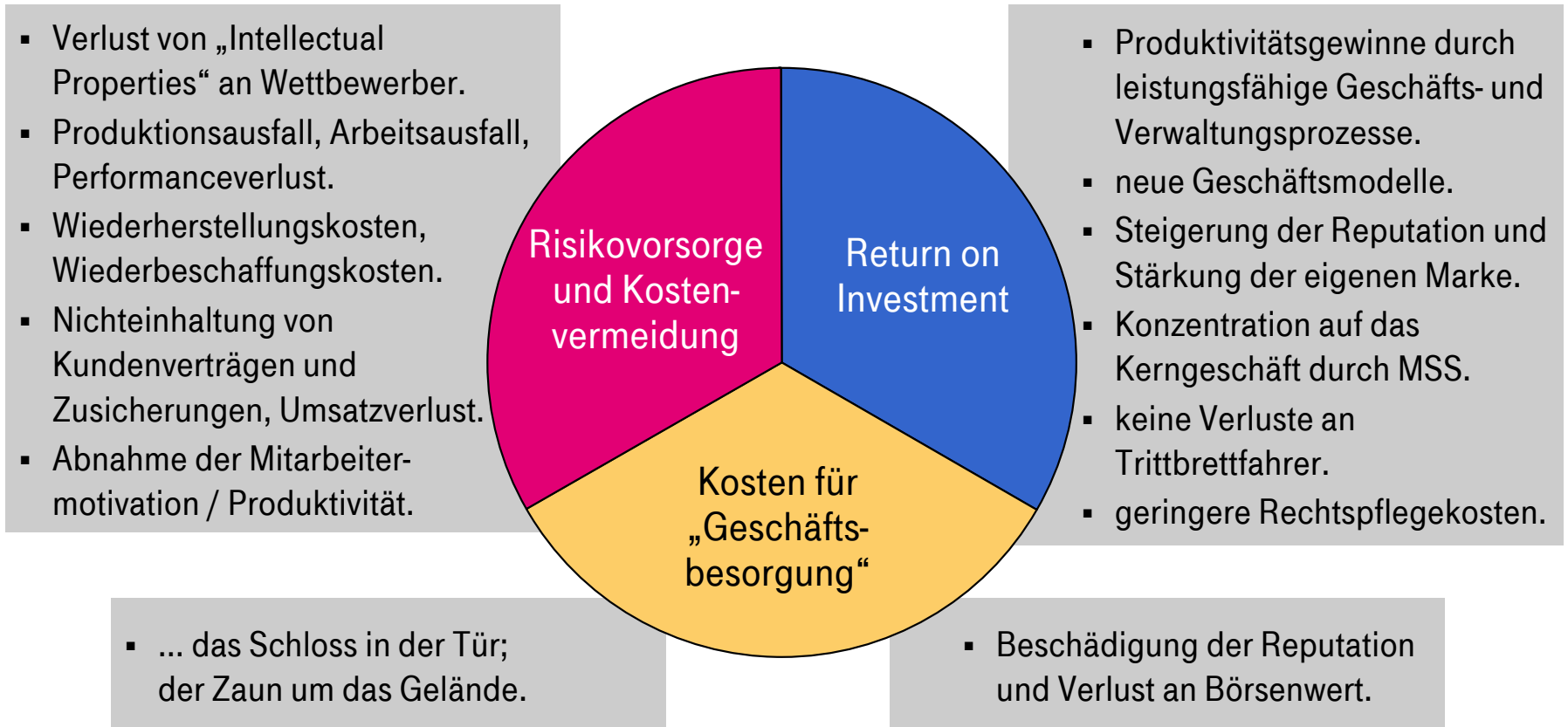
Sicherheit ist in aller Munde. Und doch werden die Ausgaben immer stärker hinterfragt. IT-Security braucht seinen eigenen Business-Case.

Was ist notwendig? Die Verantwortlichen müssen u.a. ihre Sicherheitsstrategie genau beschreiben und dann kontinuierlich und fast pedantisch dokumentieren, wie sie Zustand und Fortschritt der IT-Sicherheit messen und bewerten.

Passende Formen von „Outsourcing“ helfen, Komplexität zu beherrschen und Kosten zu senken.

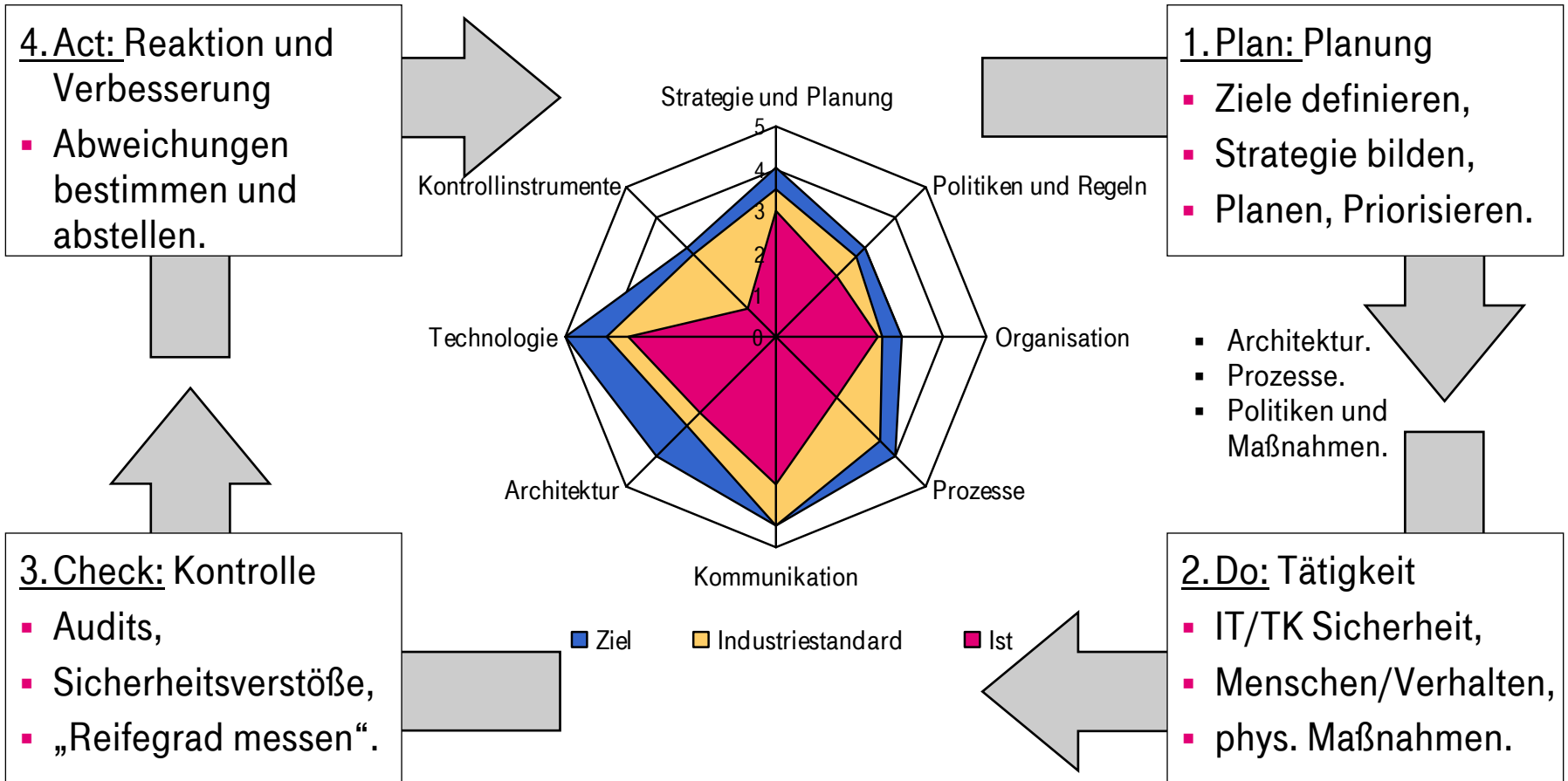
Wie rechnet sich IT-Sicherheit?

Argumente der CxOs und der Security-Anbieter.



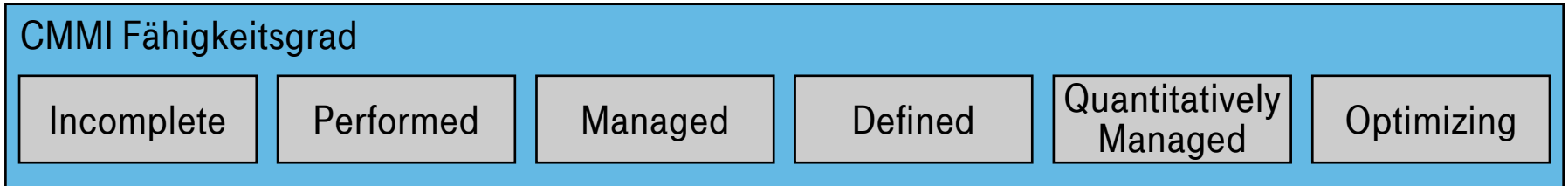
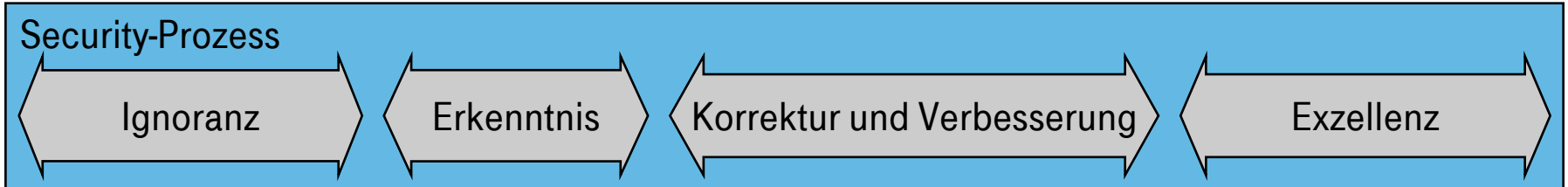
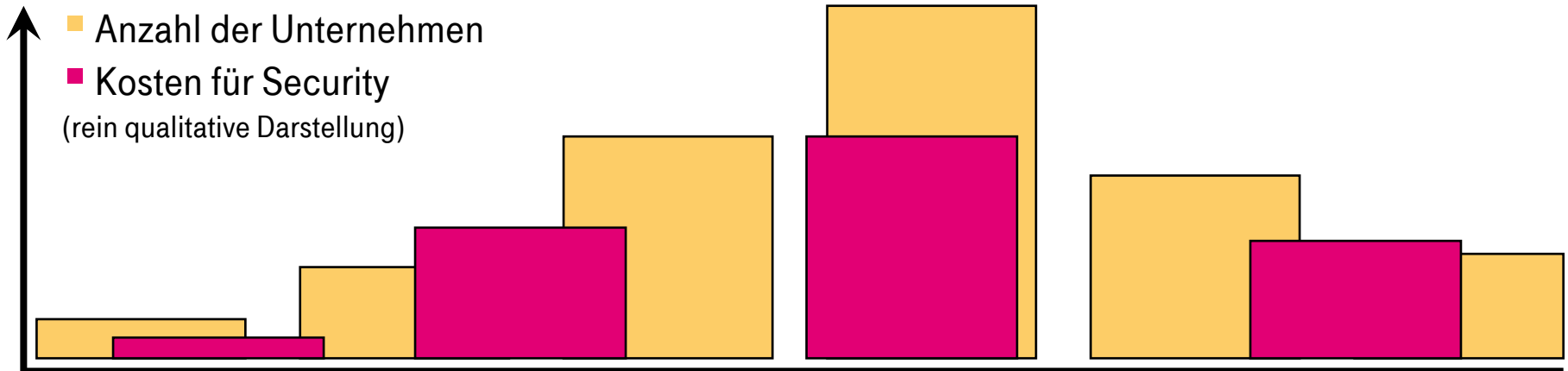
Kaizen, PDCA, KVP. „Qualitätsmanagement“.

改善



Umsetzung und Reife.

Wie weit sind die Unternehmen?





IT-Lösungen mit doppelter Unsicherheit (Mangel an Sicherheit und Vertrauenswürdigkeit).

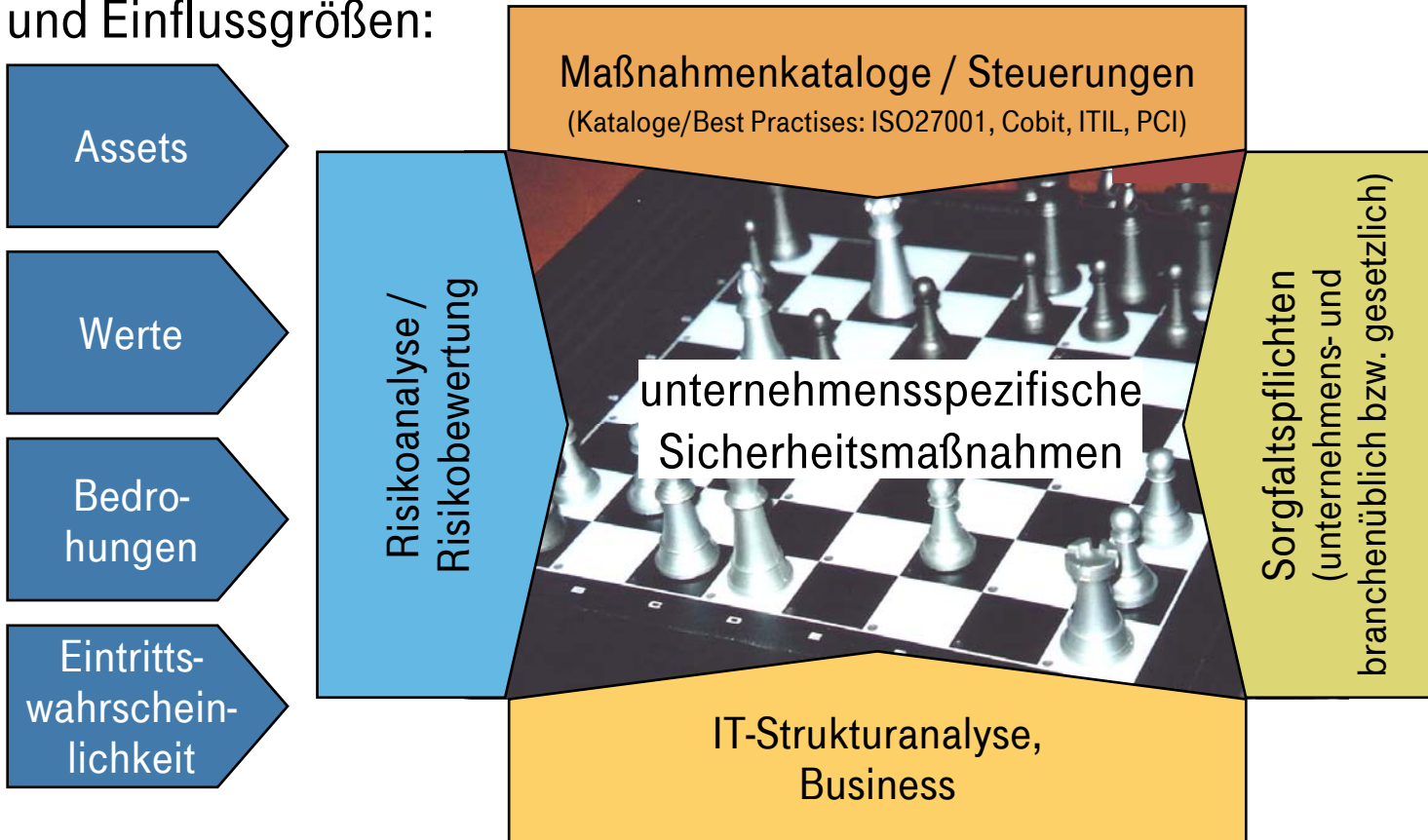
Es wird immer schwieriger, sichere und unsichere Produkte voneinander zu unterscheiden. Die Sicherheitsstrategie muss versuchen, die für die Abwehr der Massenattacken gebundenen finanziellen und personellen Ressourcen schrittweise freizusetzen, um andere Lücken zu schließen und individualisierte Angriffe abzuwehren.

Sicherheitslücken bleiben alltäglich. Anwendungsbereiche mit höheren Sicherheitsanforderungen werden Sicherheitsstandards und Anforderungen an die Vertrauenswürdigkeit bzw. die Evaluierung durch Dritte definieren wie dies bei Zahlungsverkehrssystemen heute schon gang und gäbe ist.

Welche Sicherheitsmaßnahmen sind nötig?

Rolle von Risikoanalyse und „Best Practises“.

Prozess und Einflussgrößen:





Deperimetrisierung und Device-Schwemme.

Im Zuge der Globalisierung nimmt die Arbeitsteilung zu. Aus Zulieferketten werden Zuliefernetze. Entsprechend verändert sich die Informationstechnologie. Es kommt zur Öffnung der Unternehmens-IT; ehemals wohldefinierte Perimeter verschwinden.

Die Folgen? Erstens wird Multi-Layer- und verteilte Sicherheit weiterhin erforderlich sein. Weder Host- oder End-Punkt-Sicherheit, noch Netzwerksicherheit oder die Anwendungssicherheit wird allein alle Fragen beantworten. Zweitens übernehmen immer mehr (mobile) Endgeräte Funktionen als Sicherheitsanker im ungebändigten Internet. Entsprechend hoch sind die Anforderungen an das Device-Management.

Die Folgen.

Verteilte Sicherheit. (Mobile) Endgeräte.

Wo sollte man investieren?

Pros

Cons

Netzwerk

- transportiert alle Daten: die zentrale Stelle für kostengünstige Security

- versteht die Daten aber nicht genügend gut; und: wessen Netzwerk schützen?

Hosts (Server und Desktops)

- hier sind die Daten; die Endpunkte kann man kontrollieren, Netze nicht

- sichere Betriebssysteme sind ein Traum; Host-Sicherheit kostet schon jetzt viel

Anwendungen

- Netze öffnen Ports und selbst Hosts sind blind (Bsp.: Verschlüsselung)

- wie soll das gelingen, wenn schon einfachere Elemente fehlerhaft sind
- der Nutzer wird zur entscheidenden Schwachstelle



Komplexität beherrschen, Transparenz und Reaktionsfähigkeit verbessern.

Unternehmen verfügen über eine große Anzahl von Sicherheitslösungen. Effektivität hinsichtlich Ressourceneinsatz und Wirksamkeit erfordert ein systematisches Vorgehen und ebenso umfassende wie schlanke Business- und IT-Architekturen.

Die Aktualisierung von Software sowie die Kontrolle und Anpassung von Konfigurationseinstellungen sind für sich schon eine eigene Disziplin.

Darüber hinaus müssen jedoch Informationen über sicherheitsrelevante Ereignisse gesammelt, möglichst zentral erfasst und bewertet werden. Nur dann können Unternehmen schnell und zweckmäßig reagieren.

Sicherheit durchsetzen: „Security Operations Center“.

Security and Vulnerability Management (einschl. SIEM).

Automatisieren:

- Priorisieren, Handlung empfehlen, kontrollieren
- Filtern, Zusammenfassen und Kategorisieren
- Vereinheitlichen, Vorabfiltern und Zentralisieren

S/W-Aktualisierungen
(Schwachstellen)

Penetrieren und Testen
(Scanning u.a.)

Policy & Konfiguration
(Compliance)

Verstöße erkennen
(Log-Data, Real-Time)

die Sicherheitssysteme:

- Anti-Virus, Anti-SPAM, Web-Content-Filter, e-Business-Filter, Netzwerk-Firewalls, Personal-Firewalls, IPSEC-VPN, SSL/TLS-VPN, Host-basierte IDS/IPS, Netzwerk-basierte IDS/IPS, Vulnerability Management, Betriebs-systeme, Authentisierung, Encryption, Netzwerkkomponenten...

jeweils mit:

- Softwareversionen und Schwachstellen
- Konfigurationen und Einstellungen
- Log-Daten und Alarmen

und:

- CERT u.a. Infos
- Best Practises
- Audits etc.



Prozessgestaltung und Identitätsmanagement.

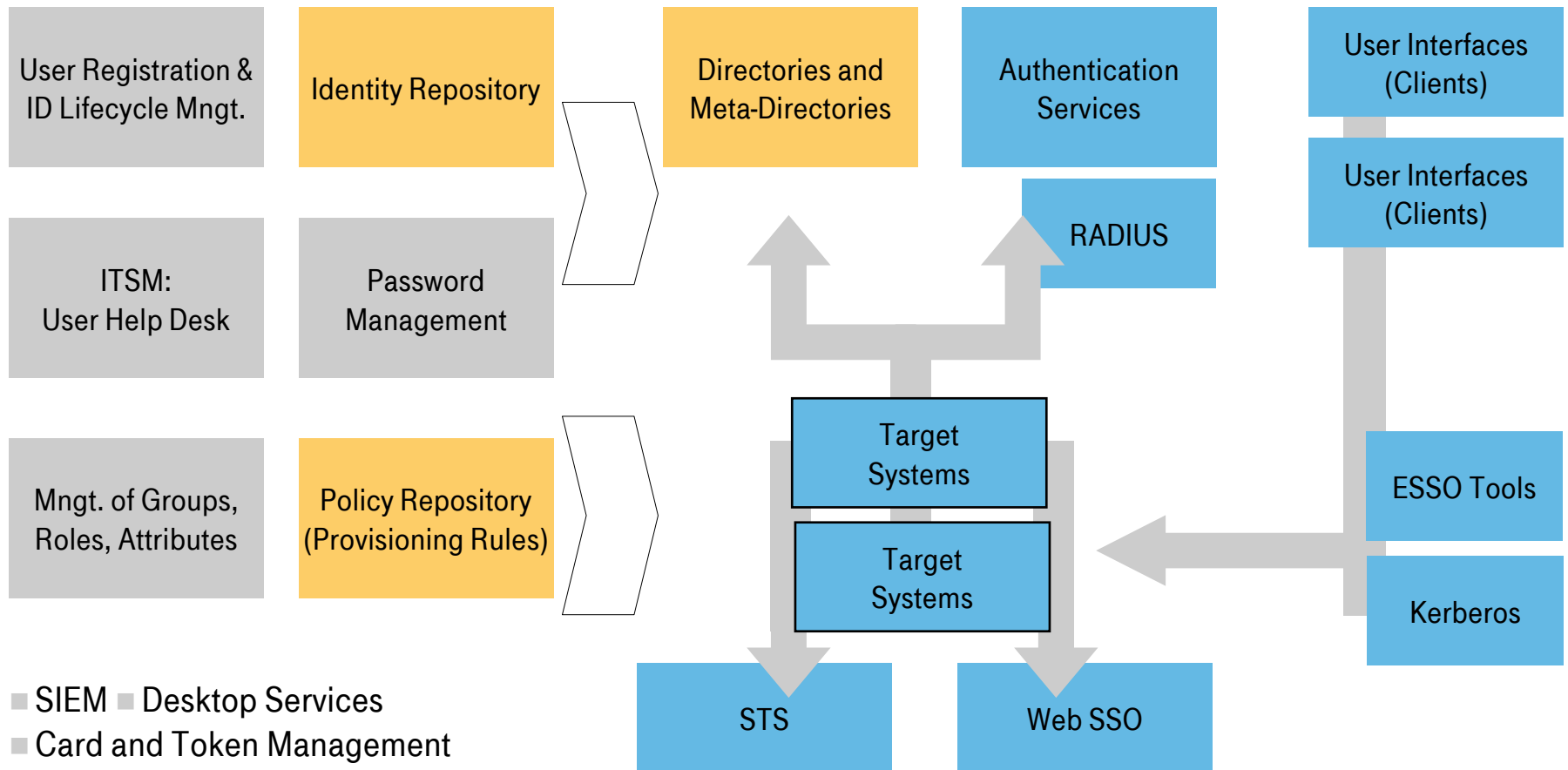
Die Verlässlichkeit IT-gestützter Geschäfts- und Verwaltungsprozesse basiert auf dem kontrollierten Fluss von Information. Die Steuerung erfolgt anhand digitaler Identitäten. Ihre Zuweisung und Verwaltung wird zur alles entscheidenden Aufgabe.

Identitäts- und Zugriffsmanagement ist dabei mehr als ein IT-Projekt, es greift tief in die Unternehmensprozesse ein und gestaltet diese mit. Auch steht nicht die Abwehr von Bedrohungen im Vordergrund, sondern die Unterstützung der Nutzer und damit die Erhöhung von Agilität und Produktivität.

Überwachung und Beweissicherung sind weitere wichtige Bestandteile.

Identity and Access Management.

Quellen? Prozesse? Architektur? AAAA technisch?





Informationssicherheit durch Zugriffskontrolle und Verschlüsselung.

Wissen (Know-how, Know-„W“) entscheidet heute den Wettbewerb.

Informationssicherheit durch granulare Zugriffskontrolle und Verschlüsselung werden höhere Priorität bekommen müssen. Trotzdem werden Datenverluste Teil des normalen geschäftlichen Alltags bleiben.

Alle Implementierungen müssen mit der Konzeption von Politiken und der Klassifikation von Daten beginnen. Komplexere Lösungen sind eng mit dem Identitätsmanagement verwoben und lassen sich ebenso wenig wie dieses allein auf der Ebene der IT lösen.

Langfristig wird sich Enterprise DRM verbreiten, da diese Technologie auch gegen unberechtigte Weitergabe von Informationen schützt.



IT wird zum Massenprodukt, Konsumenten beeinflussen IT.

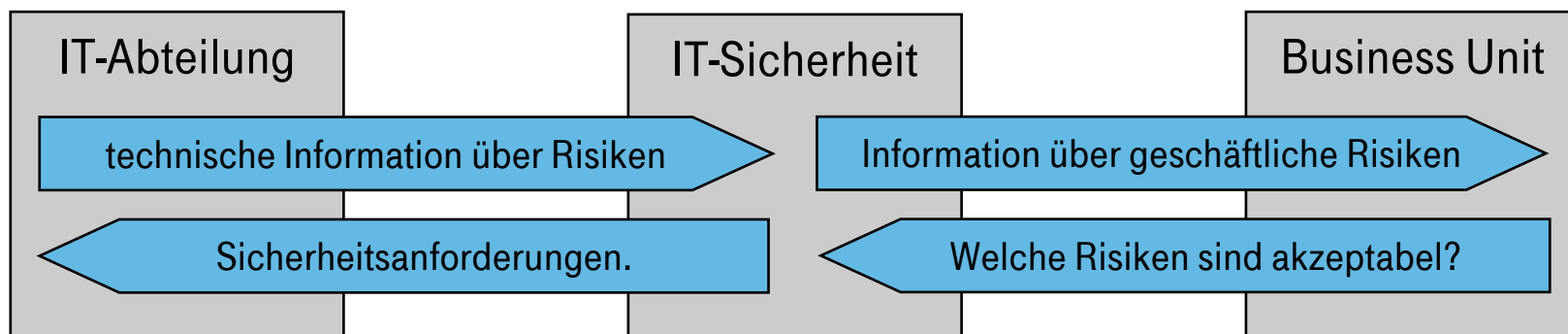
Wettbewerbsfähigkeit: Anwenderunternehmen lagern IT-Services an spezialisierte Unternehmen aus, die Skaleneffekte realisieren und damit billiger produzieren können. Gleichzeitig sinken die Kosten für schlechte IT. Die Industrialisierung der IT führt auch zur Standardisierung der Module, aus denen das Kundenprodukt entsteht.

Damit übernimmt der IT-Dienstleister auch einen Teil der Verantwortung für die IT-Sicherheit. Problematisch für die Sicherheitsverantwortlichen bei den Anwendern ist das Vordringen von Konsumententechnologien und Endverbraucherprodukten in geschäftliche Systeme. Die Folge: Sie können nur einen Teil des Systems gestalten und sicher kontrollieren.

Risiken und die Rolle der CSOs.

Industrialisierung und Konsumententechnologien.

- „CSO“: Vermittler zwischen Produktion (IT) und Anwender (BU).



- Wertschöpfungstiefe reduzieren
 - IT standardisieren
 - Skaleneffekte abschöpfen



- Einfluß der Endanwender
 - Web 2.0
 - „private“ und andere Endgeräte





Harte Faktoren in weichem Gewand. Reputation und Regulierung.

Das Internet ist ein maßgeblicher Wirtschaftsfaktor. Aber nicht allein als Medium. Die Wahrnehmung eines Unternehmens erfolgt primär über das Netz. Ihr folgt die Bewertung – vermutlich ebenfalls im Netz. Das Internet entscheidet damit über die Reputation eines Unternehmens und wird ihr bestimmender Ursprung. Der Bezug zur Informationssicherheit? Reputation ist nur aufwändig aufzubauen, aber leicht zu verlieren. Sicherheit kann sie schützen, Manipulationen beschädigen sie.

Bewiesene Verlässlichkeit ist ein zweiter Einflussfaktor. Regierungen und Verbände erlassen zunehmend Vorschriften zur Informationssicherheit, sie definieren Standards, fordern Kontrollen und verfügen Sanktionen. Die Gesetzgebung erobert die IT.



Das „Netz“ ist der „Computer“.
Daten sind „intelligent“ und „sicher“.

Heute gibt es weltweit bereits etwa eine Milliarde PCs. Die Anzahl der „intelligenten“ Geräte dürfte etwa 50 mal größer sein. Mehr und mehr dieser Geräte interagieren mit ihrer Umgebung und werden vernetzt.

Wie könnte die Entwicklung weitergehen? Unternehmen übertragen die IT- und TK-Leistungen mehr und mehr Dienstleistern und nutzen Services im Netz. Schließlich erfolgt die Speicherung und Verarbeitung überwiegend im Netz. Unternehmen haben keine IT-Abteilungen mehr. „IT-Sicherheit“ ist neu definiert. Mit mehr als 20 Milliarden sind mehr Geräte als Individuen im Netz. „Trust“ ist neu definiert. Das Informationszeitalter erreicht schließlich sein Endstadium...

Das Informationszeitalter.

1. Hälfte des Zyklus: Aufbruch und Raserei.

- 1941 Konrad Zuse stellt den ersten funktionstüchtigen Computer Z3 fertig.
- 1943 IBM-Chef Thomas Watson: „...es gibt einen weltweiten Bedarf an vielleicht fünf Computern“.
- 1964 DEC baut den Minicomputer PDP-8 für unter 20000 Dollar.
- 1976 Apple bringt den Apple I auf den Markt; Zilog entwickelt den Z80 Prozessor.
- 1980 IBM stellt den IBM-PC vor..., 1990er Internet.

heute

- rund 50 Mio. PCs in D, knapp 1 Mrd. weltweit.
- vielleicht 50× mehr „intelligente Geräte“.
- Breitbandvernetzung, Multi-Media, Unternehmensgrenzen verschwinden: value-grid durch e-SCM; e-Collaboration...

© DaimlerChrysler



Das Informationszeitalter.

2. Hälfte des Zyklus: Synergie und Reife.

bis 2015.

- Unternehmen haben keine IT-Abteilungen mehr.
- Der PC erreicht seinen Zenit. Global „Grids“ mit 10 Mio. Computer; allein 5 Mio. bei „Google“.
- 20 Mrd. „intelligente Geräte“ im Netz.

bis 2020

- Speicherung und Datenverarbeitung erfolgt im Netz. Daten sind „intelligent“ und „sicher“.
- Datenschutz (privacy) hört auf zu existieren. Alles ist verfolgbar, Identitäten sind kaum verlässlich.
- Trust ist neu definiert: communities/organizations.

bis 2025

- mehr als 100 Mrd. „intelligente Geräte“ im Netz.
- Das Informationszeitalter erreicht sein Endstadium.

Quelle: nach Steve Prentice von Gartner



Vielen Dank.

powered by
Security Management at



Dr. Eberhard von Faber
IT Sales and Solutions Security

www.t-systems.de/ict-security
info.ict-security@t-systems.com

