

Messbare Sicherheit ?

15.9.2009



Was heisst „Sicherheit“ ?

[www.wikipedia.de]

Sicherheit bezeichnet einen Zustand, der frei von unvermeidbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. Mit dieser Definition ist Sicherheit sowohl auf ein einzelnes Individuum als auch auf andere Lebewesen, auf unbelebte reale Objekte oder Systeme wie auch auf abstrakte Gegenstände bezogen.

Allgemein wird Sicherheit jedoch nur als relativer Zustand der Gefahrenfreiheit angesehen, der stets nur für einen bestimmten Zeitraum, eine bestimmte Umgebung oder unter bestimmten Bedingungen gegeben ist.Sicherheit bedeutet daher nicht, dass Beeinträchtigungen vollständig ausgeschlossen sind, sondern nur, dass sie hinreichendunwahrscheinlich sind

Was heisst „messbar“ ?



[www.wikipedia.de]

Messbar ist eine Größe, wenn es ein Messprinzip gibt, nach der sie sich messen lässt, wenn sie also innerhalb physikalischer Betrachtungsweise sinnvoll definiert werden kann, und daher insbesondere quantifizierbar ist. Dies umfasst auch alle Ansprüche der Reproduzierbarkeit des Messergebnisses.

Messbar sind **physikalische Größen**. Manche nicht physikalische Größen lassen sich auf physikalische Größen zurückführen wie Lautstärke auf Schalldruck, Farbwahrnehmungen auf die Verteilung im Lichtspektrum.

Die Ermittlung von **nicht physikalischen Größen**, wie beispielsweise die mit statistischen Methoden gewonnene Inflationsrate, der Intelligenzquotient oder die Kundenzufriedenheit, wird teilweise auch als Messung bezeichnet. Dies wird in der Regel bestritten.

....

oder Sicherheit !

Ein nur subjektiv beurteilbares Merkmal wie z. B. Schönheit (etwa einer Farbe) oder Schlauheit ist **nicht allgemein anerkannt definiert** und allein schon dadurch auch nicht quantitativ angebbar.

.....

Ist Sicherheit jetzt messbar oder nicht ?

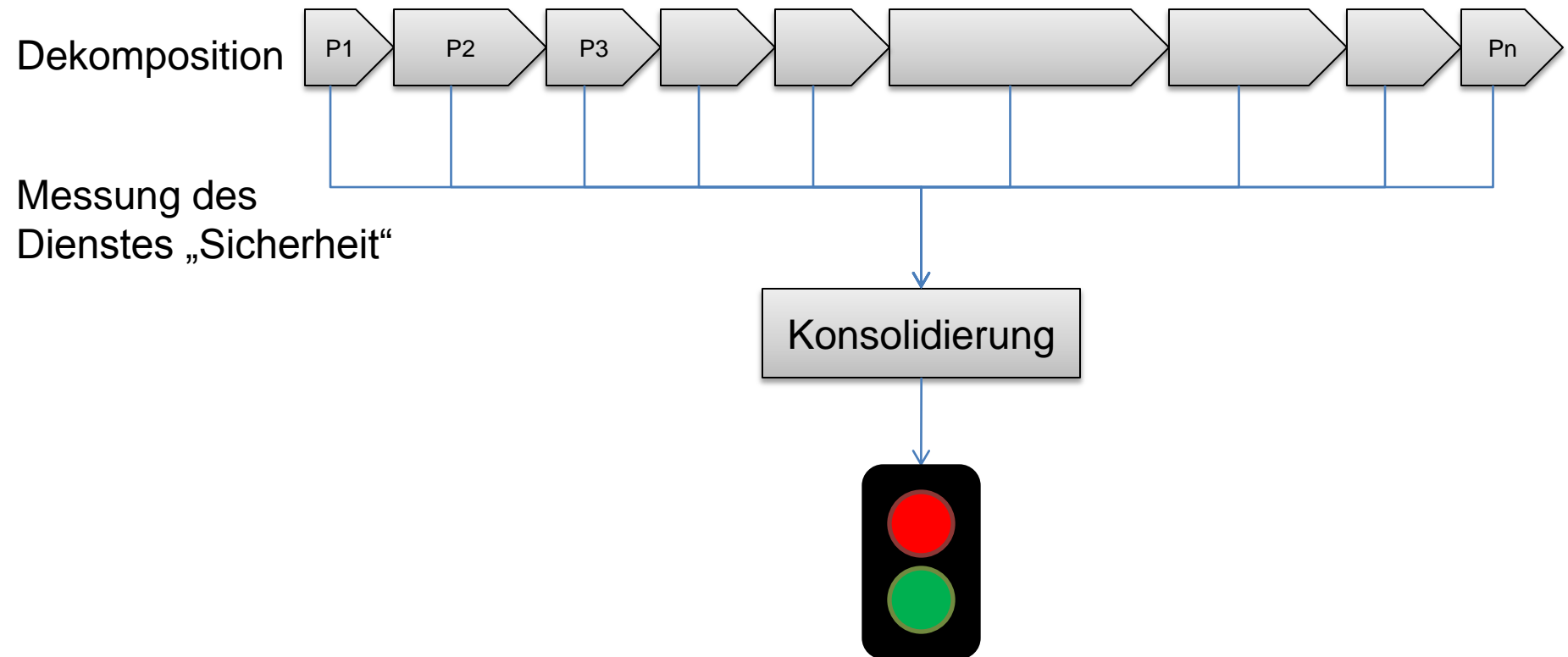
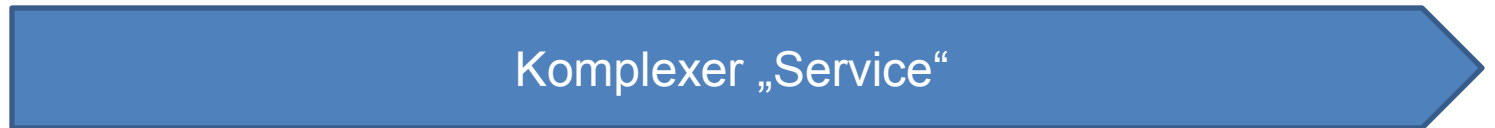
„**Sicherheit**“ ist subjektiv und ist deshalb nicht objektiv messbar.



„**Sichere Dienste**“ (Secure Services) können objektiv gemessen werden



Messung eines Sicherheits-Dienstes (SLM-Ansatz)



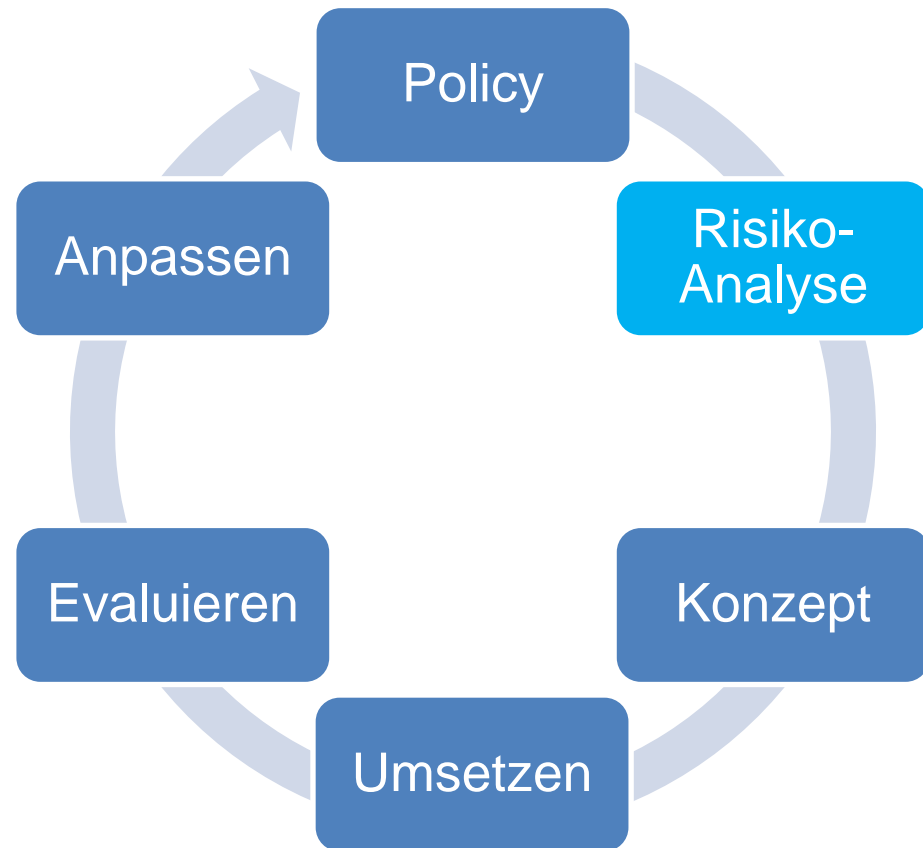
Der Standard-Ansatz

Continuous Improvement
Risiko-Analyse als Kern-Aktivität

Basis: Demingkreis:



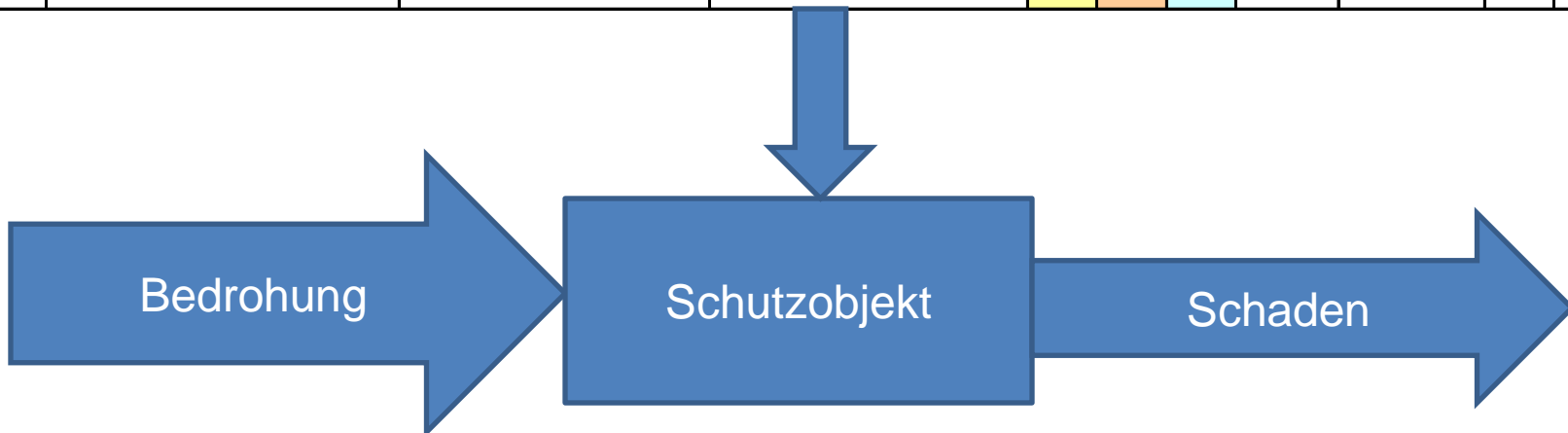
<http://de.wikipedia.org/wiki/Demingkreis>



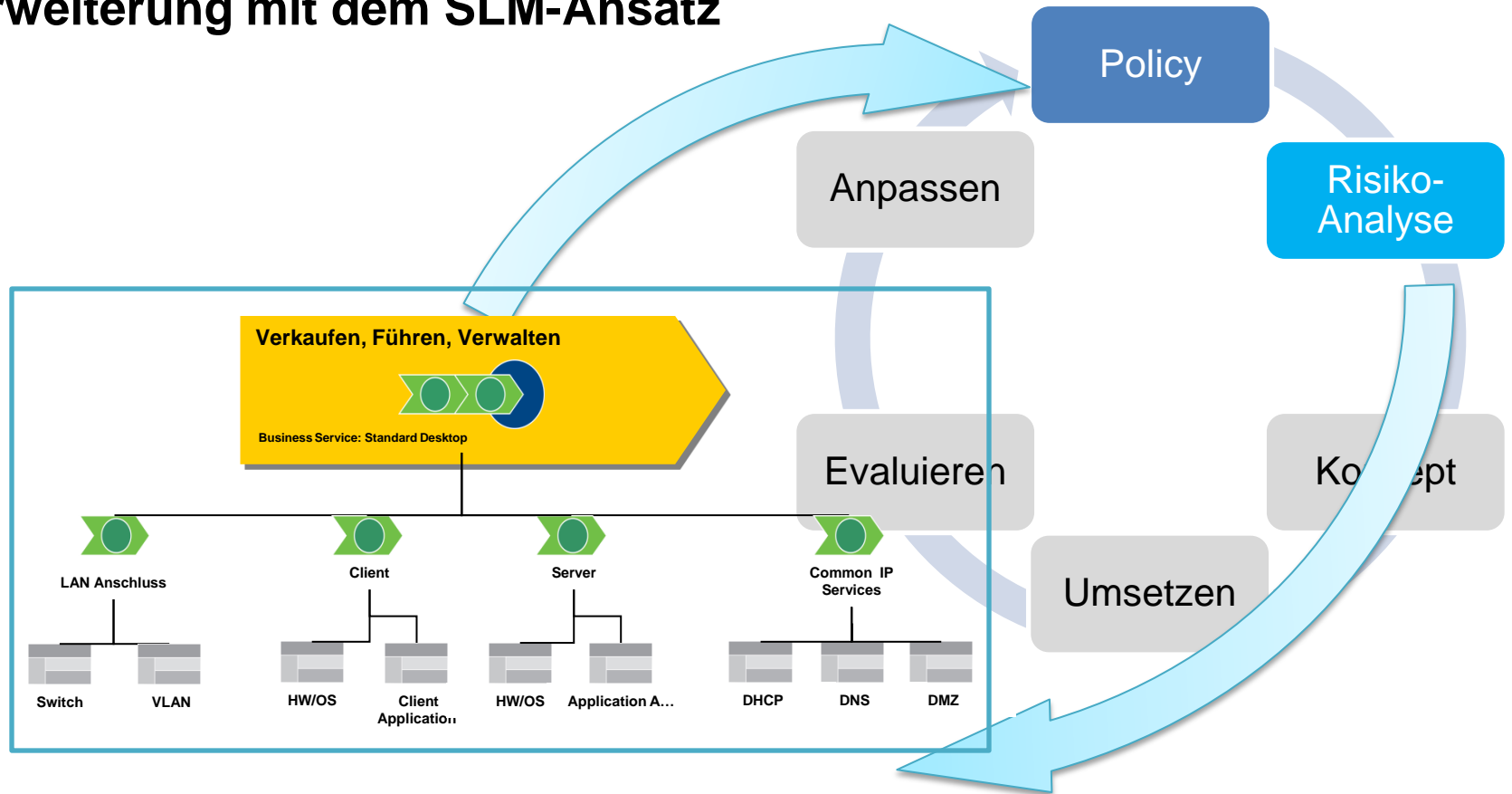
Risikoanalyse: Der traditionelle Fokus

Schutzobjekt:	<i>Web-Content (Public)</i>
Owner:	<i>Vorname, Name Telefon E-Mail-Adresse</i>

Nr.	Bedrohung		Massnahme (IST)	Impact			Schadensausmass		Eintritt 1 x in			
	Typ	Bedrohung		Verfügbarkeit	Vertraulichkeit	Integrität	Finzieller Verlust	Image/Reputationsverlust	1 - 3 Jahre	3 - 10 Jahre	10 - 30 Jahre	> 30 Jahre
27	Computer-Kriminalität	Nicht-autorisierte Veränderung von Web-Content	Zugang auf CMS mit Passwörtern geschützt	o	o	X	tief	mittel	X			



Erweiterung mit dem SLM-Ansatz



Traditionelles Sicherheits-Engineering v.s. SLM-Verfahren

Traditionelles Sicherheits-Engineering	SLM
Konzentration auf „Schutzobjekte“ (d.h. lokalisierbare Dinge)	Konzentration auf „Services“ (d.h. Prozesse und verbundene Systeme)
Ziel ist das „Verhindern“ von Schäden	Ziel ist das „Ermöglichen“ eines sicheren Dienstes
Zeigt die gefährlichen Stellen (Schutzobjekte) (punktuell) und vergleicht deren Schadenspotenzial im Prozess	Zeigt die Wirksamkeit und die Abhängigkeiten der vorgesehenen Mechanismen
Messung, Verifikation meist sporadisch (Audits)	Messung, Verifikation möglichst häufig („in Echtzeit“).

SLM-Ansatz: Bewertung

Möglichkeiten

- Ist stufengerecht einsetzbar („top-down“)
- Macht vernetzte Systeme transparent (kritische Stellen werden sichtbar)
- Zeigt die Wirkung von Investitionen im Betrieb

Grenzen

- Anwendbarkeit bei „nicht-technischen“ Diensten
- Hoher Initialaufwand für vollen Nutzen (Automatisierung)
- Messwerkzeuge nicht immer vorhanden

Danke

Paul Schöbi

paul.schoebi@cnlab.ch

+41 55 214 33 33

15.9.2009

Präsentation im Internet unter <http://www.cnlab.ch/en/company/publications.html>