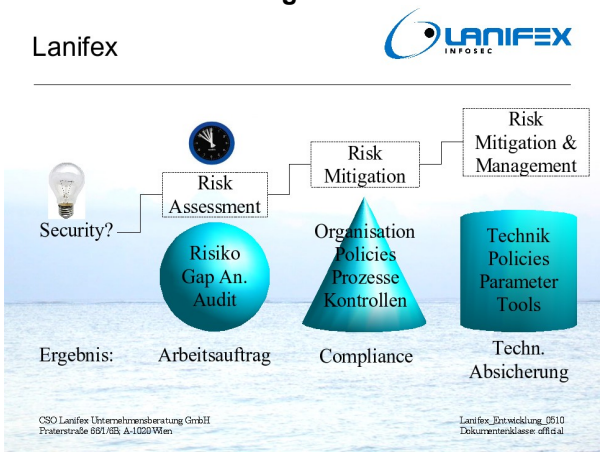
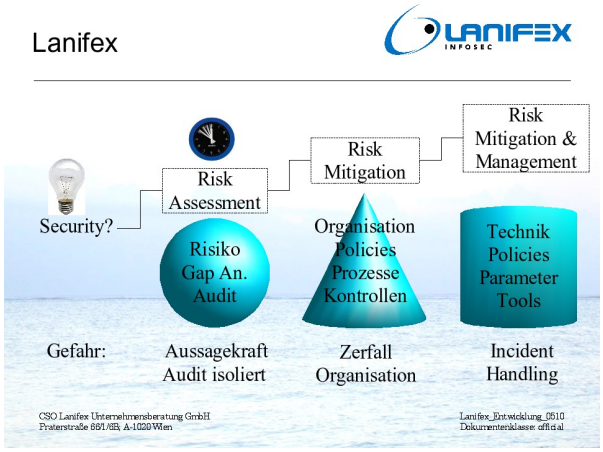
Security – Schritte zum Ziel

Wenn eine Organisation beschließt für die Security im Unternehmen mehr zu tun, dann ist immer die erste Frage:

Wo soll am Besten begonnen werden?



Viele Unternehmen fangen mit einem **Audit** an, der eine punktuelle Sicht auf die Verwundbarkeiten der Organisation und der technischen Komponenten ermöglicht. Die Aussagekraft der entdeckten Verwundbarkeiten kann aber nur im Zusammenhang mit dem **Risiko** bewertet werden. Daher sollten diese beide Punkte als Teil eines gesamten **Risiko-Assessments** durchgeführt werden, um den Arbeitsauftrag für die Organisation und für die Technik zu definieren.



Der Arbeitsauftrag versucht **bestehende Risken zu minimieren** (Risk Mitigation) und zu managen.

- **Organisatorische Maßnahmen:** Definition von Policies, in Kraft Setzen von Prozeduren und die Kontrolle.
- **Technische Maßnahmen:** So wie bei der Organisation werden auch auf der technischen Ebene Policies, Prozeduren und deren Kontrollen definiert. Tools unterstützen dieses Vorhaben auf unterschiedlichen Ebenen.

Bei der Umsetzung lauern **Gefahren**

- Über die Zeit ist ein rascher **Zerfall von organisatorischen Maßnahmen** möglich, da Security immer einen Aufwand bedeutet. Organisationen tendieren zum Weg des geringsten Widerstandes.
- Kann meine Oranisation die **Tools**, die angeschafft wurden **beherrschen** und sind sie dem Risiko **angemessen**?

Als Hilfe zu diesen beiden Themen empfiehlt sich das **zentrale Management:**

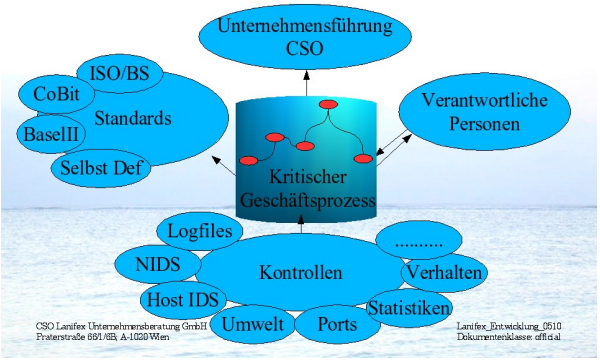
In einer Datenbank werden die **kritischen Geschäftsprozesse** mit den zugehörigen Ressourcen abgebildet. Dazu werden die Kontrollen definiert, die sich nach einem bestehenden Standard richten. Die verantwortlichen Personen werden regelmäßig vom System gefragt, ob die organisatorischen Massnahmen eingehalten werden. Die Unternehmensführung und der „Chief Security Officer“ sehen Abweichungen und können entsprechend reagieren. Damit wird eine Organisation automatisch auditierbar und das persönliche Risiko für die Unternehmensführung wird drastisch gesenkt.

Ein ähnliches Bild ist auf der technischen Ebene gegeben. Es werden unterschiedliche Tools eingesetzt, die letzendlich zentral kontrolliert werden sollten, damit die Kontrolle gegeben ist. Über diese Ebene lassen sich dann beliebige Parameter oder Applikationen überwachen, die für die Sicherheit zuständig sind

Bei der Organisation betrachten wir den periodischen Check während wir bei der Technik

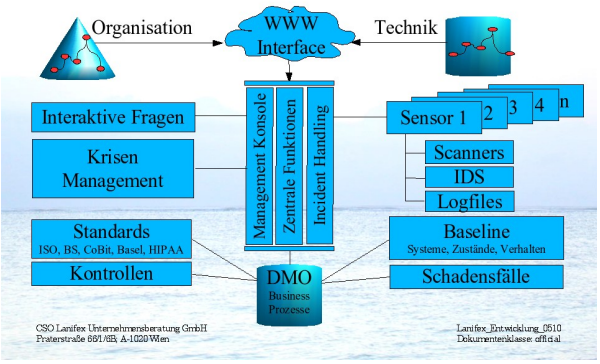
von der permanenten Systemauditierung sprechen.

Monitoring Technik



Als **umfassendes Sicherheitssystem** ergibt sich dann vereinfacht dargestellt folgendes Bild:

Gesamtsicht Monitoring



Im Zentrum sitzt eine Managementkonsole, die über ein Web-Interface erreicht werden kann. Auf der organisatorischen Ebene liegen alle relevanten Daten in einer relationalen Datenbank mit einer objektorientierten Benutzeroberfläche:

- Standards nach denen sich das Unternehmen richtet.
- Kontrollen, die zu überwachen sind, mit entsprechenden Fragebögen.
- Vordefiniertes Krisenmanagement

Auf der technischen Seite wird die gleiche Datenbank eingesetzt und enthält:

- Baseline der Systeme
- Schadenfall-Datenbank
- Das System wird mit verteilten Sensoren ergänzt, die aus den zu überwachenden Netzen und Systemen Informationen filtrieren, analysieren, speichern und weiter leiten.

Damit erreicht man die zentrale Kontrolle der Organisation und der Technik.

Das Gesamtunternehmen wird hinsichtlich Security transparent und damit ergeben sich folgende Effekte:

- **Geschäftsführerhaftung:** Als oberste Instanz ist der Geschäftsführer für die Sicherheit des Unternehmens zuständig.
- **Auditierbarkeit.** Sowohl die Organisation, als auch die Technik kann jederzeit auditiert werden.
- **Kapitalisierung:** Mit der Auditierbarkeit verbessert sich der Zugang zum Kapitalmarkt. Banken gehen immer mehr dazu über das operative Risiko eines Unternehmes zu durchleuchten.
- **Reputation:** Geschäftspartnern kann die Sicherheit über die Auditierbarkeit jederzeit nachgewiesen werden.

Lanifex berät Unternehmen in IT-Security, kann das **Risiko Assessment** (inkl. Audit) durchführen und entwickelt **Tools,** die Ihre Sicherheit hinsichtlich **Organisation** und **Technik** managen. Mit einem **Partnernetzwerk** (Computer Associates, BULL GmbH, NextiraOne, S&T, u.s.w.) werden Gesamtprojekte durchgeführt.

CSO Lanifex Unternehmensberatung GmbH
Praterstr. 66/1/6B, A-1020 Wien
Tel.: 43 1 2198222
e-Mail: office@lanifex.com
www.lanifex.com