Zur Metrik von Sicherheit und Bewusstsein

Referat für den „IISA-Stammtisch“

Philipp Schaumann

Philipp Schaumann
Dipl. Physiker
Bull GmbH Wien

http://sicherheitskultur.at/Trainingskonzept.htm
p.schaumann@bull.at

Zur Metrik von Sicherheit und Bewusstsein

Agenda - Was kann ich messen?

- Vergleich mit Standards und Best Practise
- Effektivität der technischen Maßnahmen
- Effektivität der organisatorischen Maßnahmen
- Mitarbeiter
  - Wissen und Kenntnisse der Mitarbeiter
  - Verhalten der Mitarbeiter
  - Zufriedenheit und Motivation der Mitarbeiter

Warum will ich Sicherheit messen?

- Wie effektiv sind meine technischen Maßnahmen?
- Was bekomme ich für mein investiertes Geld?
- Wie effektiv sind meine organisatorischen Maßnahmen?
- Vergeude ich Aufwand/Manpower ohne Sicherheit zu gewinnen?
- Hat sich meine Sicherheit durch die Maßnahme wirklich verbessert?
- Sichere ich an der richtigen Stelle?
- Wie gut ist das Verhalten meiner Mitarbeiter?
- An welchen Stellen läuft es schlecht?
- Wie effektiv sind meine Trainingsmaßnahmen (meine Informationen)?

Was bedeutet „Messen“?

- „Ermitteln eines Wertes durch quantitativen Vergleich der Messgröße mit einer Einheit (Normal)“ (DIN 1319 Teil 1)
- quantitative Bestimmung des Wertes einer Messgröße
- oft verbunden mit „Prüfen“: (DIN 2257 Teil 1), Vergleichen von Ist-Zustand mit Soll-Zustand

Was kann ich messen?
Vergleich mit Standards und Best Practise (1)

- **ISO 17799:2005, bzw. ISO 27001**
  Seit Dez. 2000 internationaler Standard, hervorgegangen aus British Standard BS7799, 2005 überarbeitet
  (sehr nicht-technisch, angenehm knapp)
  - http://www.iso.ch/
- **BSI Grundschutzhandbuch**
  Deutschland (extrem umfangreich (2000 Seiten) und recht technisch)
  - http://www.bsi.de/gshb/deutsch/menue.htm

Was kann ich messen?
Vergleich mit Standards und Best Practise (2)

- **Österreichisches IT-Sicherheitshandbuch**
  Herausgegeben vom Chief Information Office - Stabsstelle IKT-Strategie des Bundes
  - http://www.cio.gv.at
- **COBIT 1998 - Governance, Control and Audit for Information and Related Technology**
  - http://www.isaca.org

Typische Vorgehensweise

- **Checkliste mit Punktevergabe**
  - Beispiel CMMI, Capability Maturity Model Integration:
  - 0 - Incomplete - Ausgangszustand, keine Anforderungen
  - 1 - Performed - die spezifischen Ziele des Prozessgebiets werden erreicht
  - 2 - Managed - der Prozess wird gemanagt
  - 3 - Defined - der Prozess wird auf Basis eines angepassten Standard-Prozesses gemanagt und verbessert
  - 4 - Quantitatively Managed - der Prozess steht unter statistischer Prozesskontrolle
  - 5 - Optimizing - der Prozess wird mit den Daten aus der statistischen Prozesskontrolle verbessert
- Siehe auch: EFQM-Modell (European Foundation for Quality Management)

Was kann ich messen?
Vergleich mit Standards und Best Practise (2)

- **Probleme:**
  - Messung der theoretischen Qualität,
  - Vergleichbarkeit mit Anderen auf Grund subjektiver Bewertungen recht schwer
  - Berücksichtigt nicht die Veränderungen über die Zeit (z.B. neue Bedrohungen oder neue Risiko-Exponierungen)

Was kann ich messen?
Effektivität der technischen Maßnahmen (1)

- **Messung realer Ereignisse im Normalbetrieb „hinter“ einer Sicherungsmaßnahme**
  - **Desktop-Viren-Alarme trotz des Virenchecks im Proxy**
  - **Intrusion Detection Alarme hinter der Firewall**
  - **Stichprobenzählung von nicht-erkanntem Spam**
  - **Stichprobenzählung von falsch erkanntem Spam**
  - **Stichproben (oder vollst. Test) der Aktualität der Virensoftware**
  - **Prüfung des Patch-Zustands der Systeme**
  - **. . . .**

Was kann ich messen?
Effektivität der technischen Maßnahmen (2)

- **Probleme:**
  - **sollten regelmäßig durchgeführt werden**
  - **sind nur Momentaufnahmen**
  - **bei Stichprobentests sind keine absoluten Zahlen möglich, aber relative, z.B. Trend über Zeiträume**

Was kann ich messen?
Effektivität der technischen Maßnahmen (3)

- **Messung realer Ereignisse bei simuliertem Angriff**
  - Penetrationstest (Problem der Standardisierung)
  - Freisetzung von Test-Viren
  - „normierter“ Penetrationstest mit „allen Angriffen“ (z.B. qualys.com)

- **Probleme:**
  - bringt nur Aussagen über einen Aspekt der Sicherheit, erlaubt jedoch Trends festzustellen
  - immer nur Moment-Aufnahmen

Zur Metrik von Sicherheit und Bewusstsein

Was kann ich messen?
Effektivität der organisatorischen Maßnahmen (1)

- **Ablauf Benutzer-Administration**
  - Sperren von Accounts nach dem Ausscheiden: wieviele „Zombie-Accounts“ findet eine manuelle Überprüfung durch die Kostenstellen-Verantwortlichen?
- **Ablauf Datensicherung**
  - Datensicherungsprozeduren: Wie gut gelingen Wiederherstellungstests?
- **Ablauf System-Aktualisierungen**
  - Wie aktuell sind die Systeme wirklich?
- **Ablauf Change Management**
  - Wie oft werden Änderungen ohne Change Mgmt. Approval durchgeführt? Wie oft kommt es zu Problemen, Zeitüberschreitungen?
- **Ablauf Patch-Management**
  - z.B. MBSA (Microsoft Baseline Security Analyzer)

Was kann ich messen? Mitarbeiter-Aspekte

Kenntnis der Regeln und Gesetze	Wissen über Angriffe (Viren bis Social Engin.)	Mitarbeiter-engagement	Berichts- und Kommunikations-wege
↓	↓	↓	↓
Würde der Mitarbeiter einen Angriff oder eine Verletzung erkennen?		Würde der Mitarbeiter einen Angriff oder eine Verletzung melden?	Wüsste der Mitarbeiter, wie er/sie eine Bedrohung melden kann ? (auch Feuer, etc.)

Sicherheitsaspekt Wissen und Kenntnisse der Mitarbeiter

- **Wissen und Kenntnisse können leicht abgefragt werden, z.B. durch**
  - **improvisierte Fragebögen**
  - **selbst programmierter Quiz im Intranet**
  - **professionelle Befragung und Tests, z.B. http://www.blue-october.com/**
- **Themen (u.a.):**
  - **was ist vertraulich im Unternehmen?**
  - **welche Gefahren gibt es?**
  - **welches Verhalten ist sinnvoll?**
  - **was sind die Firmen-Regeln?**

Sicherheitsaspekt Sicherheitsverständnis der Mitarbeiter

- Verständnis für Zusammenhänge vermitteln und dann testen
  - Warum Vorsicht bei Mail-Anhängen?
  - Warum Vertraulichkeit von Dokumenten?
  - Warum Bildschirmsperre?
  - Warum am Abend den Schreibtisch säubern?
  - Warum im Bekanntenkreis, bei Ex-Kollegen Vorsicht bei der Themenwahl?
  - Warum Vorsicht im Gespräch mit fremden Verkäufern?
  - Warum im Meetingraum die Tafel säubern?
  - Warum Vorsicht auf Dienstreisen mit mobilen Geräten?

Sicherheitsaspekt Verhalten der Mitarbeiter (1)

- Direkte Stichproben:
  - Wie viel % der Desktops sind in der Mittagspause gesperrt?
  - Auf wie vielen Schreibtischen liegen Abends noch vertrauliche Materialien?
  - Wie lange dauert es, bis eine Betriebsfremder ohne Namensschild im Unternehmen angesprochen wird?
  - Wie viele der Mitarbeiter klicken auf Anhänge in Emails von unbekannten Absendern?
  - Wie gut sind die Passworte wirklich, ein Crack-Lauf gibt gezielt Auskunft?

Solche Tests auf jeden Fall vorher mit Geschäftsleitung und Betriebsrat absprechen

Sicherheitsaspekt Verhalten der Mitarbeiter (2)

- **Analyse der Helpdesk-Calls, z.B.:**
  - **Wie viele Anrufe kommen für Rücksetzen von Passworten (pro Benutzer und Jahr)?**
  - **Wie viele Anrufe kommen wegen Fragen zu E-Mail-Anhängen?**
  - **Wie viele Anrufe berichten „eigenartiges Verhalten“ „ihres“ Rechners nach Besuch einer Website?**

Sicherheitsaspekt Verhalten der Mitarbeiter (3)

- **Auswertung von Logs, z.B.:**
  - **Surf-Verhalten (auch gern anonym)**
  - **Automatisches Durchsuchen aller Rechner nach Schadsoftware (z.B. mit Ad-Aware) und nach nicht-autorisierter Software (z.B. mit SMS)**
  - **Port-Security (d.h. Feststellen des Sicherheitszustandes vor Einwahl ins Firmennetz)**

Solche Auswertungen auf jeden Fall vorher mit Geschäftsleitung und Betriebsrat absprechen

Thema Motivation

Wertschätzung

- Nur wenn der Mitarbeiter das Gefühl hat, dass sein Wert im Unternehmen geschätzt (und geschützt) wird,
- wird er die Werte des Unternehmens schützen

Zur Metrik von Sicherheit und Bewusstsein

Was gebe ich, was bekomme ich ?

Quelle: beck et al. services

Willkommen in der Wirklichkeit

	Manager	Nicht-Manager
Fühlt sich über-"belohnt"	13 %	7 %
Fühlt sich gerecht "belohnt"	34 %	10 %
Fühlt sich unter-"belohnt"	53 %	83 %

87% der subjektiv "Unterbelohnten" geben nur 50-60% ihrer tatsächlichen Leistungsfähigkeit!!

Quelle: beck et al. services

Was passiert bei empfundener Mis-Balance?

Reduktion des Gebens

- Dienst nach Vorschrift
- Überlastung vorgeben
- sinkende Leistung u.Qualität
- Reduktion der Kommunikation
- „schwarzen Peter" weitergeben
- Oppositionshaltung, Blockieren
- Keine Risiken, sich absichern
- Konfliktbereitschaft

Erhöhung des Bekommens

- Forderung nach mehr Gehalt oder Bonus
- Wunsch nach Versetzung oder Jobwechsel
- Firmeneigentum privat verwenden
- Private "Projekte" am Arbeitsplatz
- Ausnutzen des Spesenkontos
- „Sabotage"

Informations-sicherheit

Quelle: beck et al. services

„Innere Kündigung“

- 1982 geprägt von Dr. Reinhard Höhn in der FAZ
  - „Die innere Kündigung - ein schlimmes Thema“
  - Vergleich mit „Selbst-Pensionierung“
  - Dienst nach Vorschrift - passiver Widerstand
  - Persönlichkeitsveränderungen der Mitarbeiter
    - Sinkende Stresstoleranz
    - Kreativitätsarmut

Quelle: beck et al. services

Zur Metrik von Sicherheit und Bewusstsein

Gründe

- Ungenügender Informationsfluß zwischen Mitarbeitern und Vorgesetzten
  - (97 %);
- Mißbräuchlicher Einsatz von Information als Machtmittel
  - (90 %);
- Mangelnde Bereitschaft der Vorgesetzten zur offenen und sachlichen Diskussion
  - (93 %);
- Entscheidungen, die ohne Einbeziehen des Mitarbeiters getroffen werden
  - (95 %);
- Entscheidungen, die entgegen Absprachen mit dem Mitarbeiter getroffen werden
  - (85 %)

Quelle: beck et al. services

Zahlen (nach Gallup)

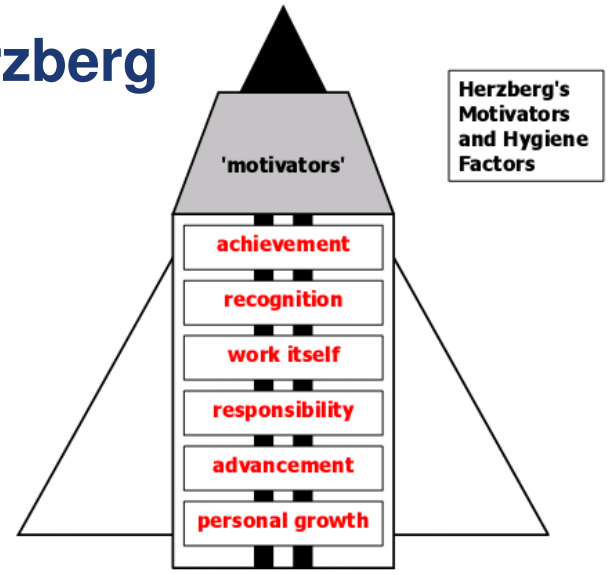
- spüren keine innere Verpflichtung gegen über der Firma — **88% der Mitarbeiter**
- „Dienst nach Vorschrift“ — **70% der Mitarbeiter**
- keine emotionale Bindung zum Job - „innere Kündigung“ — **2004 - 18%**, **2006 - 30%**

Quelle: beck et al. services

Zur Metrik von Sicherheit und Bewusstsein

Motivation nach F. Herzberg

- Motivatoren motivieren,
  - erzeugen eine positive Grund-Einstellung und Energie für die Arbeit
- Hygiene-Faktoren müssen da sein,
  - ihr Fehlen sabotiert die Motivation,
  - ihre Existenz stellt aber nur die Grundlage dar



Sicherheitsaspekt Einstellung der Mitarbeiter
-
Die Messung von Zufriedenheit und Wertschätzung

1. Messung indirekter Indikatoren

2. Mitarbeiterbefragungen

Die Messung von Zufriedenheit und Wertschätzung (1)

- **Messung indirekter Indikatoren**
  - **z.B. Krankenstand-Statistik (speziell Kurzkrankenstand Montag und Freitag- Stichwort „Restkrankenstand“)**
  - **z.B. Fluktuation (generell oder in einzelnen Abteilungen)**
  - **z.B. Verbrauch Toilettenpapier**
  - **z.B. Verbrauch Kaffeeverbrauch**
  - **. . .**

Die Messung von Zufriedenheit und Wertschätzung (2)

- **Direkte Fragen nach der Zufriedenheit und den Faktoren der Unzufriedenheit (im Rahmen der Personal-Entwicklungsaktivitäten, minimale separate Kosten)**
  - **Umfragen, Mitarbeiterzufriedenheitserhebungen**
  - **strukturierte Mitarbeitergespräche im Rahmen von Performance Reviews,**
  - **360° Beurteilungen/Reviews**

Sieben Humankriterien zur Gestaltung von Arbeit (auch nach DIN EN ISO 9241-2)

Sinnhaftigkeit der Tätigkeit und Leistung	Was ich tue hat einen sinnvollen Zweck, das Ergebnis der Arbeit hat einen Nutzen
Feedback	Mein Chef und meine Kollegen geben mir verwendbare konstruktive Rückmeldungen
Ganzheitlichkeit	Die Arbeit hat planende, kontrollierende und ausführende Anteile
Anforderungs-vielfalt	„Mischarbeit“, Wechsel von Problemlösung und Routine, Anforderungen an Körper und Psyche
Soziale Interaktion	Kooperation und Kommunikation mit anderen sind möglich
Autonomie	Es gibt Handlungs- und Entscheidungsspielräume, Möglichkeit der Selbstregulierung
Entwicklungs-möglichkeit	Die Arbeit bietet Herausforderungen und Entwicklungspotential, Fehler dürfen gemacht werden

Die Messung von Zufriedenheit und Wertschätzung (3)

Sinnhaftigkeit der Tätigkeit und Leistung	Was ich tue hat einen sinnvollen Zweck Arbeit hat einen Nutzen
Feedback	Mein Chef und meine Kollegen geben m konstruktive Rückmeldungen
Ganzheitlichkeit	Die Arbeit hat planende, kontrollierende Anteile
Anforderungs-vielfalt	„Mischarbeit“, Wechsel von Problemlösu Anforderungen an Körper und Psyche
Soziale Interaktion	Kooperation und Kommunikation mit an
Autonomie	Es gibt Handlungs- und Entscheidungss Möglichkeit der Selbstregulierung
Entwicklungs-möglichkeit	Die Arbeit bietet Herausforderungen und Entwicklungspotential, Fehler dürfen ge

Bekommen Sie so viel, wie Sie geben?

Sind Sie ausreichend gefordert?

Fühlen Sie sich gut informiert? Können Sie Ihre Fähigkeiten einbringen?

Haben Sie das Gefühl, dass Ihre Arbeit für das U. wichtig ist?

Hört ihr Chef Ihnen zu? Vertrauen Sie ihm?

Wissen Sie, was von Ihnen erwartet wird u. welche Rolle Sie in der Firmenstrategie spielen?

Empfinden Sie Ihre Arbeit als langeweilig und eintönig?

Fühlen Sie sich in ein Team eingebunden?

Haben Sie genügend Entscheidungsspielraum?

Sehen Sie Entwicklungs-möglichkeit für sich?

Dürfen Sie Fehler machen? Können Sie etwas lernen?