

Österreichisches Informationssicherheitshandbuch

Relaunch 2010

Gerald Trost, BKA
Manfred Holzbach, A-SIT



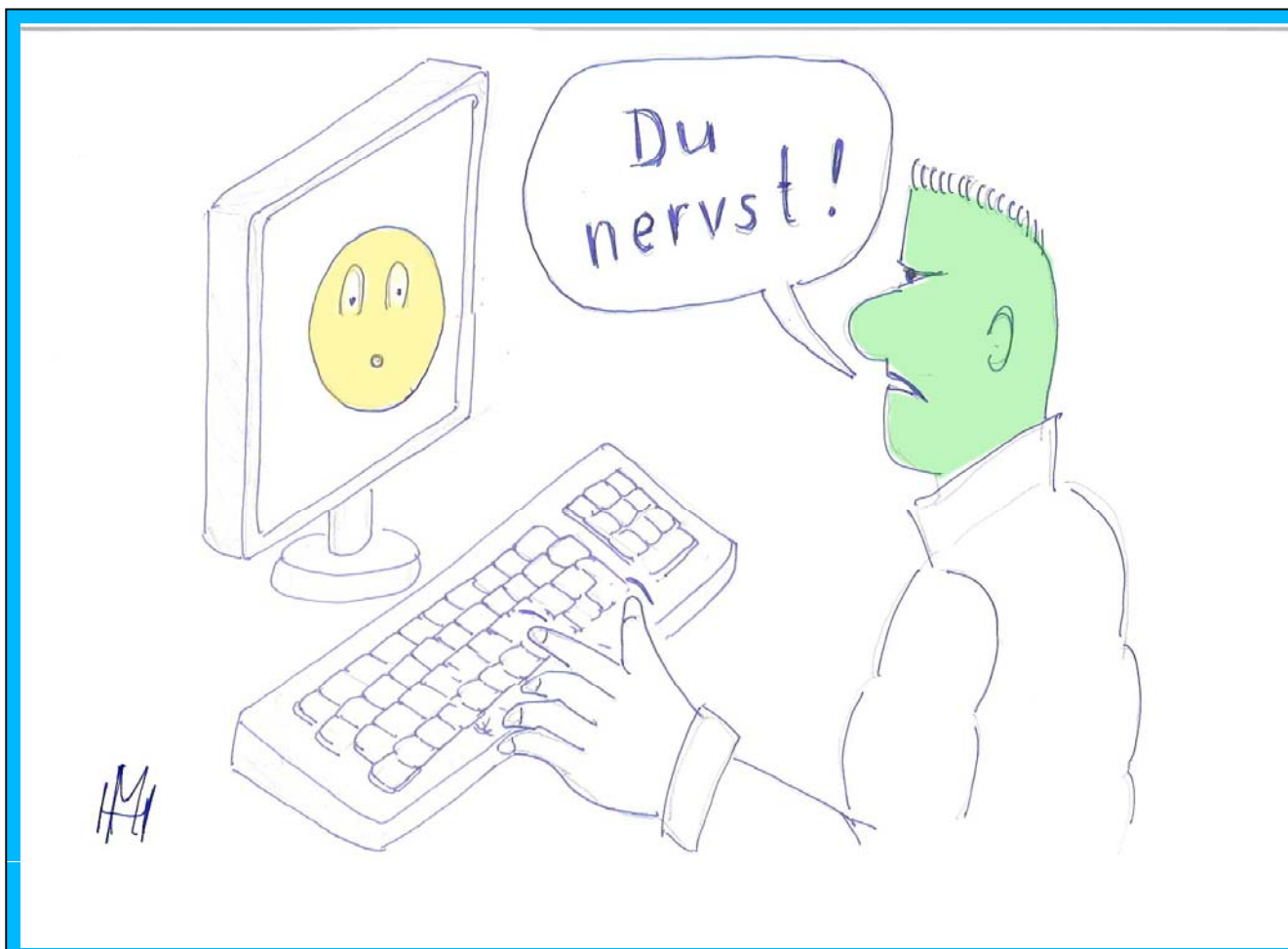
BUNDESKANZLERAMT  ÖSTERREICH

BÜRO DER INFORMATIONSSICHERHEITSKOMMISSION

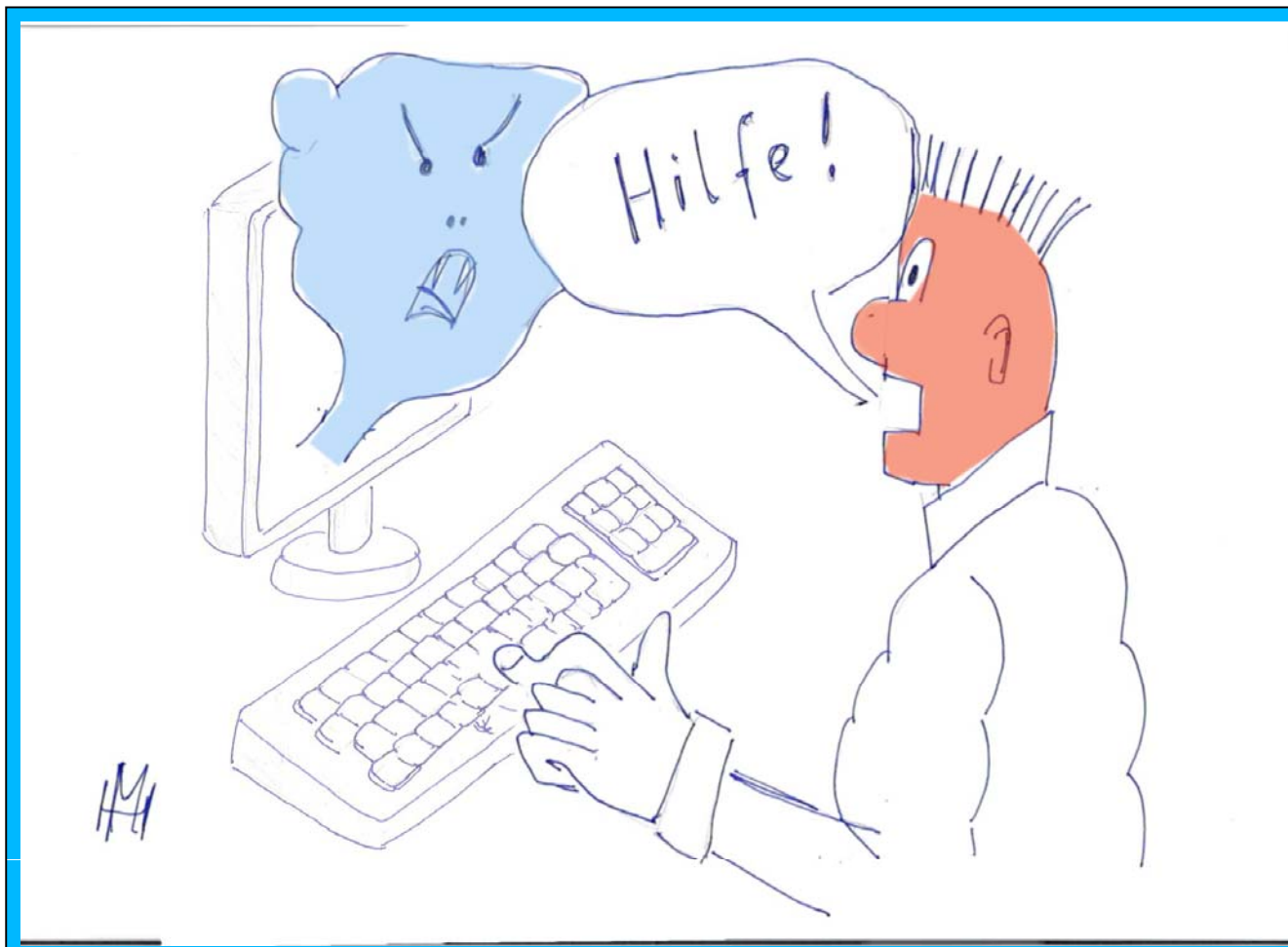
Awareness – Problem



Awareness – Problem



Awareness – Problem



Awareness - Beispiele

Jeder weiß:

- Risikoanalyse ist notwendig
- Passworte nicht aufschreiben
- Betriebssystem und Virenschutz up to date

Warum tun es dennoch nur wenige ?

Awareness - Beispiele

Jeder weiß:

- Risikoanalyse ist notwendig
- Passworte nicht aufschreiben
- Betriebssystem und Virenschutz up to date



Warum tun es dennoch nur wenige ?

Motivation

Problematik:

- Sicherheit kostet und ist unbequem
- Wer versteht die Sicherheitsmaßnahme ?
(Verstehen / Verständnis; zB eingeschränkte Rechte)
- Wie setzt man Maßnahme angemessen um ?
(zB Handy-Verbot)

Bewusstsein und Akzeptanz

Motivation

- Welche Maßnahme ist angemessen ?
- Für Wen ?

Motivation

- Welche Maßnahme ist angemessen ?
- Für Wen ?

Auswahl aus der Vielfalt

Zielgruppen

Rolle der Verwaltung bei IKT-Sicherheit

- Kritische Infrastrukturen sind öffentliches Gut
- Verantwortung des Staates wird auch eingefordert (z.B. Bankenkrise)
- Schaffung von Rahmenbedingungen und Vorgaben (z.B. Policies, Best Practises)

Rolle der Verwaltung bei IKT-Sicherheit

- Gesetzgeber (z.B. InfoSig)
- Aufsicht / Kontrolle (z.B. TKK, ISK)
- Betreiber / Benutzer (z.B. ELAK)
- Schaffung von Awareness / Best Practises

Durchgängige, einheitliche Sicherheitsstandards,
wo möglich => Sicherheitshandbuch

3 Beispiele: BKA und IKT-Sicherheit

- Betreiber:
E-Government (buergerkarte.at)
- Kontrolle:
GovCERT
- Best Practise:
Relaunch Sicherheitshandbuch



Historie Si-Handbuch

Grundschutz-Handbuch BSI-D

Koop-Vereinbarung BSI-ASIT

SIHA 1998 (BMI)

SIHA 2001 (BMÖLS-ASIT)

SIHA 2003 (BKA-ASIT)

SIHA 2006 (BKA-ASIT)

SIHA 2010 (BKA-ASIT-ISB)

Österr. Gegebenheiten
Gesetze, Normen

e-Government
IKT-Board

Neue Darstellung

(XML Online)

Neue Darstellung

Industrielle
Sicherheit

ISO 27000
Struktur



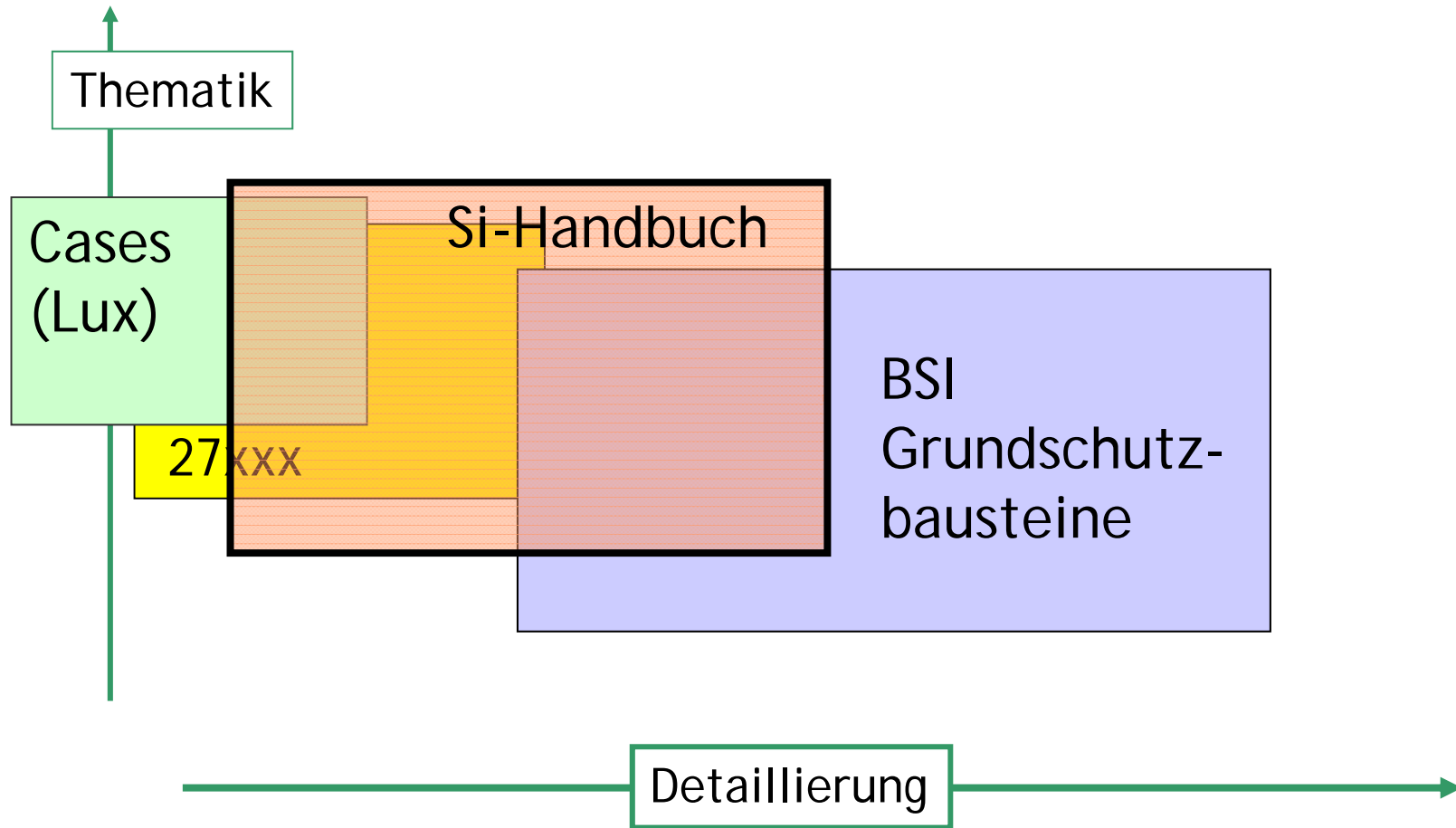
BUNDESKANZLERAMT  ÖSTERREICH

BÜRO DER INFORMATIONSSICHERHEITSKOMMISSION

Ziele des Relaunch 2010

- Inhaltliche Aktualisierung
 - künftig kontinuierlich
- Ausweitung der Einsatzgebiete
 - Implementierungshilfe 27000
 - Wissensbasis für Schulung und Awareness
 - Self-Check, Self-Audit
- Verbesserung der Akzeptanz
 - Zielgruppenorientierte Textierung
 - Neue Web-Anwendung

Quellen



Neuheiten

- Struktur nach ISO 27001 / 27002 (15 Kapitel)
- Aktualisierte Inhalte
- Web-basierte Anwendung
- Auswahl von Maßnahmen-Bausteinen für:
 - eigene lokale Si-Handbücher (*mit Wartungsautomatik*)
 - Checklisten
 - Querschnittsmaterien
- Personalisierung nach unterschiedlichen Zielgruppen
 - Autorengruppe aus untersch. Fachbereichen
- Export als PDF / RTF (CD oder Buch)

Besonderheiten

- Links zum RIS (Rechtsinformationssystem)
- Mehrsprachen - Unterstützung
- Erweiterte Filter (Funktionen / Branchen / Org-Größen)
- Referenztabellen
 - V 3 – V.2.3 und umgekehrt
 - V 3 – 27001 / 27002



Anwendung

Österreichisches Informationssicherheits-Handbuch

Sicherheitshandbuch: Ansicht/Ausschnitt

0 Vorwort und Management Summary

0.1 Zur Version 3.0 Beta

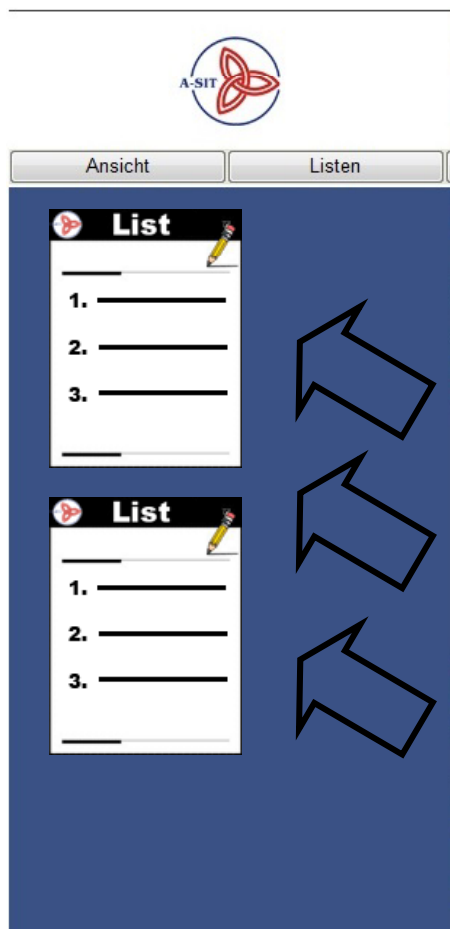
Herzlich willkommen bei der Lektüre der Beta-Version 3.0 des Österreichischen Informationssicherheitshandbuches. Sie sehen hier das vorläufige Ergebnis eines ehrgeizigen internationalen Projekts mit dem Ziel, dem bewährten Österreichischen Sicherheitshandbuch nicht nur neue Inhalte, sondern auch neue Einsatzgebiete und neue, interaktive Funktionalitäten zu geben. Die markantesten Neuheiten sind:

- Die bisherige Struktur mit 2 Teilen wurde an die Struktur der Normen ISO 27001 und 27002 angepasst, es gibt jetzt einen Teil mit 15 Kapiteln. Damit wird der Einsatz als Implementierungshilfe für ein ISMS gemäß ISO 27001 erleichtert.
- Es werden unterschiedliche Sprachen unterstützt. Damit wird das Sicherheitshandbuch international.
- Es werden unterschiedliche Textversionen des gleichen Themas für verschiedene Zielgruppen unterstützt. Diese können jeweils mit Filtern gewählt werden.
- Eine moderne Benutzeroberfläche erleichtert die Erarbeitung von lokal erzeugten Auswahl- und Checklisten mit eigenen Kommentaren. Damit können "eigene" Sicherheitshandbücher und -policies erarbeitet werden.
- Die inhaltliche Wartung erfolgt nun kontinuierlich, um die Aktualität sicherzustellen.
- Ein Update-Mechanismus vergleicht lokal ergänzte Themen mit allfälligen Änderungen in der zentralen Wissensbasis.

Dies ist allerdings noch eine Beta-Version mit dem primären Zweck, gemeinsam versteckte Fehler und Schwachstellen zu finden und darüber Feedback zu erhalten. Bisher lag der Fokus unserer Tätigkeiten auf der Neustrukturierung und technischen Realisierung; die Aktualisierung der Inhalte wurde erst begonnen, als die Datenstruktur stabil war. Daher werden die Inhalte und Textbausteine jetzt nach und nach auf aktuellen Stand gebracht, bzw. neue Entwicklungen wie "Cloud Computing" erst eingebracht. Unbeschadet dessen sind wir auch für inhaltliche Feedbacks dankbar.

Anwendung: Auswahl => Listen

Auswahlen können mit beliebigen Inhalten aus dem Handbuch gefüllt werden.



Weniger ist zu beachten, dass die Bedingungen bzw. Auflagen von etwaigen Versicherungen einzuhalten sind.

Wo sinnvoll bzw. hilfreich werden in den nachfolgenden Maßnahmenbeschreibungen Normen beispielhaft herausgegriffen und angeführt. Dabei handelt es sich nicht um eine vollständige Aufzählung aller für einen Bereich relevanten Normen und auch nicht um verbindliche Einsatzempfehlungen, die angeführten Beispiele sollen lediglich einen Hinweis auf existierende, möglicherweise zur Anwendung kommende Normen geben und ein detailliertes Einarbeiten in die Materie erleichtern.

9.1 Bauliche Maßnahmen

Relevanz:

9.1.1 Geeignete Standortauswahl

Relevanz:

Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen. Gebäude, die direkt an Hauptverkehrsstrassen (Autobahn, Bundesstraße, Bahn, ...) liegen, können durch Unfälle beschädigt werden, für Gebäude in Einflugschneisen von Flughäfen besteht Gefahr durch einen eventuellen Flugzeugabsturz.
- Die Nähe zu optimalen Verkehrswegen wird in vielen Fällen als Vorteil angesehen werden, kann aber - da diese Verkehrswege auch potentielle Fluchtwege darstellen können - unter Umständen auch die Durchführung eines Anschlages erleichtern. Vor- und Nachteile sind entsprechend abzuwägen.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- Bei Überbauten von U-, S- oder Eisenbahnen kann es zu Störungen von Datenleitungen und CRT-Bildschirmen kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z.B. durch Evakuierung oder großräumige Abspernung) beeinträchtigt werden.
- Streunende Haustiere können Fehlalarme von Bewegungsmeldern verursachen.

9.1.2 Anordnung schützenswerter Gebäudeteile

Relevanz:

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen.

Besteht die Möglichkeit, auch das Umfeld des Gebäudes in das Sicherheitskonzept einzubeziehen (etwa bei einer eigenen, ausschließlich der betreffenden Organisation gehörigen Liegenschaft), so können zusätzliche bauliche und technische Sicherheitsmaßnahmen getroffen werden ("Perimeterschutz", "Freilandchutz"). Dazu zählen etwa:

- Zäune und Mauern
- Tore, Schranken und Fahrzeugsperren
- Kamerabewachung und Bewegungsmelder

9.1.3 Einbruchschutz

Wann ? Wo ? Wie ?

4.10.2010 V 3.0 Beta für Usability Test
(Anfrage an office@a-sit.at)

Ende 10/2010: Autorengruppe

Mitte 11/2010 V 3.1 Rollout Wissensbasis

Voraussichtlich: www.sicherheitshandbuch.gv.at



BUNDESKANZLERAMT  ÖSTERREICH

BÜRO DER INFORMATIONSSICHERHEITSKOMMISSION

Danke für Ihre Aufmerksamkeit

manfred.holzbach@a-sit.at
gerald.trost@bka.gv.at



BUNDESKANZLERAMT  ÖSTERREICH

BÜRO DER INFORMATIONSSICHERHEITSKOMMISSION