

Informationssicherheit in der kommunalen Verwaltung - Schaffung eines IT- Grundschutzniveaus für kl. und mittlere Gemeinden

04.Juni 2014

ADV eGovernment-Konferenz 2014

Dipl.-Ing.ⁱⁿ Sandra Heissenberger (CISO)

Magistratsdirektion der Stadt Wien

Projektauftrag

Sicherheitsprofil für kleine bis mittlere Gemeinden zur Implementierung eines Minimum-Standards im Bereich der Informationssicherheit

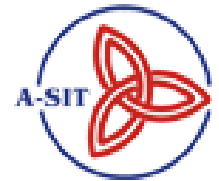
- aus BLSG-Arbeitsgruppe Recht und Sicherheit
- aus der Verwaltungsreform des BKA

Projektpartner

□ Projektpartner

BUNDESKANZLERAMT  ÖSTERREICH

StadT  Wien



Projektdaten

Zielsetzung

- Entwicklung einer Sicherheitspolicy für kleine und mittlere Gemeinden niederschw. Ansatz
- Risikomanagement als Basis
- Awareness der verantwortlichen Personen steigern
- Zielgruppengerechte Umsetzung

Dauer

- Projektbeginn Q4/2011, Projektende Q1/2014

Zieldefinition

- Ermittlung der Zielgruppe
 - für wen ist das Ergebnis bestimmt?
- Beschreibung der Methode
 - Risikomanagementprozess oder Checkliste?
- Beschreibung der Besonderheiten
 - Portalverbund, Sicherheitsklassen, ...
- Definition der gewünschten Ergebnisse

Zieldefinition

Social Networking



Vorgehensweise

- geplante Umsetzung
 - Erarbeitung eines Gefährdungskataloges
 - Beschreibung der Maßnahmen
 - Umsetzung als Checkliste
 - für kleine und mittlere Gemeinden

Größen der Gemeinden

Österreichweit

Einwohner	Gemeindeanzahl
bis 100	6
101 bis 500	175
501 bis 1.000	431
1.001 bis 2.500	1.093
2.501 bis 5.000	423
5.001 bis 10.000	155
10.001 bis 20.000	47
20.001 bis 50.000	16
über 50.000	8
Gesamt	2.354

Quelle: Österr. Gemeindebund

Vorgehensweise

Umsetzung des Projektes in 3 Phasen in Kooperation mit Forschung und Lehre

- Projektabwicklung durch Projektpartner
- Kooperation mit FH Hagenberg
 - Durchführung der Gemeindebefragung
 - Erstellung des Referenzmodells
 - Ermittlung der Gefährdungen
 - Auswahl der Sicherheitsmaßnahmen

Projektphase 1

- Ermittlung des Profils einer kleinen bzw. mittleren Standardgemeinde
- Umsetzung durch Studentinnen der FH Hagenberg als Projektarbeit
 - Recherche vor Ort bei mehreren Gemeinden
 - Beschreibung der Prozesse
 - Beschreibung der Infrastruktur

Projektphase 1

- Ergebnis zeigt
 - Umgang mit IT Infrastruktur
 - Grundlegende Aspekte der Sicherheit
 - Beschreibung der Infrastruktur
 - Bereitgestellte Leistungen

- Definition der Mustergemeinden

Projektphase 1

BESCHREIBUNG	REFERENZMODELL (kleine Gemeinde)	REFERENZMODELL (mittlere Gemeinde)
ALLGEMEINES		
Einwohner	2500-3000	5000-6500
Mitarbeiter im Haus	8 - 10	15 – 20
IT-Verantwortlicher	Ja, Amtsleiter bzw. Koordinator	Ja, eigener Admin
Bearbeiten von Anliegen der Bürger	Im Normalfall wird kein Ausweis verlangt („jeder kennt jeden“)	Ausweis wird teilweise verlangt
IT-INFRASTRUKTUR		
IT	Extern (als Dienstleistung ausgelagert)	Intern (nicht ausgelagert)
IT-Systeme	1-2 Server, 1 Client/MA, 2-3 Laptops, teilweise zentrale Drucker, teilweise Arbeitsplatzdrucker, Handys/Smartphones, Netzwerkkomponenten	Mehrere Server, 1 Client/MA, 2-6 Laptops, teilweise zentrale Drucker, teilweise Arbeitsplatzdrucker, Handys/Smartphones, Netzwerkkomponenten
Inventar der IT-Systeme	Ja (evtl. nicht immer aktuell)	Ja (evtl. nicht immer aktuell)
Standard-Arbeitsplatz	Rechner, Bildschirm, Tastatur, Maus, Telefon, teilweise Drucker	Rechner, Bildschirm, Tastatur, Maus, Telefon, teilweise Drucker

Projektphase 2

In Anlehnung an das Österreichische Sicherheitshandbuch und an den BSI-Grundschutzkatalog

- Umsetzung durch Studentinnen der FH Hagenberg als Projektarbeit
 - Erarbeitung eines Bedrohungskataloges und eines Maßnahmenkataloges
 - Erarbeitung einer Checkliste

Projektphase 2

- Ergebnis Checkliste
 - ca. 220 ausgewählte Prüfpunkte
 - 21 Kapitel
 - 6 Themenbereiche

- Beschreibung der Maßnahmen für jeden Prüfpunkte auf Basis des Informationssicherheitshandbuches

Projektphase 2

Checkliste					
Nr.	Frage	Umgesetzt?		Relevante Maßnahmen	
1 Organisation					
1.1	Werden die Sicherheitsmaßnahmen allen Mitarbeitern kommuniziert?	Ja	Nein	2.1. Informationssicherheitsmanagement	
1.2	Wird regelmäßig überprüft, ob die Sicherheitsmaßnahmen vollständig und korrekt umgesetzt sind?	Ja	Nein	2.1. Informationssicherheitsmanagement	
1.3	Werden Daten und Informationen klassifiziert?	Ja	Nein	2.2. Regelungen zum Umgang mit klassifizierten Informationen	
1.4	Werden klassifizierte Informationen gemäß ihrer Klassifizierungsstufe behandelt?	Ja	Nein	2.2. Regelungen zum Umgang mit klassifizierten Informationen	
1.5	Ist festgelegt, wer für die Klassifizierung der Daten verantwortlich ist?	Ja	Nein	2.2. Regelungen zum Umgang mit klassifizierten Informationen	
1.6	Ist schriftlich festgehalten, welche Mitarbeiter für welche Aufgaben und Bereiche zuständig sind?	Ja	Nein	2.3. Verantwortlichkeiten	
1.7	Für den Fall, dass Dienstleistungen ausgelagert sind: ist dies vertraglich geregelt?	Ja	Nein	2.4. Auslagerung von IT-Dienstleistungen (Outsourcing)	
1.8	Für den Fall, dass Dienstleistungen ausgelagert sind: Sind die Anforderungen aus dem Dokument „Vertragliche Regelungen.pdf“ erfüllt?	Ja	Nein	2.4. Auslagerung von IT-Dienstleistungen (Outsourcing)	
2 Maßnahmen für die kommunale Verwaltung					
2.1	Wird der PIN der Bürgerkarte geheim gehalten (nicht aufgeschrieben und nicht weitergegeben)?	Ja	Nein	3. Maßnahmen für die kommunale Verwaltung	

Projektphase 3

- Umsetzung der Checkliste in eine Anwendung
 - Anonymer Selbstcheck der Gemeinde
 - Gewichtung der Checkliste (risikobasierter Ansatz)
- Ausrollung an die Zielgemeinden durch den Gemeindebund
- Integration der Ergebnisse in das Österreichische Sicherheitshandbuch

Projektphase 3



Projektphase 3

Informationssicherheit in der kommunalen Verwaltung

Einleitung

Hinweise auf den Weg

Anwenderinformation

Für den Fragenkatalog

Gefährdungskatalog

Ausgewählte Gefährdungen

Maßnahmenbeschreibung

Bausteine Sicherheitshandbuch, IT-Grundschutz

Referenzmodell

Modell der Referenzgemeinde

Literatur, Abkürzungen

Weiterführende Quellen, Begriffserklärungen



Evaluation

Starten Sie das Programm

Kontakt für technische Fragen

Ihre Anlaufstelle

Hotline des BKA
TelNr.: +43 1 53115 202777
In der Zeit von Montag bis Freitag 8 - 17 Uhr

Kontakt Städtebund

Rathaus, 1082 Wien

E-Mail: post@staedtebund.gv.at
TelNr.: +43 1 4000 89980

Kontakt Gemeindebund

Löwelstraße 6, 1010 Wien

E-Mail: office@gemeindebund.gv.at
TelNr.: +43 1 5121480

Projektphase 3

The screenshot shows a web application interface with a dark green background. At the top, there are logos for 'BUNDESKANZLERAMT ÖSTERREICH', 'Österreichischer Gemeindebund', and 'Österreichischer Städtebund'. The main content area is titled 'Evaluation' and contains three columns: 'Checkliste' (with a document icon), 'Auswertungen' (with a bar chart icon), and 'Berichte' (with a pen icon). A navigation button at the bottom left reads '← Zum Hauptscreen'. In the top right corner of the application area, there are window control icons (down arrow, maximize, close).

Projektphase 3

Checkliste

Exportieren Komplette Checkliste exportieren Per E-Mail versenden Importieren

Id-Nr.	Frage	Vollständig	In großen Teilen	In einigen Teilen	Kaum oder gar nicht	Nicht anwendbar	Auswertung	Relevante Maßnahme	Erläuterung	Zwischenergebnis	Gewichtungsfaktor	Auswertung
<input type="checkbox"/> 1	Organisation											
<input type="checkbox"/> 1.1	Werden die Sicherheitsmaßnahmen allen Mitarbeiterinnen und Mitarbeitern kommuniziert?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Management	2.1. Informationssicherheitsmanagement		3	3	9
<input type="checkbox"/> 1.2	Wird regelmäßig überprüft, ob die Sicherheitsmaßnahmen vollständig und korrekt umgesetzt sind?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Management	2.1. Informationssicherheitsmanagement		0	2	0
<input type="checkbox"/> 1.3	Werden Daten und Informationen klassifiziert?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Management	2.2. Regelungen zum Umgang mit klassifizierten Informationen		2	2	4
<input type="checkbox"/> 1.4	Werden klassifizierte Informationen gemäß ihrer Klassifizierungsstufe behandelt?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Management	2.2. Regelungen zum Umgang mit klassifizierten Informationen		0	2	0
<input type="checkbox"/> 1.5	Ist festgelegt, wer für die Klassifizierung der Daten verantwortlich ist?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Management	2.2. Regelungen zum Umgang mit klassifizierten Informationen		0	1	0
	Ist schriftlich festgehalten, welche						Management	2.3				

Zur Evaluation

Mathematik 1

Auswertung = Zwischenergebnis *
Gewichtungsfaktor

- Gewichtung der Prüfpunkte 1 - 3
- Gewichtung der Umsetzung 0 – 3
 - vollständig 0
 - In großen Teilen 1
 - In einigen Teilen 2
 - Kaum oder gar nicht 3
 - Nicht anwendbar 0

Projektphase 3

BUNDESKANZLERAMT  ÖSTERREICH

 Österreichischer
Gemeindebund



StadT  Wien

Auswertungen

Organisation und Personal

Administration

Gesamtauswertung

Betrieb

Infrastruktur

Informations- und
Kommunikationstechnik

Outsourcing

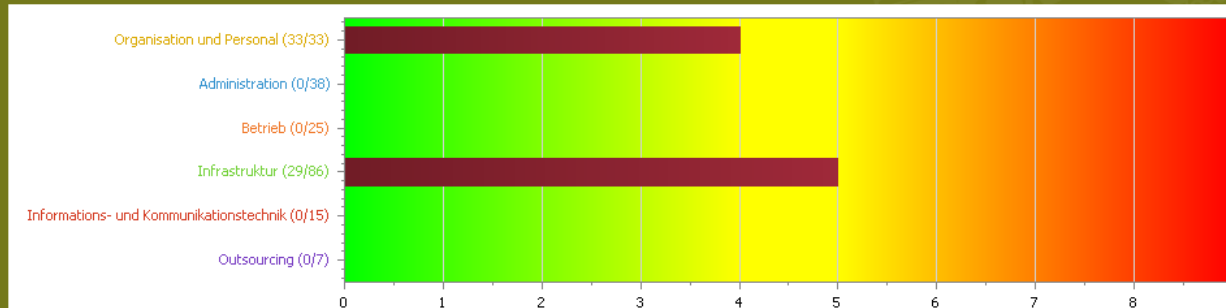


◀ Zur Evaluation

Projektphase 3

Gesamtauswertung

 Druckvorschau  Zur Checkliste



Prüfpunkte die kaum oder gar nicht erfüllt sind

Id	Prüfpunkt	Auswertung	Erläuterung	Verantwortlich	Zieltermin
1.1	Werden die Sicherheitsmaßnahmen allen Mitarbeiterinnen und Mitarbeitern kommuniziert?	Management			
1.8	Für den Fall, dass Dienstleistungen ausgelagert sind: Sind die Anforderungen aus dem Dokument „Vertragliche Regelungen.pdf“ erfüllt?	Organisatorische Regelungen			
2.2	Wird die Identität von Bürgerinnen und Bürgern, die der Mitarbeiterin oder dem Mitarbeiter der Gemeinde nicht persönlich bekannt sind, bei den jeweiligen Anfragen überprüft (z.B. durch Vorzeigen eines Ausweises)?	Organisatorische Regelungen			

 Zu den Auswertungen

Mathematik 2

Berechnung des Handlungsbedarf

- Pro Auswertungskategorie (Hauptkategorie) wird der Maximale Gewichtungsfaktor ermittelt
 - Gewichtung 3: 100%
 - Gewichtung 2: 66,67% (2 / 3)
 - Gewichtung 1: 33,33% (1 / 3)

Projektphase 3

BUNDESKANZLERAMT ÖSTERREICH

Österreichischer Gemeindebund

Österreichischer Städtebund

Stadt Wien

Berichte

Managementbericht	Gesamtbericht	Detailbericht
-------------------	---------------	---------------

◀ Zur Evaluation

Projektphase 3

BUNDESKANZLERAMT ÖSTERREICH Österreichischer Gemeindebund Österreichischer Städtebund Stadt Wien

Detailbericht

Drucken Exportieren Per E-Mail versenden Bericht anpassen

Detailbericht
Informationssicherheit

03.05.2014

Gesamtauswertung

Organisation und Personal (33/33)	4
Administration (0/38)	
Betrieb (0/25)	
Infrastruktur (29/86)	5
Informations- und	

Seite 1 von 1 100%

Zu den Berichten

Eckpunkte des Projektes

- Ermittlung des Gemeindeprofils
- Bereitschaft der Mitarbeit der Gemeinden
- Entwicklung eine Checkliste
- Umsetzung durch die FH Hagenberg
 - keine Informationen vorhanden
 - neutrale Herangehensweise der Studentinnen
- Kostengünstig durch Kooperation mit FH Hagenberg

Mögliche Ausbaustufen

- Auswertung der Ergebnisse
 - Anonym (kein Gemeindennamen)
 - Bundesland als kleinste Einheit
- Sicherheitslandkarte der Gemeinden
- und vieles mehr ...

Informationen

Österreichischer Städtebund

Organisation Services Themenfelder Städtetag **ÖGZ** Ausschüsse Presse

- Aktuelles
- ÖGZ
- Termine
- Veranstaltungsergebnisse
- Umfrageergebnisse
- Publikationen
- Tools
- FAQ
- Fotogalerie
- Links
- Jobs

Services ▶ Tools ▶

Informationssicherheit in der kommunalen Verwaltung

Die globale Bedrohung der Cyber-Kriminalität ist eine Herausforderung mit der sich die öffentliche Hand im Umgang der Datenverwaltung konfrontiert sieht. Städte haben große Rechenzentren, wo Unmengen von Informationen zusammenfließen, die natürlich durch Sicherungsmechanismen vor Missbrauch geschützt gehören - und auch werden. Wir können getrost sagen, dass österreichische Städte und Gemeinden enorm viel dafür tun, dass die Sicherheit mittels hochprofessionellem Know how gewährleistet werden kann und durch die internationalen Compliance-Richtlinien gestützt wird. Dennoch muss noch viel getan werden.

Wir freuen uns Ihnen in Kooperation mit dem Bundeskanzleramt und weiteren Partnern das "Sicherheitshandbuch für Gemeinden" anbieten zu können. Es steht Ihnen nachstehend zum Download und zur kostenlosen Verwendung zur Verfügung.

Technische Details:

Sollte auf Ihrem Computer kein Microsoft .NET Framework installiert sein, so wird im Laufe der Installation die benötigte Version automatisch installiert.

SYSTEMVORAUSSETZUNGEN!

Betriebssystem:
Microsoft Windows® XP SP2
Microsoft Windows® Vista
Microsoft Windows® 7
Microsoft Windows® 8

Zusätzlich benötigte Software:
Microsoft .NET Framework 4.0 (oder höher)
Microsoft Office 2000 (oder höher)
Adobe Acrobat Reader

Prozessoren:
min. 800 MHz, empfohlen 1,5 GHz

Arbeitsspeicher:
min. 512 MB, empfohlen 1024 MB

Festplattenspeicher:
min. 500 MB freier Speicher (abhängig vom zu erwartenden Datenvolumen)

Bildschirmauflösung:
Um das Programm optimal nutzen zu können, empfehlen wir eine Bildschirmauflösung von mindestens 1280x1024 Pixel.

 [Informationssicherheit \(28 MB\)](#)

• zurück

Österreichischer Städtebund

Suche
Ihr Suchbegriff
» Erweiterte Suche

Login
Ihre E-Mail-Adresse
» Passwort vergessen
» Neue Registrierung

OGZ

Landesgruppen

- Burgenland
- Kärnten
- Niederösterreich
- Oberösterreich
- Salzburg
- Steiermark
- Tirol
- Vorarlberg

amtstafel 20

f

Danke

Dipl.-Ing.ⁱⁿ Sandra Heissenberger (CISO)
Magistratsdirektion der Stadt Wien

Sandra.Heissenberger@wien.gv.at

Mathematik 2

Berechnung des Handlungsbedarf:

$7 * 100\% = 7$, $2 * 66,67\% = 1,33$, $3 * 33,33\% = 1$
Ergibt eine Gewichtung von: $9,33$ ($7 + 1,33 + 1$)

Alle Fragen mit 3 beantwortet:

$$((7*3*3)+(2*2*3)+(3*1*3)) = 84$$

Dividiert durch die Gewichtung von $9,33 = 9,00$

Handlungsbedarf = 9