Österreichischer Städtebund

Security Leitfäden „Self Assessment Tool“

Initiative des ÖStB

FLGÖ NÖ Tagung

26. August 2024

Dr. Ronald Sallmann

„Informationssicherheit“ im Blickpunkt

„Städte werden immer öfter Opfer von Cyber-Kriminellen“

Die neue Kriminalität

„Städte werden immer öfter Opfer von Cyber-Kriminellen“

Keine Begräbnisse mehr möglich: Wie gefährlich es ist, wenn Hacker Gemeinden lahmlegen, erlebte jüngst Korneuburg (NÖ). Auch Putins Cyber-Armeen sind aktiv – ein Internet-Experte warnt.

Das Rathaus von Korneuburg (NÖ) hat unruhige Zeiten hinter sich. Seit mehr als einer Woche geht nichts mehr.

„Krone“-Cyber-Experte Dr. Cornelius Granig

Nachdem Cyber-Kriminelle die Server des Rathauses von Korneuburg (NÖ) mit Schadsoftware lahmgelegt hatten (die „Krone“ berichtete), war die Aufregung groß. Die Stadt konnte nicht mehr auf ihre eigenen Daten zugreifen, weil diese von Hackern verschlüsselt worden waren. Dramatische Konsequenz: Nichts ging mehr – sogar Begräbnisse mussten schweren Herzens abgesagt werden, da die Stadtverwaltung keine Sterbeurkunden mehr ausstellen konnte. Mittlerweile funktioniert immerhin das Bürgerservice wieder, auch Beurkundungen sind wieder möglich. Eine Gemeinderatssitzung kann abgehalten werden. Spezialisten kümmern sich um die Datenwiederherstellung. Mit den Betrügern, die die Server lahmlegten, hatte man keinerlei Kontakt. Anzeige wurde erstattet.

„Korneuburg ist freilich kein Einzelfall“, weiß „Krone“-Cyber-Experte Dr. Cornelius Granig. Städte und Gemeinden würden immer öfter von Kriminellen angegriffen. Größe und Lage des Ortes spielen keine Rolle.

Zar Putin schickte seine Hacker-Armeen aus

In den letzten Jahren erwischte es etwa auch die beiden steirischen Städte Weiz und Feldbach. Ziel der Kriminellen sei es, Lösegeld zu erpressen, indem Druck auf die verantwortlichen Politiker ausgeübt wird.

Alarmierend: Seit Ausbruch des Ukraine-Krieges häufen sich Cyber-Attacken, die aus Russland gesteuert auch auf heimische Behörden aus Russland. Putin schickt seine Hacker-Armeen auf das „Internet-Schlachtfeld“. Immer wieder auffallend ist laut Granig, wie einfach die Täter über Mails mit dahinter liegenden Links („Phishing-Mails“) in die kommunalen Netzwerke eindringen können.

Dadurch gelangen sie an Zugangsdaten von Gemeinde-Angestellten – der Schaden ist angerichtet. Korneuburg und anderen Kommunen rät der „Krone“-Experte für die Zukunft regelmäßige Schulungen der Mitarbeiter, solche Links nicht zu öffnen. Verlässliche Backups sorgen dafür, dass durch möglichen Angriffen Ersatzsysteme greifen können.

S. Steranger, M. Party

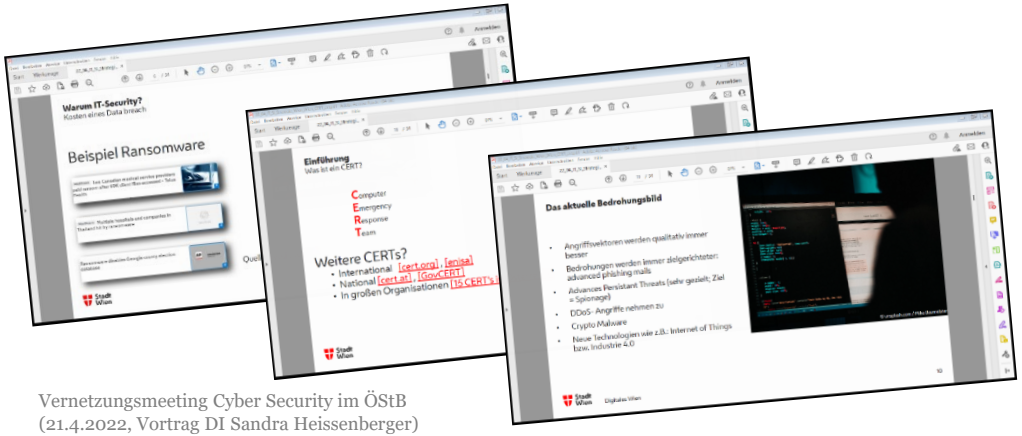
Die Top-6 Deloitte Tech Trends 2024:

- **Trend 1:** GenAI wird Wachstumstreiber für Unternehmen
- **Trend 2:** Immersive Technologien sind am Vormarsch
- **Trend 3:** Ausbau der IT-Infrastruktur wird zum Erfolgsfaktor
- **Trend 4:** IT-Kernmodernisierung ist weiterhin notwendig
- **Trend 5:** Sensibilisierung für Cyber-Risiken gewinnt an Bedeutung
- **Trend 6:** Tech-Talente stehen im Fokus

Projektentstehung:
Warum gemeinsame Security Initiative des ÖStB?

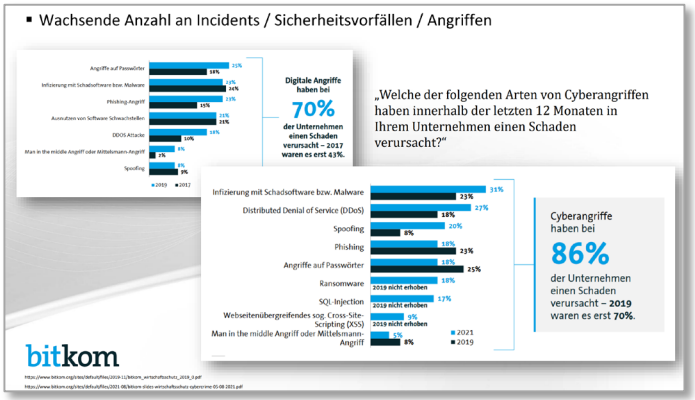
Österreichischer Städtebund

- Security Bedrohungen wachsen weiter
- NIS 1 & NIS 2 mit neuen Herausforderungen für die Kommunen
- IT-Personalsituation
- Awareness (auch der kommunalen Verantwortungsträger)
- Konkrete Unterstützung durch die ÖStB - Initiative



Vernetzungsmeeting Cyber Security im ÖStB
(21.4.2022, Vortrag DI Sandra Heissenberger)

Lagebild Informationssicherheit
(FIT 07.11.2023, Vortrag FH-Prof. DI Robert Kolmhofer)



Eckpfeiler der Initiative

Österreichischer Städtebund

- Erarbeitung eines Self-Assessment Tools zur Maßnahmenbewertung „Informationssicherheit / Datenschutz (inkl. NIS) mit UNINET it-consulting GmbH
- „Awareness – Kampagne“ durch persönliche Information in den ÖStB Fachausschüssen und Landesgruppen
- Unterstützung bei Anwendung des Self-Assessment Tools - wo gewünscht / erforderlich (IT-Kommunal)
- Etablierung Austausch-Plattform der IT-Verantwortlichen bzw. IT-Sicherheits-Verantwortlichen der österreichischen Städte

Projektverlauf:
Projektauftrag – Stand Juni 2023

Österreichischer Städtebund

- Erstellung eines elektronischen Self-Assessment Fragenkatalogs („Tool“) zur Bewertung von Maßnahmen im Informationssicherheits-/Datenschutz/NIS(2)-Umfeld zur automatisierten Ableitung von Handlungsfeldern (inklusive Aufteilung in Standard-IT-Security-Erfordernisse und NIS(2)-relevante Anforderungen)
  - Erstellung eines Fragenkatalogs nach international anerkannten Vorgehensmodellen, Normen, Empfehlungen und Richtlinien (ISO27xxx, BSI, Ö Informationssicherheitshandbuch) sowie national relevanten Anforderungen aus DSG/DSGVO/NIS(2)
  - Erstellung einer Mapping-Logik aus der Fragebeantwortung zur automatisierten Ableitung von Handlungsfeldempfehlungen zur Verbesserung der IT-Security/Informationssicherheit
  - Die Toolimplementierung als Microsoft Excel-basierende-Anwendung
  - Die Tests des Tools samt Auswertelogik und Handlungsempfehlungsableitung erfolgt mit zwei vom Österreichischen Städtebund ausgewählten Städten.
- Einmaliger Updatezyklus für den NIS-relevanten Teil (aktueller Stand 2023 ist die NISG/NISV zur NIS-RL aus dem Jahr 2018 = NIS1 Version) zur Anpassung an die NIS2 Vorgaben, die voraussichtlich im Herbst 2024 in nationales Ö-Recht umgesetzt werden.

Projektverlauf:
Projektstruktur- und Vorgehen

Österreichischer Städtebund

Projektsteuerungsgruppe

- Manfred Wundara
- Roman Breitfuß
- Clemens Madlener
- Sandra Heissenberger
- Johannes Eschenbacher
- Robert Kolmhofer
- Alexander Leitner
- Ronald Sallmann
- Norbert Weidinger

Projektleitung i.A. ÖStB (N. Weidinger)

- Vertretung des Gesamtprojektes nach außen
- Projektsteuerung
- Information / Präsentation

Tool-Umsetzung

- Uninet - FH-Prof. DI Robert Kolmhofer & Team

Pilotstädte für das Self-Assessment-Tool

- Salzburg
- Ansfelden

➢ **Operative Anwendung des Self-Assessment-Tools für Mitgliedsstädte kostenfrei**

Projektverlauf:
Status / Projektergebnis

Österreichischer Städtebund

- Leitfäden in Version 1 fertiggestellt zum Abrufen
- Lizenzinfo als eigenes Tabellenblatt im Tool:

  "Nutzungsrecht umfasst alle Abteilungen bzw. Dienststellen und Kommunalbetriebe der Mitgliedsstädte/Mitgliedsgemeinden des ÖStB“

Projektverlauf:
Projektergebnis Security Assessment Tool -> Leitfäden

Österreichischer Städtebund

- Elektronisches Self-Assessment Tool zur Bewertung von Maßnahmen im Informationssicherheits- und NIS(2)-Umfeld zur automatisierten Ableitung von Handlungsfeldern
- Tool-Umsetzung in Excel mit Fragen-/Auswertelogik und Berichterstellung
- Fragenset
  - **Informationssicherheit** | 50 Haupt- und 110 Detailfragen
    - Aufteilung in organisatorische und technische Aspekte
    - Berücksichtigung von anerkannten Normen/Standards (z.B. ISO/IEC 27001, BSI IT-Grundschutz, Österreichisches Informationssicherheitshandbuch)
  - **NIS** | 53 Haupt- und 146 Detailfragen
    - Kategorien entsprechend NISG/NISV und NIS Fact Sheet 9/2022
    - 29 Themenbereiche in 11 Kategorien
- Fragenkaskade für Anwendung des NIS-Fragenkatalogs mit Berücksichtigung von NIS2 nach aktuell verfügbaren Informationen der betroffenen Sektoren/Bereiche

Projektverlauf:
Informationssicherheit-Fragenkatalog

Österreichischer Städtebund

- Aufteilung in organisatorische und technische Aspekte
- Berücksichtigung von anerkannten Normen/Standards (z.B. ISO/IEC 27001, Österreichisches Informationssicherheitshandbuch, BSI IT-Grundschutz)

ORGANISATORISCHE ASPEKTE

1. Informationssicherheitsrichtlinie / -regelungen
2. Sicherheitsorganisation & Systemlandschaft
3. Verantwortungsbereiche
4. Informationssicherheit im Projektmanagement
5. Asset-Management
6. IT-Risikomanagement
7. Mitarbeiter und Mitarbeiterinnen
8. Zutritts- / Zugangs- / Zugriffsmanagement, Datenträger & Schutzmaßnahmen
9. Physische Sicherheit
10. Schulungen
11. IT-Dokumentation & Informationsklassifizierung
12. Change Management
13. Externe Dienstleister & Lieferanten
14. Incident Management
15. Business Continuity Management
16. Audits
17. Compliance

TECHNISCHE ASPEKTE

1. Netzwerk
2. WLAN
3. Applikations- & Systemlandschaft
4. Endpoint Security
5. Schadsoftwareschutzkonzept
6. Software und Patch Management
7. Datensicherung
8. Fernzugriff
9. Cloud-Dienste

Projektverlauf:
NIS-Fragenkatalog

Österreichischer Städtebund

Kategorien entsprechend NISG/NISV & NIS Fact Sheet 9/2022

1. GOVERNANCE UND RISIKOMANAGEMENT
- 1.1 Risikoanalyse
- 1.2 Sicherheitsrichtlinie
- 1.3 Überprüfungsplan der Netz- und Informationssysteme
- 1.4 Ressourcenmanagement
- 1.5 Informationssicherheitsmanagementsystemprüfung
- 1.6 Personalwesen

2. UMGANG MIT DIENSTLEISTERN, LIEFERANTEN UND DRITTEN
- 2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten
- 2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

3. SICHERHEITSARCHITEKTUR
- 3.1 Systemkonfiguration
- 3.2 Vermögenswerte
- 3.3 Netzwerksegmentierung
- 3.4 Netzwerksicherheit
- 3.5 Kryptographie

4. SYSTEMADMINISTRATION
- 4.1 Administrative Zugangsrechte
- 4.2 Systeme und Anwendungen zur Systemadministration

5. IDENTITÄTS- UND ZUGRIFFSMANAGEMENT
- 5.1 Identifikation und Authentifikation
- 5.2 Autorisierung

6. SYSTEMWARTUNG UND BETRIEB
- 6.1 Systemwartung und Betrieb
- 6.2 Fernzugriff

7. PHYSISCHE SICHERHEIT
- 7.1 Physische Sicherheit

8. ERKENNUNG VON VORFÄLLEN
- 8.1 Erkennung
- 8.2 Protokollierung und Monitoring
- 8.3 Korrelation und Analyse

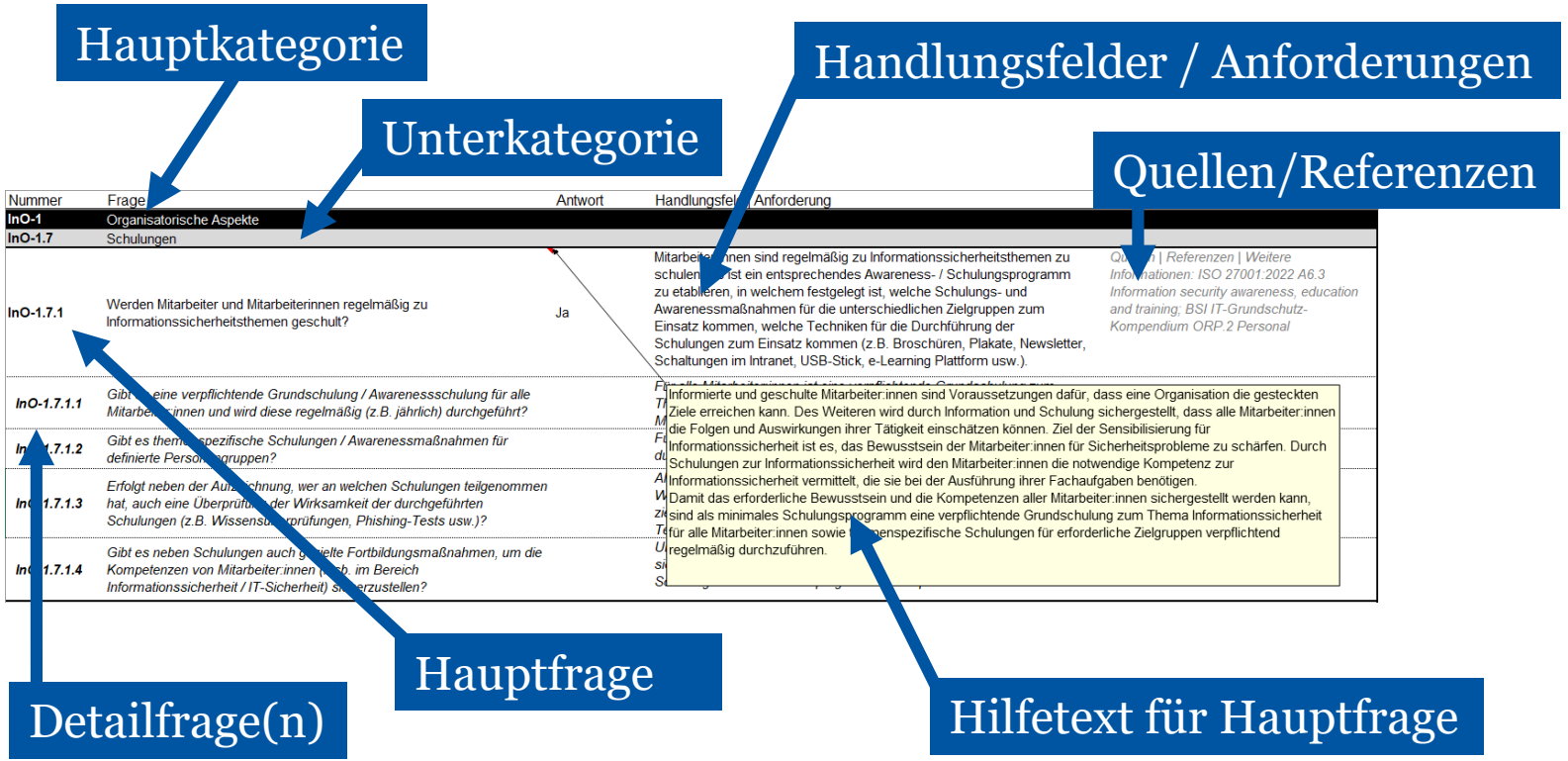
9. BEWÄLTIGUNG VON VORFÄLLEN
- 9.1 Vorfallsreaktion
- 9.2 Vorfallsmeldung
- 9.3 Vorfallsanalyse

10. BETRIEBSKONTINUITÄT
- 10.1 Betriebskontinuitätsmanagement
- 10.2 Notfallmanagement

11. KRISENMANAGEMENT
- 11.1 Krisenmanagement

UNINET it-consulting GmbH

Projektverlauf:
Aufbau Fragenkatalog



Projektverlauf:
NIS(2)-Bewertung

Österreichischer Städtebund

Sind Sie von NIS2 betroffen?

Die verwendeten Informationen basieren auf der Richtlinie(EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 sowie auf dem aktuellen Wissenstand vom 06.02.2024. Die tatsächliche NIS2-Betroffenheit kann erst nach der Verabschiedung der NIS2-Richtlinie im nationalen NISG bzw. NISV ermittelt werden. Dies gilt gleichermaßen für die Schwellenwerte der KMU-Regelung.

Österreichischer Städtebund

Hatten Sie einen NIS(1)-Bescheid erhalten?	Nein
Wie viele Mitarbeiter:innen beschäftigen Sie?	50 bis 249
Wie hoch war der Rechnungsabschluss (Jahresumsatz)?	< 50 Mio. EUR
Wie hoch war die Rechnungsabschluss (Jahresbilanzsumme)?	< 43 Mio. EUR

WICHTIG
Für die Einstufung des Unternehmens muss neben der Unternehmensgröße (d.h. Anzahl der Mitarbeiter:innen und Jahresumsatz bzw. Jahresbilanzsumme) berücksichtigt werden, ob es sich um ein eigenständiges Unternehmen, ein Partnerunternehmen (Beteiligungen an anderen Unternehmen ab 25 % bis 50 %) oder ein verbundenes Unternehmen (Beteiligungen an anderen Unternehmen über 50 %) handelt. Da bei Kommunen die Begriffe Jahresumsatz und Jahresbilanzsumme nicht verwendet werden, ist hier in beiden Fällen der Rechnungsabschluss einzutragen.
Bitte prüfen Sie, ob Sie Beteiligungen an anderen Unternehmen haben und/oder ein verbundenes Unternehmen sind [1, S.15 ff]!
Es gilt die Definition gemäß des Benutzerleitfaden zur Definition von KMU der Europäischen Union [1, S.11, Art. 2].
Vom ÖStB wird zum Zeitpunkt der Veröffentlichung dieses Self-Assessment-Tools eine rechtliche Prüfung, welche Parameter von Kommunen anzuwenden sind, durchgeführt.

Sie sind ein mittleres Unternehmen

Sind Sie in einem der folgenden Sektoren tätig?

Energie

Teilsektor:	Elektrizität	Fernwärme und/oder -kälte	Erdöl	Erdgas	Wasserstoff
	Nein	Nein	Nein	Nein	Nein

Verkehr

Teilsektor:	Straßenverkehr	Luft-, Schienenverkehr oder Schifffahrt
	Nein	Nein

Gesundheitswesen	Nein
Trinkwasser	Nein
Abwasser	Nein
Öffentliche Verwaltung	Nein
Post- und Kurierdienste	Nein
Abfallbewirtschaffung	Ja

Weitere Sektoren, falls zutreffend
(bitte am linken Rand die nächsten Sektoren aufklappen)

Ergebnis: Sie sind voraussichtlich ein wichtiges Unternehmen!
Bitte beantworten Sie für die nachfolgenden Sparten/Bereiche/Abteilungen den NIS-Fragenkatalog jeweils in einer eigenständigen Kopie des NIS-Self-Assessment Tools (Excel-Dokument).
|Abfallbewirtschaffung|

Projektverlauf:
Bericht / Ergebnis

Österreichischer Städtebund

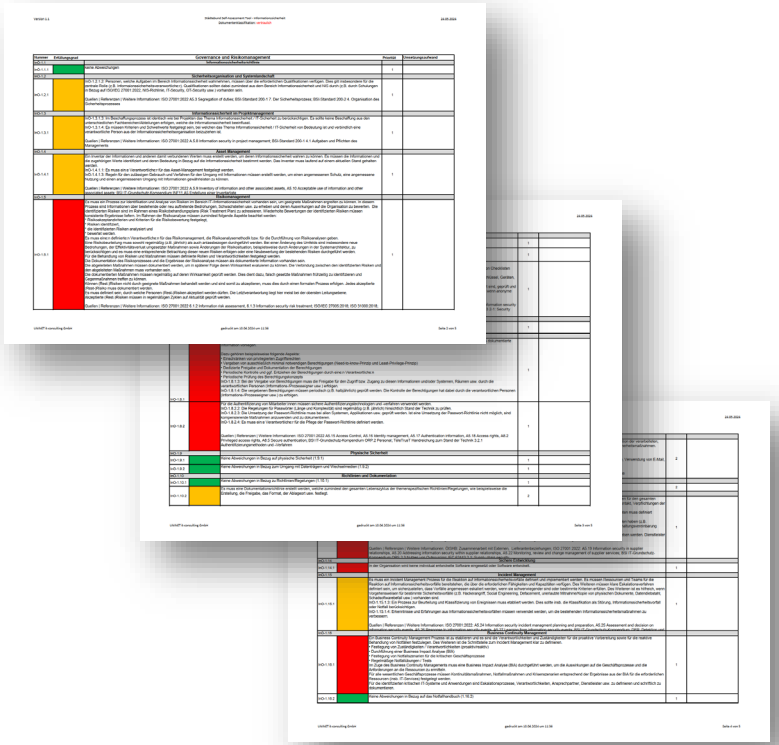
Self-Assessment des österreichischen Städtebunds

Auswertungsergebnisse der organisatorischen Informationssicherheit

Stadt/Gemeinde:	Musterstadt
Verwaltungsadresse:	Musterstraße 1 1234 Musterstadt
Durchführungsdatum:	19.06.2024
Kontaktperson:	Musterperson
Position:	Verantwortlicher
Telefonnummer:	+43 123 45678910
E-Mail-Adresse:	musterperson@must

Österreichischer Städtebund

gedruckt am 10.06.2024 um 11:36



Tool-Nutzung

Österreichischer Städtebund

- kostenfreie Nutzung durch alle Mitgliedsstädte
- Nutzungsvereinbarung MS mit ÖStB erforderlich
- Abrufbar über ÖStB (Johannes Eschenbacher)
- E-Mail Adresse: security@staedtebund.gv.at

Nächste Schritte

Österreichischer Städtebund

- Klärung NIS Betroffenheit
- Dokumentenvorlagen
  - Angebot UNINET liegt vor
  - ÖStB Aussendung Städte wegen Muster
- Unterstützungsangebot
  - InfoSec & NIS (gemeinsam) anbieten
- Austauschplattform ÖStB
- SAT – Phase 2 (nach NISG NR-Beschluss)

Informationssicherheit als Top Management Thema

Österreichischer Städtebund

Erfolg und Nutzen der Security Initiative des ÖStB hängt ausschließlich von der tatsächlichen Anwendung in den Mitgliedsstädten ab!

Dipl.-Ing. Norbert Weidinger
(Projektleitung)

weidinger-consulting@outlook.at

Dr. Ronald Sallmann
(Projektteam, Moderation Assessments)

ronald.sallmann@staedtebund.gv.at oder

ronald.sallmann@it-kommunal.at