WIENER NETZE

WIR LEITEN DIE ZUKUNFT EIN.

„Potential einer dezentralen Stadt – Im Spannungsfeld der Informationssicherheit und des Datenschutzes“

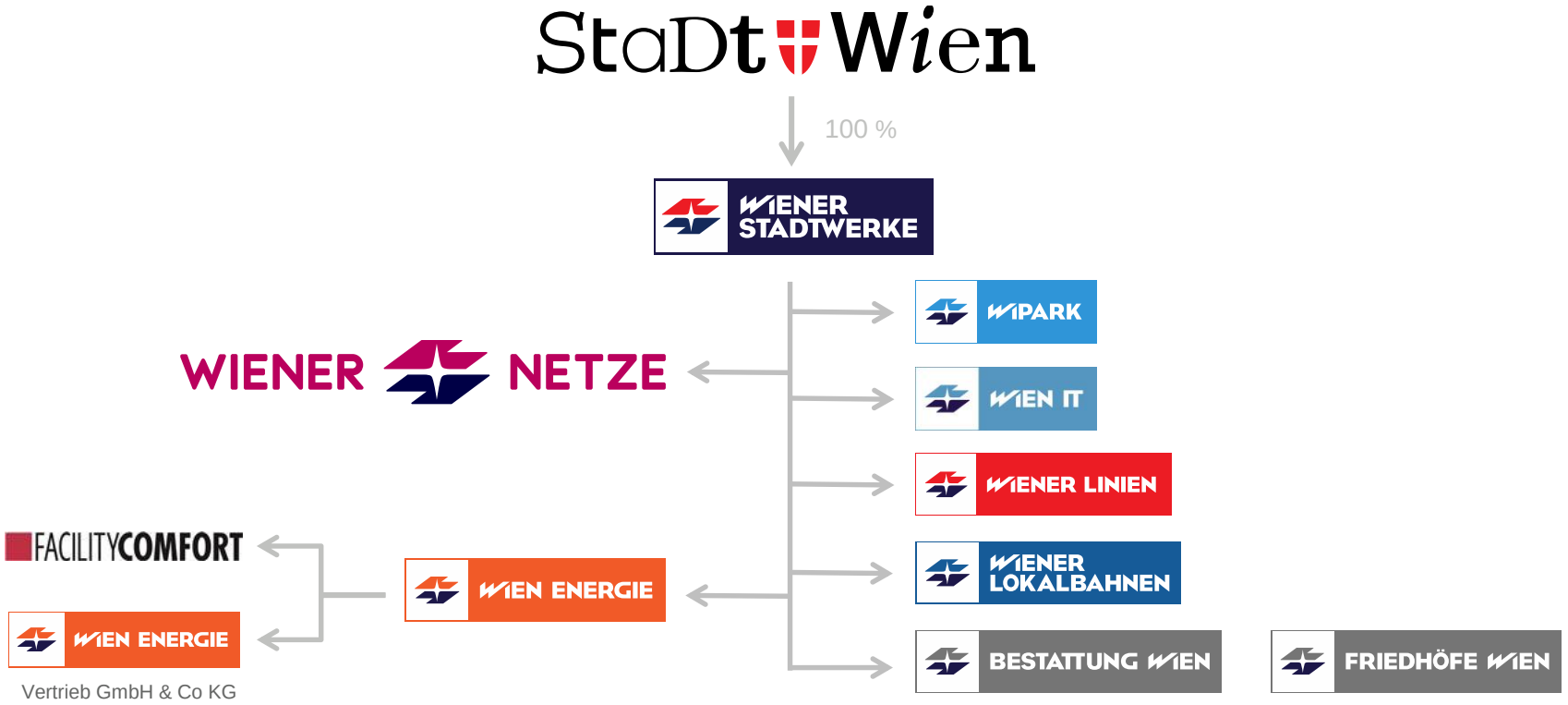
Christoph Eberl – Digitale Information und IKT Governance | K-DIG | CISO

INHALT

- Vorstellung der Wiener Netze GmbH
- Smart City Ziele & Lösungsansätze
- Anforderungen an Smart Grids
- Welche Problemfelder resultieren daraus für die Informationssicherheit?
- Datenschutzrechtliche Implikationen
- Der Wandel zu einem modernen Netzbetreiber im Sinne der Informationssicherheit

Vorstellung der Wiener Netze GmbH

WIENER NETZE IM STADTWERKE UMFELD



NETZE – DIE LEBENSADERN WIENS UND UMGEBUNG

Österreichs größter Kombinetzbetreiber – Strom, Gas, Fernwärme und Glasfaser

Wir planen, bauen und betreiben ein Energienetz mit 30.000 km Länge – „einmal um die Welt“

Investitionen von mehr als 200 Millionen Euro jährlich – bis 2020 mehr als eine Milliarde Euro in das Wachstum der Stadt

Ein Stromausfall in Wien an einem Wochentag würde einen Schaden von 14 Millionen Euro pro Stunde verursachen

Zuverlässigkeit von 99,99 % – eines der besten und sichersten Netze weltweit

APA-AUFTRAGSGRAFIK

WIENER NETZE

VERSORGUNGSGEBIET

- **1,2 Millionen KundInnen** in Wien, Teilen von Niederösterreich und Burgenland
- **46 Umspannwerke** und **11.176 Trafostationen**
- 1.518.681 Stromzähler, 656.393 Gaszähler, 381.000 Wärmezähler
- **Versorgungssicherheit von 99,99 %**

AUFGABEN DER WIENER NETZE

WAS MACHEN WIR ALS GRÖSSTER KOMBINETZBETREIBER?

- **Netzkundendienst**
- **Netzstrategie und Netzplanung**
- **Planung, Ausbau, Betrieb und Instandhaltung** des Gas-, Fernwärme-Primär-, Strom- und des Glasfasernetzes
- **Ausbau und Instandhaltu**ng des Fernwärme-Sekundärnetzes im Auftrag von Wien Energie
- **Zähler- und Datenmanagement**
- **Regulationsmanagement**

WAS MACHEN WIR ALS GRÖSSTER KOMBINETZBETREIBER?

- **Netzdienstleistungen** in den Bereichen:
  - Beratung, Planung, Bau und Betrieb von Schaltanlagen und Transformatoren
  - Beratung und Analyse von Ölen
  - Beratung und Überprüfung von Zählerinstallationen und Zählereichungen
  - Kabelmessungen und Vermessungsleistungen
  - Akkreditierte Prüf- und Inspektionsstelle

SMART METERING

Größtes Projekt in der Unternehmensgeschichte

WIENER NETZE

Größter Rollout im deutschsprachigen Raum

1,6 Millionen Zählertäusche

Massenrollout: 7 Zähler / Minute
Aktuell: 1 Zähler / Minute

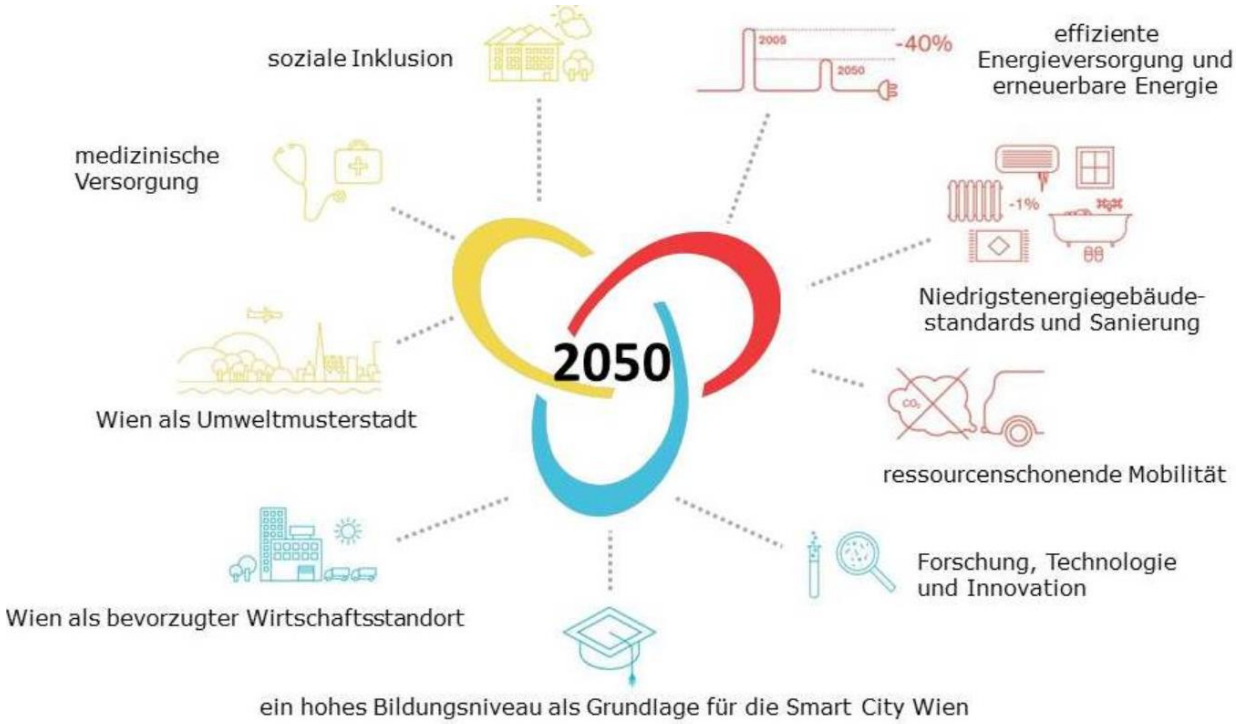
Hoher Personaleinsatz über Jahre: 500 MitarbeiterInnen

SMART METERING BEI DEN WIENER NETZEN

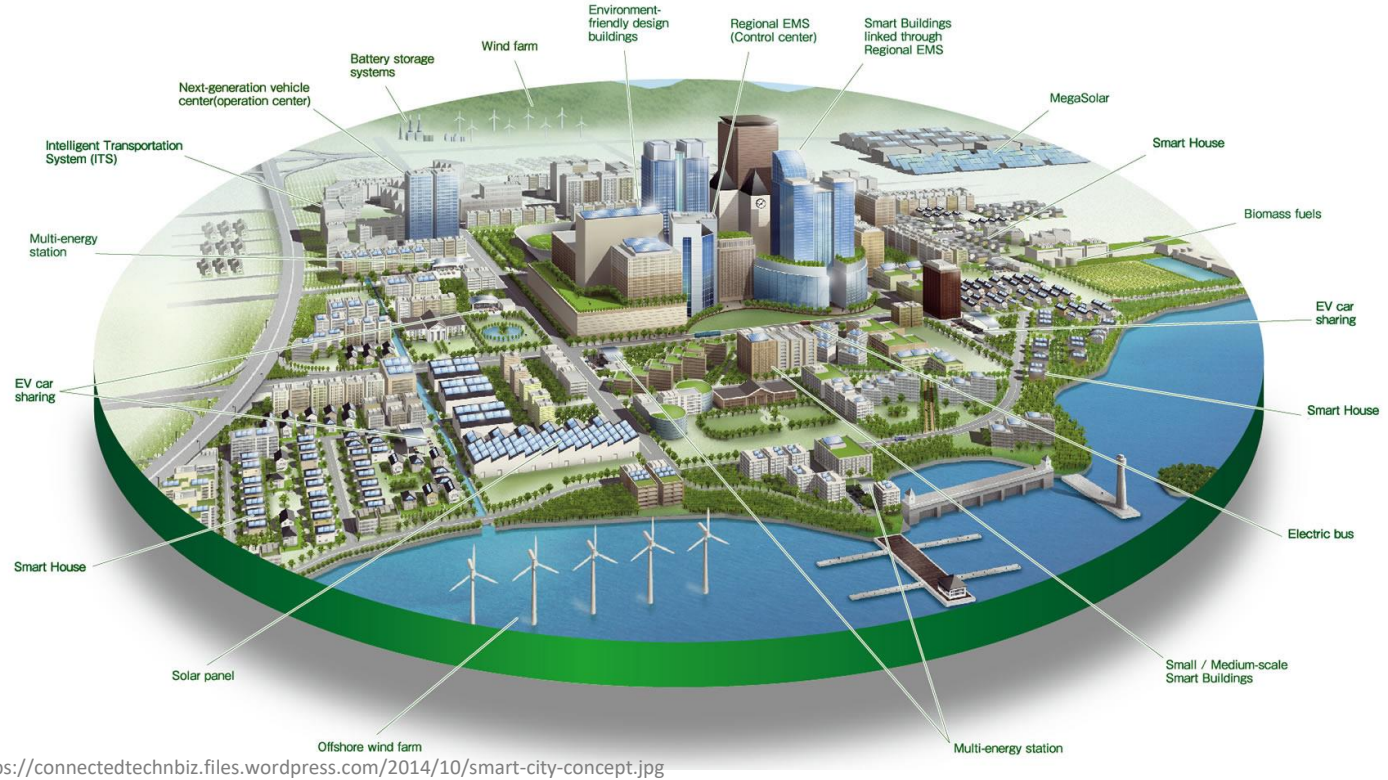
- Die Wiener Netze verantworten den derzeit **größten Smart Meter Rollout** im deutschsprachigen Raum
  - Bis 2017 wurden bereits rund 4.000 Zähler in Testgebieten installiert
  - Nach sorgfältiger Planung und Ausschreibung wird 2017 der Lead- und Technologiepartner gefunden, der den gesamten Rollout begleitet (Technologie, effiziente Rolloutabwicklung, IKT-Integration).
  - Die Wiener Netze streben die Erfüllung der EU-Richtlinie an, die eine Rollout-Quote von **80 Prozent bis 2020** vorsieht.

Smart City Ziele & Lösungsansätze

Smart City Wien – Ziele



Smart City Wien – Energie



https://connectedtechnbiz.files.wordpress.com/2014/10/smart-city-concept.jpg

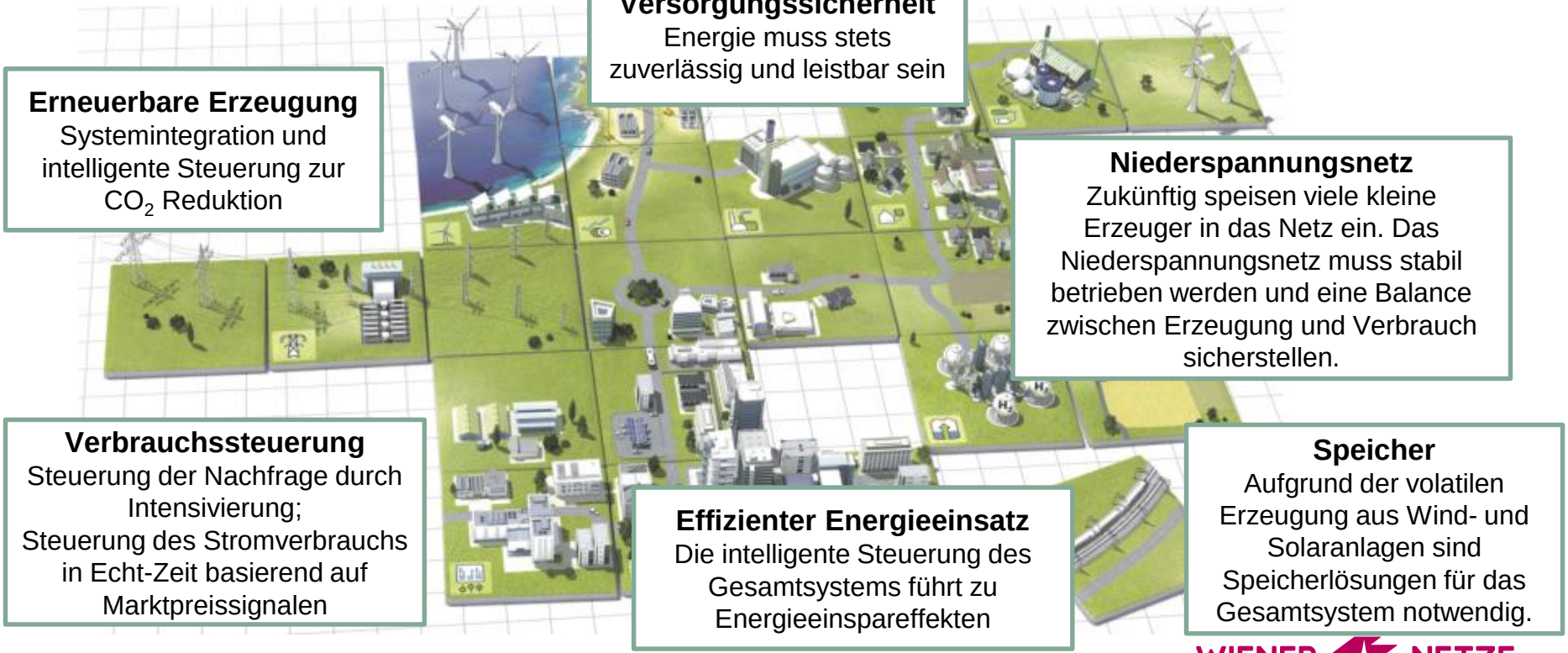
Anforderungen an Smart-Grids

WIENER NETZE IM STADTWERKE UMFELD

Smart City Wien – Energie

Versorgungssicherheit
Energie muss stets zuverlässig und leistbar sein

Erneuerbare Erzeugung
Systemintegration und intelligente Steuerung zur CO_2 Reduktion



Niederspannungsnetz
Zukünftig speisen viele kleine Erzeuger in das Netz ein. Das Niederspannungsnetz muss stabil betrieben werden und eine Balance zwischen Erzeugung und Verbrauch sicherstellen.

Verbrauchssteuerung
Steuerung der Nachfrage durch Intensivierung;
Steuerung des Stromverbrauchs in Echt-Zeit basierend auf Marktpreissignalen

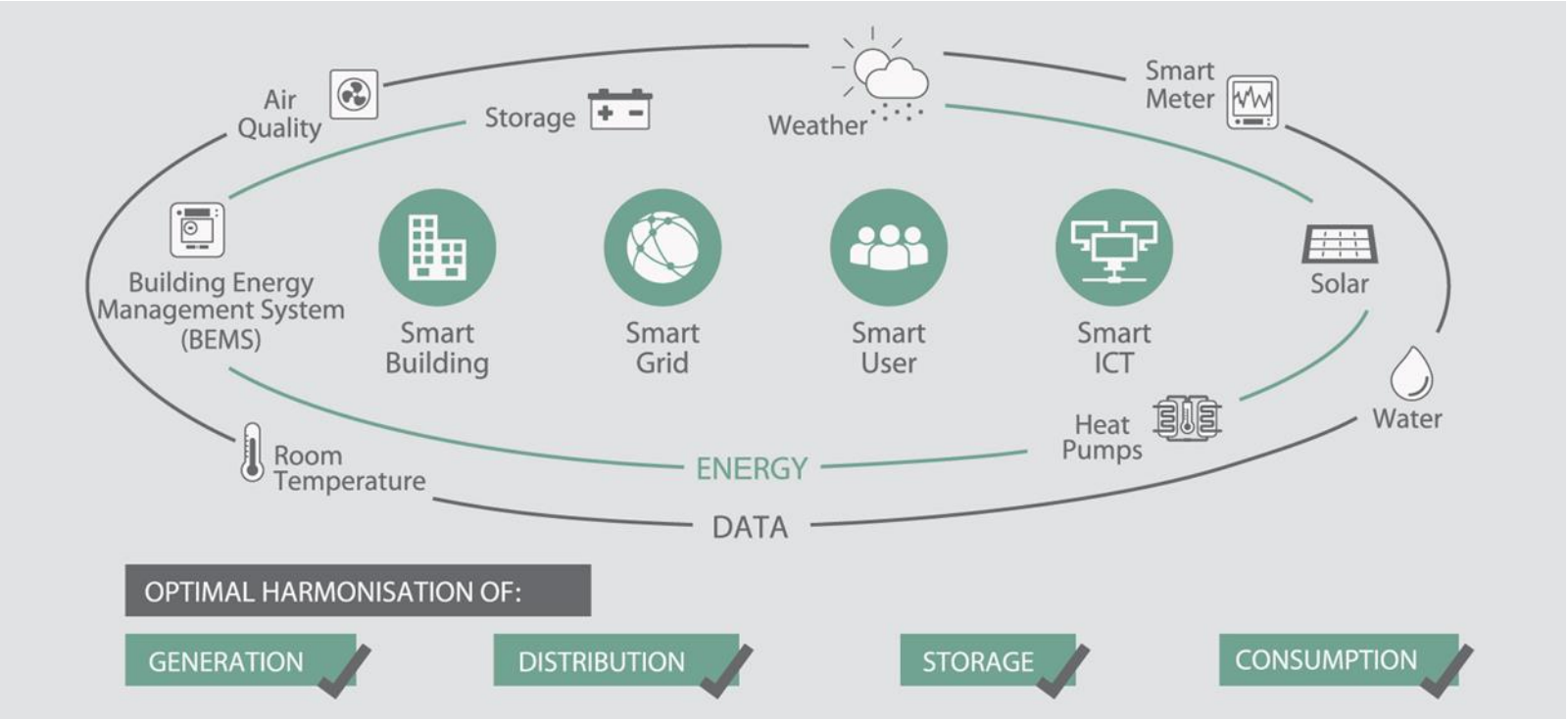
Effizienter Energieeinsatz
Die intelligente Steuerung des Gesamtsystems führt zu Energieeinspareffekten

Speicher
Aufgrund der volatilen Erzeugung aus Wind- und Solaranlagen sind Speicherlösungen für das Gesamtsystem notwendig.

Quelle: CC Siemens (Siemens-Welt Dezember 2012)

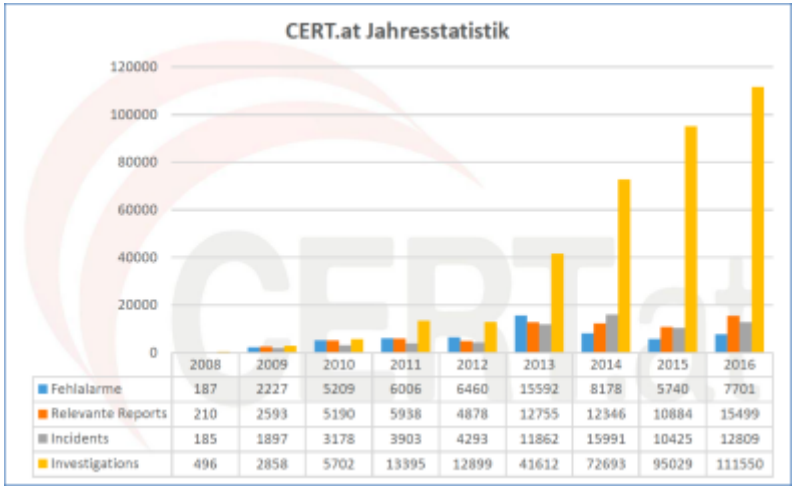
WIENER NETZE IM STADTWERKE UMFELD

Smart City Wien – optimale Harmonisierung



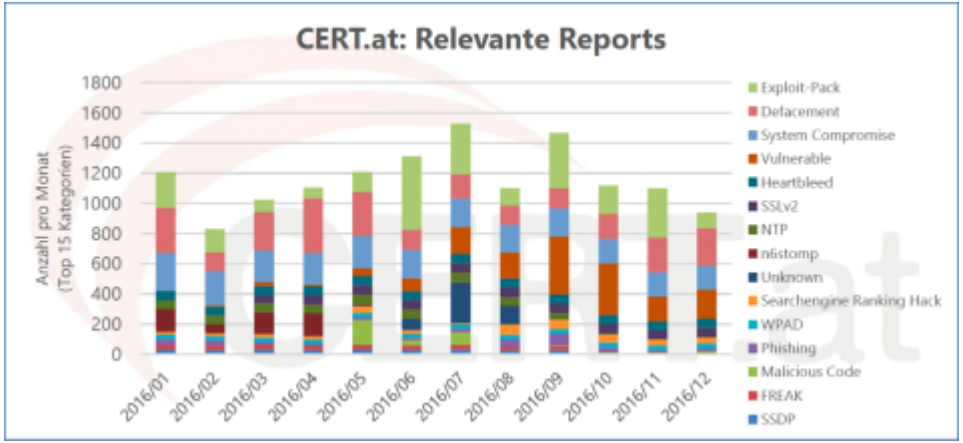
Welche Problemfelder resultieren daraus für die Informationssicherheit?

WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?



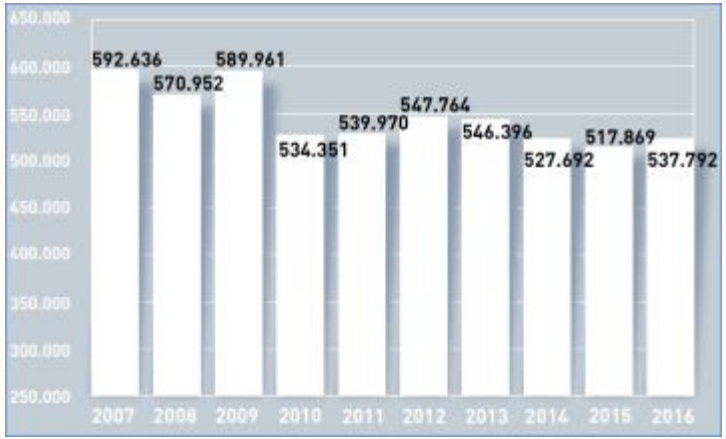
	2008	2009	2010	2011	2012	2013	2014	2015	2016
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550

Quelle: https://www.cert.at/reports/report_2016_chap05/content.html

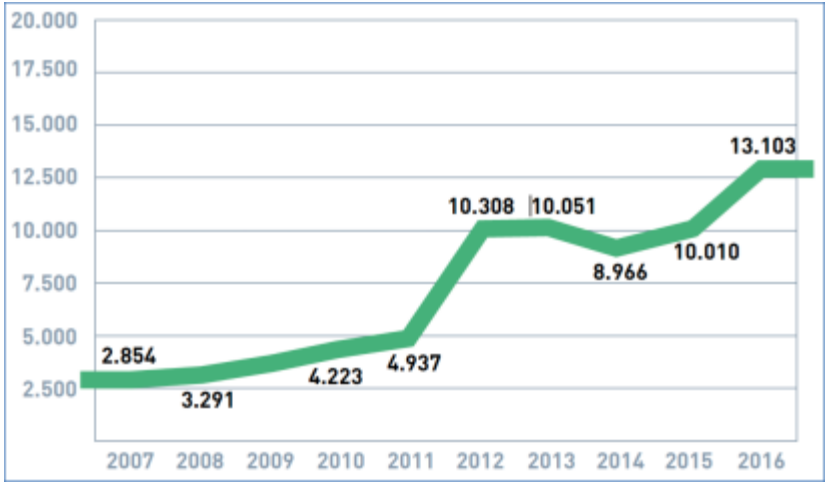


Quelle: https://www.cert.at/reports/report_2016_chap05/content.html

WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?



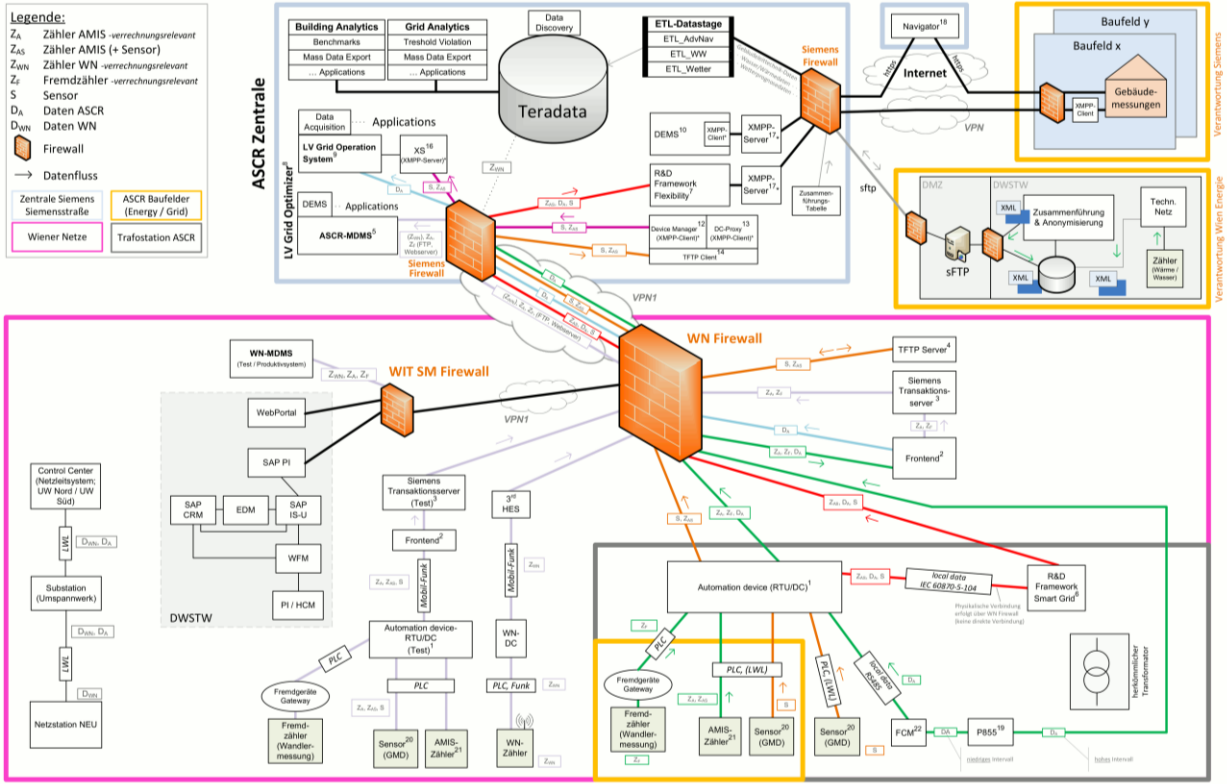
Gesamtkriminalität Anzeigen Quelle: http://www.bmi.gv.at/cms/BK/publikationen/files/30102016_Cybercrime_2015.pdf



Cybercrime Quelle: http://www.bmi.gv.at/cms/BK/publikationen/files/30102016_Cybercrime_2015.pdf

WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?

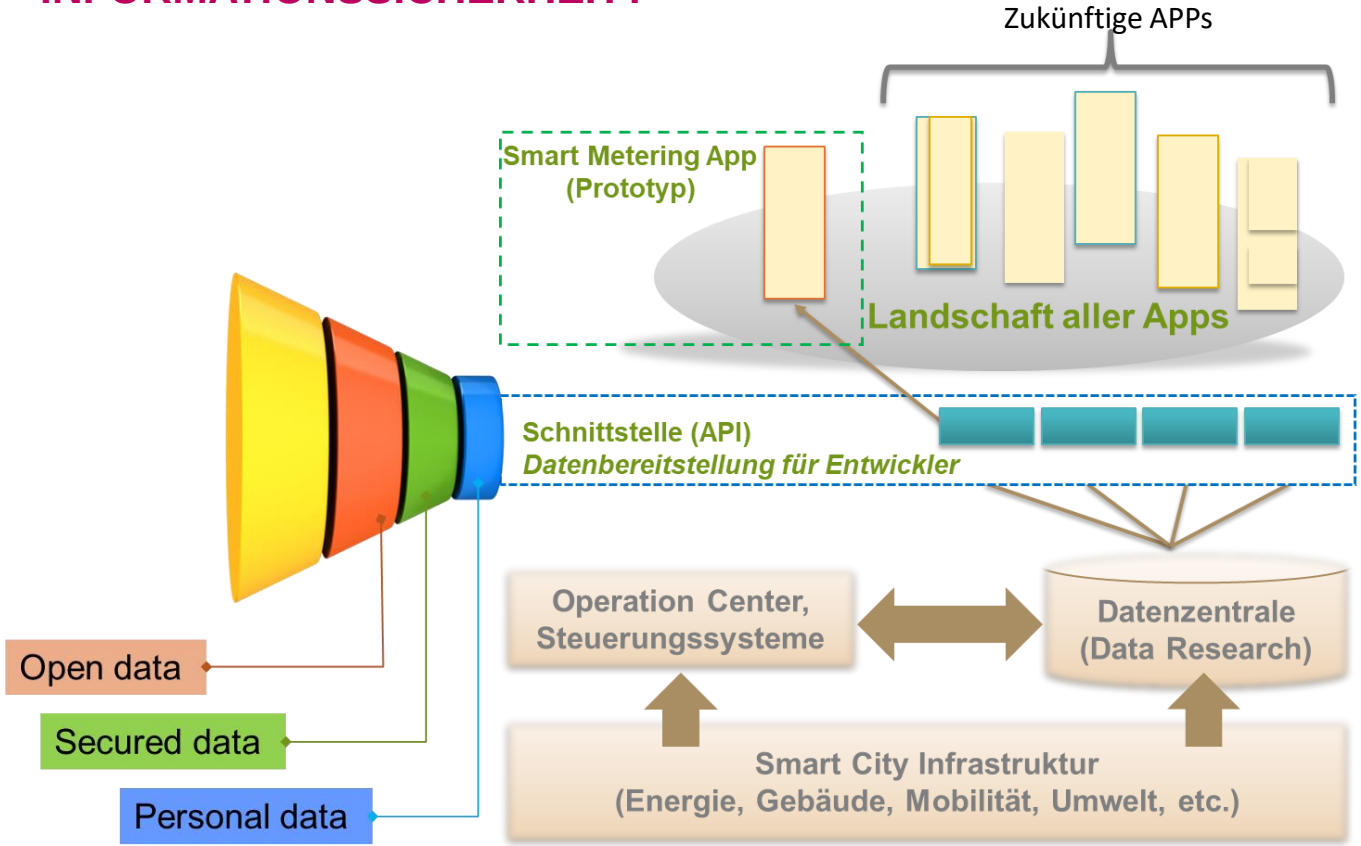
Smart City Wien – Moderne Infrastruktur eines Netzbetreibers



ASCR
Aspern Smart City Research
WORLD SMART CITY PROJECT AWARD WINNER 2016

WIENER NETZE

WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?



WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?

- Schnittstellen und Interkationen zwischen Domänen
- Datenmanagement
- Kommunikationsleitungen
- Konvergenz der Kommunikationsnetze
- Große Datenmengen durch Netzsensoren
- ……

WELCHE PROBLEMFELDER RESULTIEREN DARAUS FÜR DIE INFORMATIONSSICHERHEIT?

- Netz und Informationssicherheits-Richtlinie der EU
  - Die Richtlinie zur Netz und Informationssicherheit wurde am 6. Juli 2016 durch das Europäische Parlament verabschiedet
  - Die NIS-RL ist für alle EU-Mitgliedstaaten anzuwenden und bis Mai 2018 in nationales Recht umzusetzen
  - Ziel der Richtlinie ist es die Netz- und Informationssicherheit aller EU-Mitgliedstaaten zu erhöhen und somit die Tragweite, Häufigkeit und auch die Auswirkungen von Sicherheitsvorfällen zu minimieren.
  - Betreiber wesentlicher Dienste - Es sind jene Betreiber aus den in der NIS-RL angeführten Sektoren zu ermitteln, deren Dienste, wenn sie gestört sind, zu erheblichen Einschränkungen auf die Gesellschaft führen.
  - Ein erster Gesetzesentwurf ist noch ausständig, zu rechnen ist aber mit einer Meldepflicht für Sicherheitsvorfälle und mit der Einführung von sektorspezifischen Mindeststandards. Ebenso ist mit der Einführung von hohen Geldstrafen bei fahrlässigen Sicherheitsvorfällen zu rechnen!!

Datenschutzrechtliche Implikationen

DATENSCHUTZRECHTLICHE IMPLIKATIONEN

EU-DGSVO

- Die EU-Verordnung Nr. 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist mit 25. Mai 2016 in Kraft getreten und ist nach einer 24-monatigen Frist mit 25. Mai 2018 anzuwenden.
- Stärkung der Betroffenenrechte (mehr Transparenz; Verankerung des Rechts auf „Vergessenwerden“)
- Neuer Fokus auf die Datensicherheit (verpflichtende angemessene Sicherheitsvorkehrungen; Datenmissbräuche und Sicherheitsverletzungen müssen den Aufsichtsbehörden gemeldet werden)
- Bestellung von Datenschutzbeauftragten im öffentlichen Bereich
- Erhöhter Strafrahmen: Strafen bis zu 20 Millionen Euro beziehungsweise 4 Prozent des Konzernumsatzes sind möglich.

DPIA – Data Protection Impact Assesment (Datenschutz Folgenabschätzung)

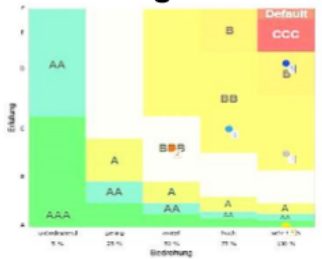
- Eine Risikobeurteilung für den Betroffenen aus der Verarbeitung seiner personenbezogenen Daten
- Analyse der vorhandenen technischen und organisatorischen Vorkehrungen bei der Verarbeitung von personenbezogenen Daten
- Identifikation von Verarbeitungstätigkeiten welche nach den Kriterien Verfügbarkeit, Vertraulichkeit, Integrität, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit bewertet werden
- Ergebnis →

Risiko Kennzahlen

AAA	: übererfüllt ***
AA	: übererfüllt **
A	: übererfüllt *
BBB	: Stand der Technik
BB	: unter gängiger Praxis
B	: leicht fahrlässig
CCC/Default	: grob fahrlässig

⇦

Scoring Modell



Der Wandel zu einem modernen Netzbetreiber im Sinne der Informationssicherheit

EXTERNE GREMIEN

- BKA
  - Bundeskanzleramt (NIS-Behörde) Aufgaben → die Koordination einer Strategie und eines jährlich erscheinenden Berichts zur Sicherheit von Netz- und Informationssystemen. Organisatorische/Strategische Behörde
- BM.I
  - Bundesministerium für Inneres (NIS-Behörde) Betrieb einer zentralen Anlaufstelle zum Informationsaustausch & Koordination der operativen Organisationen innerhalb des BM.I.
- CERT
  - Computer Notfallteam
- ECA Risikoanalyse
  - Risikoanalyse der IKT Strukturen der österreichischen Netzbetreiber (Netzbetreiber/OE/ECA).
- CSP
  - Cyber Security Plattform → zentrale Plattform Österreichs für die Kooperation zwischen dem privaten und öffentlichen Sektor in Sachen Cyber-Sicherheit und dem Schutz kritischer Infrastrukturen

EXTERNE GREMIEN VERBAND OE

- PG IKT-Sicherheit
- AK IKT-Sicherheit
- PG end2end Security Smart Metering

- Diverse bereits abgeschlossene Projektgruppen
  - Sicherheit der Zählerschnittstellen
  - Sicherheit im Smart Grid

- Anlassbezogene Arbeitskreise

INTERNE GREMIEN

IT-Sicherheitsarbeitskreis

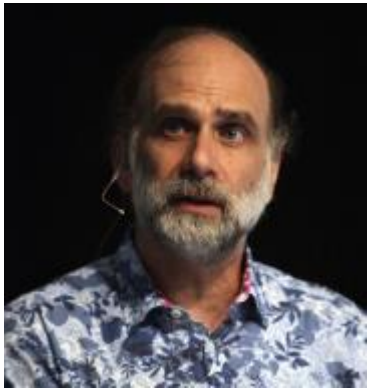
- Leitung Konzern CISO Herbert Schindelka
- Monatliche Sitzungen, im Bedarfsfall auch außerordentliche Sitzungen
- Entwicklung der konzernweit gültigen IT Sicherheitsrichtlinie
- Gremium für die Abstimmung und Diskussion von sicherheitsrelevanten Angelegenheiten (Policy Einstellungen, WLAN, Warnmeldungen usw.)

Informationssicherheitsgremium

- Entwicklung von unternehmensspezifischen Richtlinien
- Meldestelle für IT-Sicherheitsvorfälle im Unternehmen
- Analyse und Verarbeitung der vom Energy CERT versendeten Reports
- Etablierung von geordneten Meldestrukturen (die auch im Notfall, am Wochenende und auch bei Ausfall von Telefonanlagen, Mail usw. funktionieren)
- Erste Anlaufstelle für das Austrian Energy CERT und die NIS Behörden

AUSBLICK VON BRUCE SCHNEIER IN RICHTUNG IoT

„Wir bauen einen weltweiten Roboter und wir merken es nicht einmal. Wir bauen ein Internet das spürt, denkt und handelt. Ein Internet welches die Welt in einer direkten physischen Weise beeinflusst. Und da das Internet physisch unsere Welt beeinflusst, werden die Bedrohungen größer. Es sind die gleichen Computer, die gleichen Betriebssysteme, die gleichen Applikationen und die gleichen Verwundbarkeiten, aber es gibt einen grundlegenden Unterschied dazwischen ob meine Tabellenkalkulation abstürzt und ich meine Daten verliere oder ob die Software im Auto abstürzt und ich mein Leben verliere.“



Quelle: https://de.wikipedia.org/wiki/Bruce_Schneier