



# Aktuelle Entwicklungen im Bereich Cybercrime

Mag. (FH) Gert Seidl

Leiter Referat 1, Cybercrime Competence Center

BM.I – Bundeskriminalamt

Harald Wenisch

Sachverständiger für IT und Sicherheitsthemen

Sprecher der IT Security Experts Group WKO



# Agenda



- Anforderungen an IT-Sicherheitssysteme und Prozesse
- Worauf kommt es bei der Vorbeugung wirklich an
- Kritische Daten und Infrastruktur, was tun wenn der Hut brennt



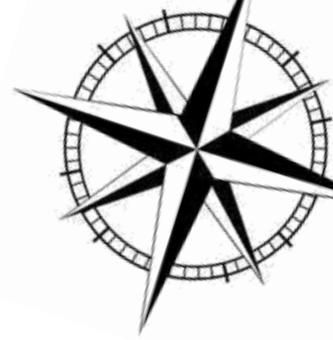
# Abgrenzung

- Cybersecurity
- Cybercrime
- Zuständigkeit der Polizei

# Zuständigkeit

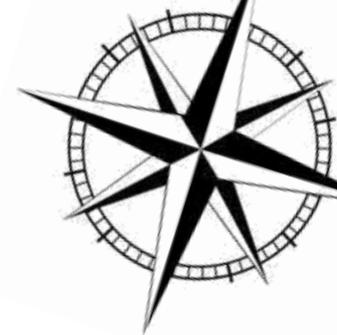
- Örtliche Zuständigkeit – Sachliche Zuständigkeit
- Der Generalist – Spezialisierung

# Wer ist die Security Experts Group ?



- 300 Personen im Verteiler
- Durchschnittlich 20 TeilnehmerInnen je Sitzung
- 180 aktive Mitglieder

# Wer ist die Security Experts Group ?



- Ziel
  - Schaffung von Awareness
  - Schaffung und Erhaltung von KnowHow bei den Mitgliedsbetrieben
  - Bindung der Mitglieder an den Fachverband
  - Schnittstelle für Sicherheitsprobleme
- Nutzen für Mitglieder
  - Kooperationen und Netzwerk
  - Plattform für Sicherheitsaktivitäten
  - Anlaufstelle für Security-Herausforderungen



.BK



REPUBLIK ÖSTERREICH  
BUNDEMINISTERIUM FÜR INNERES  
BUNDESKRIMINALAMT



# Kooperation Experts Group



## DEEPSEC

IN-DEPTH SECURITY CONFERENCE 2016 EUROPE — 8TH TO 11TH NOVEMBER 2016  
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

2016 Schedule Register Venue Call for Papers Blog 2013 2012 2011 2010 2009 2008 2007

**Trainings NOV 8-9**  
> 4-7 In-Depth Security Trainings

**Conference NOV 10-11**  
> 2 Tracks  
> 32 bleeding-edge Security Talks

**Events NOV 10-11**  
> Evening Programme  
> Hacker Lounge  
> Community Afterparty @ metalab



### About DeepSec

The Call for Papers for DeepSec 2016! is open! Submit your work looking for talk and workshop submissions! Make sure you check our [blog](#).

Bringing together the world's most renowned security professionals, academics, government, industry, and the underground hacker community.

#### Neutral

We are neutral and we stick to our principles: If a topic is interesting, we will consider a submission for our conferences. We will not discriminate on the basis of submitting a talk or attending our conference, that potential visitors share our stance and posture.

#### Novelty, Quality & Impact

When selecting talks or workshops from our submissions, we will not discriminate on the basis of anything else than the impact or relevance of that specific submission. Often we will accept a newcomer to the stage if the content is more promising than...

BSidesVienna 0x7E0 Index CFP Talks Schedule Venue Registration Sponsors Code of Conduct Past Events

### 2016 - INDEX

#### What's BSides?

“Each BSides is a community-driven framework for building events for and by information security community members. The goal is to expand the spectrum of conversation beyond the traditional confines of space and time. It creates opportunities for individuals to both present and participate in an intimate atmosphere that encourages collaboration. It is an intense event with discussions, demos, and interaction from participants. It is where conversations for the next-big-thing are happening.” – **Security BSides**



REPUBLIK ÖSTERREICH  
BUNDESMINISTERIUM FÜR INNERES  
BUNDESKRIMINALAMT



# Kooperation Experts Group



**IT-SICHER**.kaufen  
BESCHAFFUNGSPLATTFORM

**ifh** ///  
st. pölten

-  Standard Software
-  In Auftrag gegebene Software
-  Hardware mit integrierter Software

 Quelloffene Software

 Mindestanforderungen der CSP Austria

 Empfehlungen

## Beschaffung

Dieser Bereich dient als Beschaffungsunterstützung, um IT Sicherheitsanforderungen für ein Produkt zu formulieren. Die Anforderungen können sowohl in Ausschreibungen als auch als Checklisten bei einer Produktbeschaffung ohne Ausschreibung verwendet werden.

Die IT Sicherheitsanforderungen sind in folgende Kategorien gegliedert:

### Standard Software

IT Sicherheitsanforderungen für Standard-Software, die als vorgefertigte Produkte erworben werden können.

### In Auftrag gegebene Software

Zusätzliche IT Sicherheitsanforderungen für Individualsoftware, die gezielt für den Einsatz bei einem Kunden bzw. Unternehmen entwickelt wird.

### Hardware mit integrierter Software

Zusätzliche IT Sicherheitsanforderungen für Produkte, die sowohl Software- als auch Hardware-Komponenten beinhalten.

### Quelloffene Software

Bewertungskriterien für die Gegenüberstellung quelloffener Softwareprodukte.

### Mindestanforderungen der CSP Austria

IT Sicherheitsanforderungen der Arbeitsgruppe „Standardisierung und Zertifizierung“ der Cybersecurity Plattform Austria.

# Kooperation Experts Group



**KOMPETENT - VERLÄSSLICH -  
SICHER - DAS ABWEHRAMT**



**.BK**



REPUBLIK ÖSTERREICH  
BUNDEMINISTERIUM FÜR INNERES  
BUNDEKRIMINALAMT



# [www.it-safe.at](http://www.it-safe.at) – Sicherheit für KMU



 WKO ONLINE RATGEBER



## Herzlich Willkommen beim Online-Ratgeber it-safe!

Dieser Online-Ratgeber informiert Sie umfassend, wie es um die **IT-Sicherheit in Ihrem Unternehmen** bestellt ist.

Der Ratgeber richtet sich in erster Linie an EPU (Einpersonenunternehmen) und KMU (Klein- und Mittelbetriebe). Die Fragen können sowohl von der Geschäftsführung als auch von interessierten Mitarbeiter/innen beantwortet werden.

Sicherheit ist von vielen verschiedenen Komponenten abhängig. Der Online-Ratgeber befragt Sie zu Ihrer Betriebspraxis sowie zu den vier häufigsten Sicherheitsbedrohungen in Unternehmen: Angriffe auf Daten, Vermögen, Mensch und Reputation.

Nehmen Sie sich bitte 15 bis 20 Minuten Zeit für die Beantwortung. Dies ist eine wertvolle Investition in Ihre IT-Sicherheit. Sie erhalten dafür eine gründliche Analyse mit konkreten Umsetzungsvorschlägen und einen Vergleich mit anderen Unternehmen. Selbstverständlich können Sie Ihre Angaben auch zwischenspeichern und zu einem späteren Zeitpunkt unter der Adresse [restart.wkoratgeber.at](http://restart.wkoratgeber.at) wieder fortsetzen.

Haben Sie einen akuten **Security-Notfall?** Erste Hilfe dazu erhalten Sie schon nach der Beantwortung von drei kurzen Fragen.

Wir wünschen Ihnen viel Erfolg!

Weiter

## Ist Ihr Betrieb it-safe?

Jetzt den Online-Ratgeber testen:

[www.it-safe.at](http://www.it-safe.at)

**WKO**

WIRTSCHAFTSKAMMER ÖSTERREICH

**bmwfw**

Business & Marketing



**.BK**



REPUBLIK ÖSTERREICH  
BUNDESMINISTERIUM FÜR INNERES  
BUNDESKRIMINALAMT



CYBER CRIME  
COMPETENCE CENTER

**WKO**  

WIRTSCHAFTSKAMMER ÖSTERREICH  
Unternehmensberatung • IT

IT-Security Experts

# Webinar IT Security



Online Webinare  
**DIE WEBINARE**  
FÜR UNTERNEHMEN UND VEREINIGUNGEN



© WKO

### Wie kann ich meine MitarbeiterInnen einbinden?

- Sicherheitskultur
- Jede/r im Unternehmen ist Ziel
- Wer darf was?
- Innentäter
- regelmäßige Schulungen → Sicherheitshandbuch:  
<https://www.wko.at/Content.Node/it-safe/Mitarbeiter-Handbuch.html>



© WKO Service GmbH



© Sasa Dobrovodska/moodboard/Corbis

Seite 15

© WKO

# Kooperation Experts Group



BUNDESKANZLERAMT  ÖSTERREICH

CSP  AUSTRIA



**.BK**



REPUBLIK ÖSTERREICH  
BUNDEMINISTERIUM FÜR INNERES  
BUNDESKRIMINALAMT

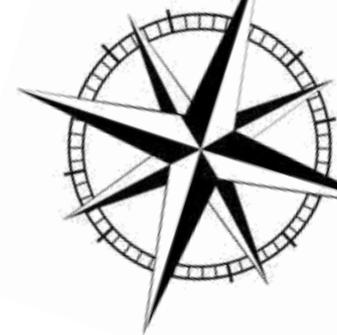


CYBER CRIME  
COMPETENCE CENTER



WIRTSCHAFTSKAMMER ÖSTERREICH  
Unternehmensberatung • IT  
IT-Security Experts

# Kooperation Experts Group



# Lage 2016

## Cybercrime Österreich 2007 - 2016



Das Jahr 2009 beinhaltet zwei Internetbetrugsfälle mit insgesamt 6624 Einzeldelikten

Quelle: .BK/PKS

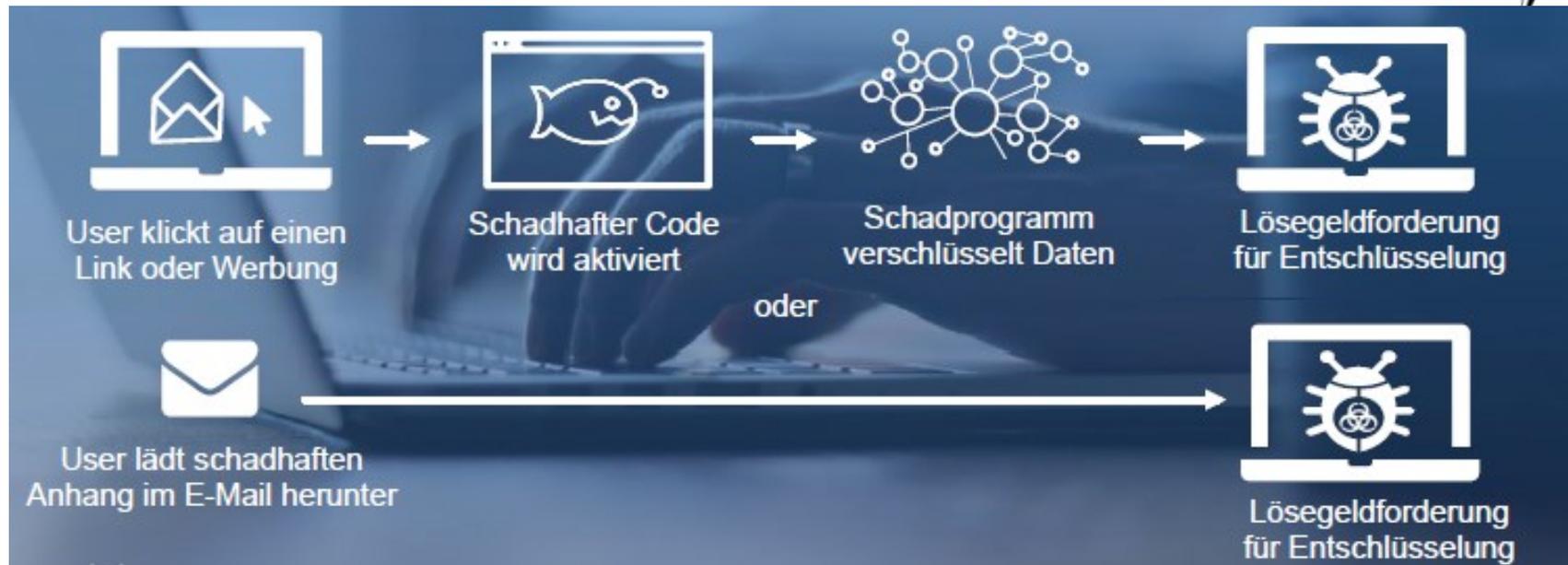
# Lage 2016

- National: Cybercrime Report (2015)
- Europa: IOCTA (2016)
  - Internet Organised Crime Threat Assessment
- <http://www.bmi.gv.at/cms/BK/publikationen/> - Internetkriminalität
- <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#tabs-0-bottom-2>

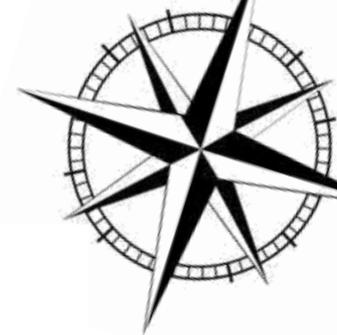
# Aktuelle Phänomene

- Ransomware
- DDoS
- CEO – Fraud / Inkassobetrug / Bestellbetrug

# Aktuelle Vorgehensweise der Angreifer

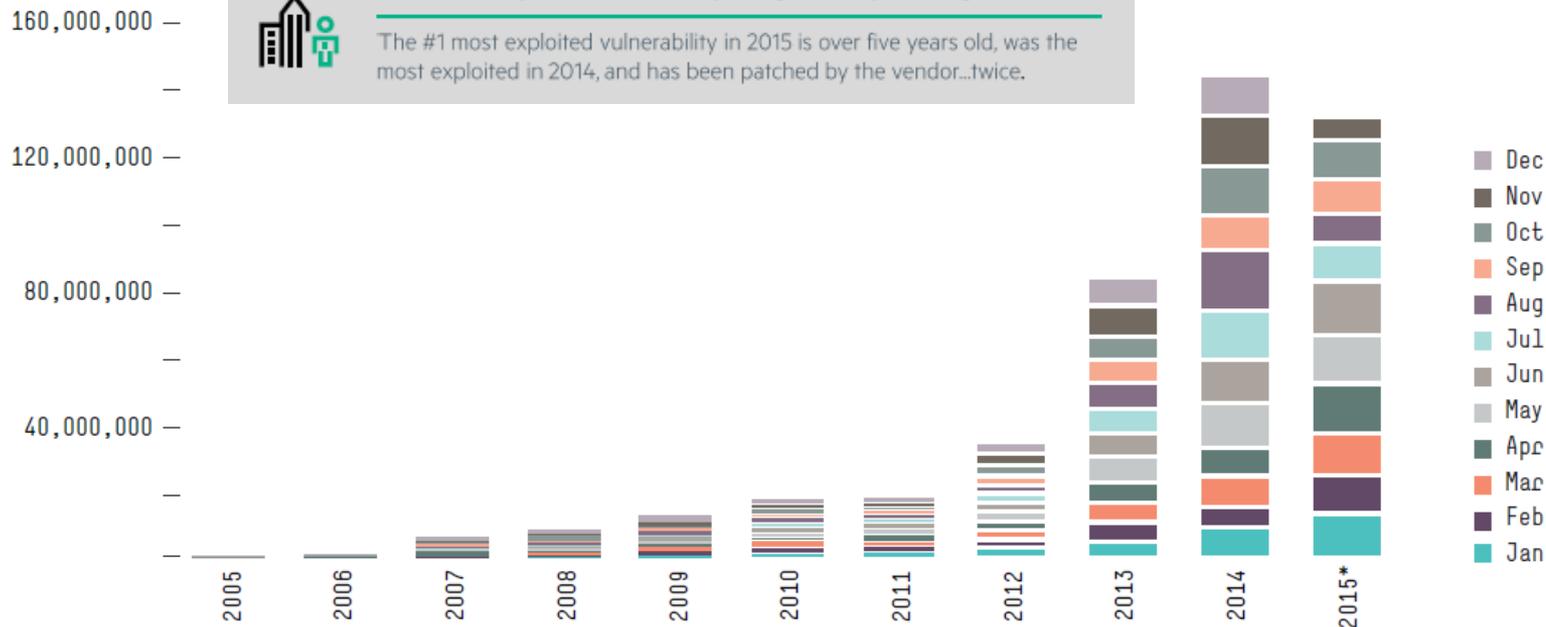


# Noch nie so viele Sicherheitslücke



## The industry didn't learn anything about patching in 2015

The #1 most exploited vulnerability in 2015 is over five years old, was the most exploited in 2014, and has been patched by the vendor...twice.



\* Note: 2015 data extends from Jan–Nov only.

# Exemplarische Schwerpunkte

- Schulungen
- Präventionsprojekte
- Kooperationen (Schlagwort PPP)

# Internationale Zusammenarbeit

- Europol
  - EC3 – European Cybercrime Center
- Interpol
  - DC2 – Digital Crime Center

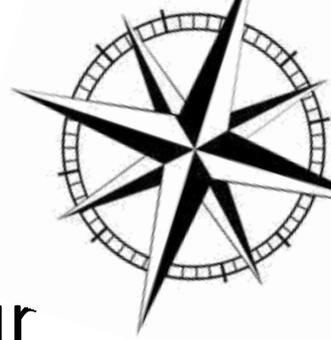
# Warum kaum ein Unternehmen vorbereitet ist



- Falsche Einschätzung
- Spare-Froh Gedanke
- Fehlendes Leadership
- Mangelnde Risiko Awareness
- Aushebeln bestehender und bewährter Vorkehrungen bzw. Prozesse



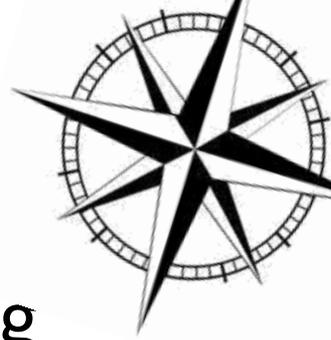
# Vorbeugung und Prävention



- Aufbau und Leben einer Sicherheitskultur
- Prozesse, klare Abläufe und Dokumentation
- Einheit der Führung
- Kommunikation
- Fire Drill & KVP

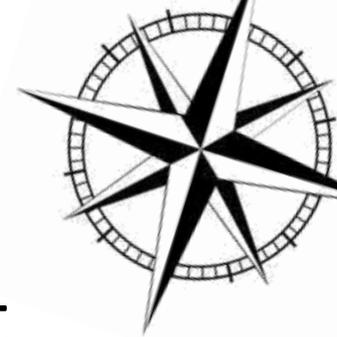


# Richtiger Umgang - Thema Krise



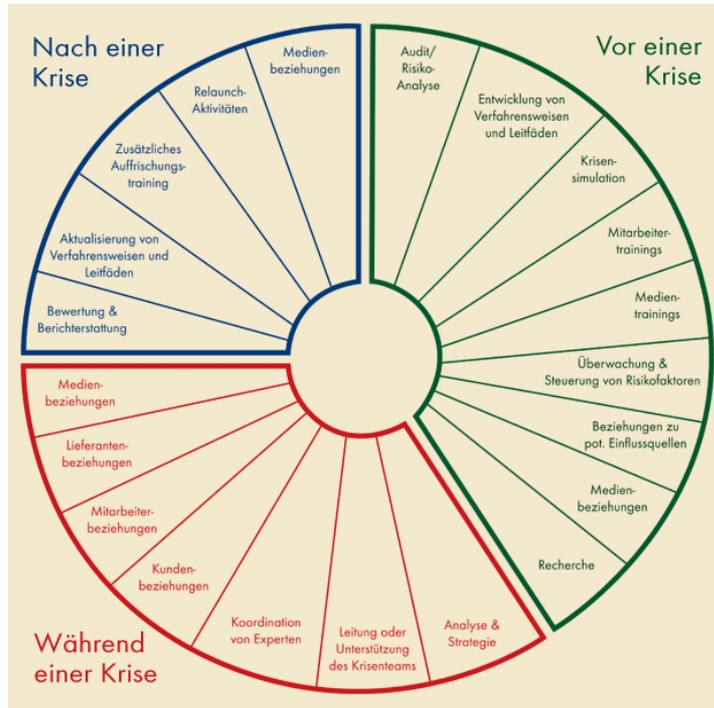
- Krisenmanagement durch Früherkennung
- Stabsarbeit muss geübt werden
- Nachlieferung von Ressourcen (techn. & personell) berücksichtigen
- Wie lange kann ich überleben (>3 Tage)

# Richtiger Umgang - Thema Krise



- Was ist wenn ich ein Gebiet länger nicht betreten/erreichen kann
- Krisenmanagement – eine ganzheitliche Aufgabe
- Aktive Unterstützung vorbereiten (PR Berater, ext. Krisenmanager ...)

# PR Krisen Management



## Gute Krisen Kommunikation!

- Über mehrere Kommunikationskanäle (Sozial-Web, Twitter, etc)
- PR verantwortlichen bereits in der Vorbereitung einschulen
- Kontakt mit Behörden und Medien bereits in der Vorbereitung aufnehmen
- Keine Schuldzuweisung

# AG Krisenmanagement



→ *Start 5.5.2017*

BUNDESKANZLERAMT  ÖSTERREICH

CSP  AUSTRIA



**DAY 17**  
DIGITALISIERUNG  
ERLEBEN

**.BK**



REPUBLIK ÖSTERREICH  
BUNDESMINISTERIUM FÜR INNERES  
BUNDESKRIMINALAMT

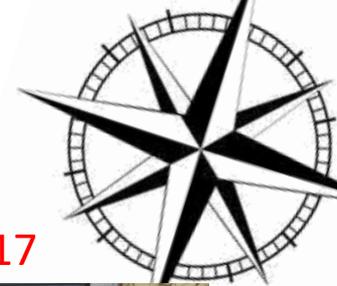


CYBER CRIME  
COMPETENCE CENTER



WIRTSCHAFTSKAMMER ÖSTERREICH  
Unternehmensberatung • IT  
**IT-Security Experts**

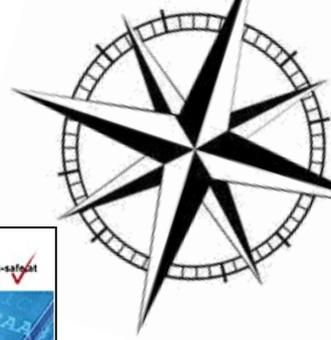
# Aus- und Weiterbildung



→ Nächster offizieller Termin 3.Oktober 2017



# Security Experts Group am eDAY



- Stand 14
- Stand 19

**GEWINNSPIEL eDAY**  
DIGITALISIERUNG ERLEBEN  
17.30 Uhr  
Stand #14

Die **WKO Experts Group IT Security** verlost  
**10 x Security Beratungsgutscheine**  
im Gesamtwert von **2.500 EUR**

**WKO**  
WIRTSCHAFTSKAMMER ÖSTERREICH  
Unternehmensberatung • IT  
IT-Security Experts

HAUPTINGANG

Der Gewinn kann nicht in Bar abgelöst werden. Der Rechtsweg ist ausgeschlossen. Teilnahmebedingungen finden sie am Stand.

**IT-Sicherheit**  
CHECKLISTS FOR EMPLOYEES' UND MITARBEITER  
IT-Sicherheit  
CHECKLISTS FOR EMPLOYEES' UND MITARBEITER  
IT-Sicherheit  
CHECKLISTS FOR EMPLOYEES' UND MITARBEITER

**10 FRAGEN**  
an die Geschäftsleitung  
zur Abwehr von  
Schadprogrammen

IT-Security Experts

# Vielen Dank für die Aufmerksamkeit



## Mag.(FH) Gert Seidl

Bundesministerium für Inneres  
Bundeskriminalamt, Büro 5.2  
C4 – Cybercrime Competence Center

C4 - Meldestelle:

<http://www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx>



## Harald Wenisch

Sachverständiger für IT und Sicherheitsthemen  
Sprecher der IT Security ExpertsGroup  
der Wirtschaftskammer Österreich

Tel.: +43/ 1/ 21 22441

email:[office@wenisch-consulting.com](mailto:office@wenisch-consulting.com)

Postfach 545  
1011 Wien