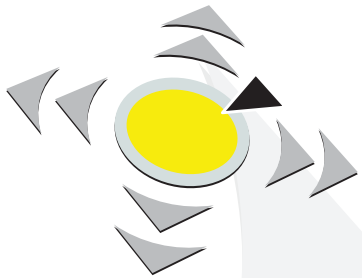
SPRING

GI FG SIDAR Graduierten-Workshop über Reaktive Sicherheit

Ulrich Flegel
Konrad Rieck

Gesellschaft für Informatik e.V.· Fachbereich Sicherheit
Fachgruppe **Security** · **Intrusion Detection and Response**

12. Juli 2006




DIMVA 2004


Spring

Idee von SPRING

Ziele

- Förderung des wissenschaftlichen Nachwuchses
- frühzeitige themenbezogene Vernetzung
- zwanglos Erfahrungen sammeln (Betreuer bleiben draußen ;-)

Kernmaßnahmen

Beiträge: möglichst breiter Überblick

- auch laufende oder (bald) publizierte Arbeiten
- Themen aus Diplomarbeit oder Dissertation
- keine Papierauswahl

Kosten: möglichst viele sollen teilnehmen können

- keine Teilnahmegebühren (Finanzierung durch SIDAR)
- Reduktion der Notwendigkeit von Übernachtungen
- argumentierbarer Reisebedarf: Vortrag und Publikation

Idee von SPRING

Ziele

- Förderung des wissenschaftlichen Nachwuchses
- frühzeitige themenbezogene Vernetzung
- zwanglos Erfahrungen sammeln (Betreuer bleiben draußen ;-)

Kernmaßnahmen

Beiträge: möglichst breiter Überblick

- auch laufende oder (bald) publizierte Arbeiten
- Themen aus Diplomarbeit oder Dissertation
- keine Papierauswahl

Kosten: möglichst viele sollen teilnehmen können

- keine Teilnahmegebühren (Finanzierung durch SIDAR)
- Reduktion der Notwendigkeit von Übernachtungen
- argumentierbarer Reisebedarf: Vortrag und Publikation

Idee von SPRING

Ziele

- Förderung des wissenschaftlichen Nachwuchses
- frühzeitige themenbezogene Vernetzung
- zwanglos Erfahrungen sammeln (Betreuer bleiben draußen ;-)

Kernmaßnahmen

Beiträge: möglichst breiter Überblick

- auch laufende oder (bald) publizierte Arbeiten
- Themen aus Diplomarbeit oder Dissertation
- keine Papierauswahl

Kosten: möglichst viele sollen teilnehmen können

- keine Teilnahmegebühren (Finanzierung durch SIDAR)
- Reduktion der Notwendigkeit von Übernachtungen
- argumentierbarer Reisebedarf: Vortrag und Publikation

Die GI-Fachgruppe SIDAR

Der Name **SIDAR**

- Security – Intrusion Detection and Response
- Erkennung und Beherrschung von Vorfällen der Informationssicherheit

Themenschwerpunkte **Reaktive Sicherheit**

Verwundbarkeitsanalyse: z.B.

- neue Verwundbarkeiten
- Verwundbarkeits-Scanner

Angriffserkennung: z.B.

- Intrusion Detection
- IT-Frühwarnung
- Viren-Scanner
- Wurm-Abwehr

Vorfallsbehandlung: z.B.

- Computer Emergency Response Teams (CERTs)

IT-Forensik: z.B.

- Spurensicherung und -analyse zur Vorfallsrekonstruktion
- Angreiferverfolgung

Die GI-Fachgruppe SIDAR

Der Name **SIDAR**

- Security – Intrusion Detection and Response
- Erkennung und Beherrschung von Vorfällen der Informationssicherheit

Themenschwerpunkte **Reaktive Sicherheit**

Verwundbarkeitsanalyse: z.B.

- neue Verwundbarkeiten
- Verwundbarkeits-Scanner

Angriffserkennung: z.B.

- Intrusion Detection
- IT-Frühwarnung
- Viren-Scanner
- Wurm-Abwehr

Vorfallsbehandlung: z.B.

- Computer Emergency Response Teams (CERTs)

IT-Forensik: z.B.

- Spurensicherung und -analyse zur Vorfallsrekonstruktion
- Angreiferverfolgung

Themengebiets-Ansprechpartner

Verwundbarkeitsanalyse

- Marc Heuse — marc.heuse@nruns.com
- Oliver Heinz — heinz@arago.de
- Oliver Göbel — goebel@cert.uni-stuttgart.de

Intrusion Detection

- Roland Büschkes — roland.bueschkes@t-mobile.de
- Michael Meier — michael.meier@udo.edu

Malware

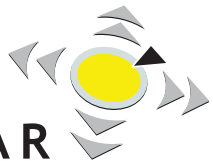
- Jens Nedon — nedon@consecur.de
- Dirk Schadt — Dirk.Schadt@ca.com
- Toralv Dirro — toralv_dirro@mcafee.com

Vorfallsbehandlung

- Detlef Günther — detlef.guenther@volkswagen.de
- Oliver Göbel — goebel@cert.uni-stuttgart.de

IT-Forensik

- Jens Nedon — nedon@consecur.de
- Dirk Schadt — Dirk.Schadt@ca.com
- Dietmar Mauersberger — dietmar.mauersberger@polizei.bayern.de



Vision

- Es gibt geeignete und nutzbare Methoden und Verfahren zur Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Der Nutzen dieser Methoden und Verfahren ist allgemein bekannt. Methoden und Verfahren werden von Anwendern und Verantwortlichen akzeptiert.
- Der breite Einsatz dieser Methoden und Verfahren erfolgt im Rahmen wirtschaftlicher und gesellschaftlicher Abwägungen.
- Bislang getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.

Vision

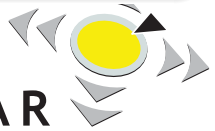
- Es gibt geeignete und nutzbare Methoden und Verfahren zur Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Der Nutzen dieser Methoden und Verfahren ist allgemein bekannt. Methoden und Verfahren werden von Anwendern und Verantwortlichen akzeptiert.
- Der breite Einsatz dieser Methoden und Verfahren erfolgt im Rahmen wirtschaftlicher und gesellschaftlicher Abwägungen.
- Bislang getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.

Vision

- Es gibt geeignete und nutzbare Methoden und Verfahren zur Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Der Nutzen dieser Methoden und Verfahren ist allgemein bekannt. Methoden und Verfahren werden von Anwendern und Verantwortlichen akzeptiert.
- Der breite Einsatz dieser Methoden und Verfahren erfolgt im Rahmen wirtschaftlicher und gesellschaftlicher Abwägungen.
- Bislang getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.

Vision

- Es gibt geeignete und nutzbare Methoden und Verfahren zur Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Der Nutzen dieser Methoden und Verfahren ist allgemein bekannt. Methoden und Verfahren werden von Anwendern und Verantwortlichen akzeptiert.
- Der breite Einsatz dieser Methoden und Verfahren erfolgt im Rahmen wirtschaftlicher und gesellschaftlicher Abwägungen.
- Bislang getrennt betrachtete Aspekte wie reaktive, präventive und organisatorische Methoden und Verfahren wirken integriert zusammen.



Mission

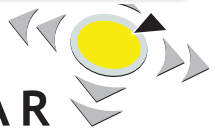
- Neutraler Ansprechpartner für die Fachleute und Wissenschaftler, die die Entwicklung geeigneter Methoden und Verfahren vorantreiben.
- Förderung eines fachlich integrierenden Austausches über präventive, reaktive und organisatorische Methoden und Verfahren auf nationaler und internationaler Ebene.
- Verbreitung des Wissens über Methoden und Verfahren sowie die Schaffung eines entsprechenden Bewußtseins für deren Vorteile, Nutzen und Wirtschaftlichkeit.
- Förderung und Mitgestaltung der Entwicklung von Methoden und Verfahren.

Mission

- Neutraler Ansprechpartner für die Fachleute und Wissenschaftler, die die Entwicklung geeigneter Methoden und Verfahren vorantreiben.
- Förderung eines fachlich integrierenden Austausches über präventive, reaktive und organisatorische Methoden und Verfahren auf nationaler und internationaler Ebene.
- Verbreitung des Wissens über Methoden und Verfahren sowie die Schaffung eines entsprechenden Bewußtseins für deren Vorteile, Nutzen und Wirtschaftlichkeit.
- Förderung und Mitgestaltung der Entwicklung von Methoden und Verfahren.

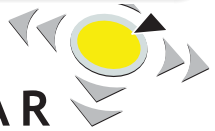
Mission

- Neutraler Ansprechpartner für die Fachleute und Wissenschaftler, die die Entwicklung geeigneter Methoden und Verfahren vorantreiben.
- Förderung eines fachlich integrierenden Austausches über präventive, reaktive und organisatorische Methoden und Verfahren auf nationaler und internationaler Ebene.
- Verbreitung des Wissens über Methoden und Verfahren sowie die Schaffung eines entsprechenden Bewußtseins für deren Vorteile, Nutzen und Wirtschaftlichkeit.
- Förderung und Mitgestaltung der Entwicklung von Methoden und Verfahren.



Mission

- Neutraler Ansprechpartner für die Fachleute und Wissenschaftler, die die Entwicklung geeigneter Methoden und Verfahren vorantreiben.
- Förderung eines fachlich integrierenden Austausches über präventive, reaktive und organisatorische Methoden und Verfahren auf nationaler und internationaler Ebene.
- Verbreitung des Wissens über Methoden und Verfahren sowie die Schaffung eines entsprechenden Bewußtseins für deren Vorteile, Nutzen und Wirtschaftlichkeit.
- Förderung und Mitgestaltung der Entwicklung von Methoden und Verfahren.



Dienstleistungen und Aktivitäten

- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Dienstleistungen und Aktivitäten

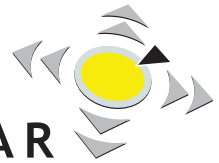
- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Dienstleistungen und Aktivitäten

- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Herzlichen Dank!

- Redner
- Autoren
- Moderatoren
- DIMVA-Tagungsbüro



Programm

Verwundbarkeiten und Malware

Moderation: *Ulrich Flegel*

Realisierungsaspekte bei Intrusion Detection

Moderation: *Konrad Rieck*

Modellgenerierung und -validierung

Moderation: *Robin Sommer*

Neue Technologien

Moderation: *Ulrich Flegel*

Incident Management und Forensik

Moderation: *Bernhard Hämmerli*

Programm

Verwundbarkeiten und Malware

Moderation: *Ulrich Flegel*

Realisierungsaspekte bei Intrusion Detection

Moderation: *Konrad Rieck*

Modellgenerierung und -validierung

Moderation: *Robin Sommer*

Neue Technologien

Moderation: *Ulrich Flegel*

Incident Management und Forensik

Moderation: *Bernhard Hämmerli*

Programm

Verwundbarkeiten und Malware

Moderation: *Ulrich Flegel*

Realisierungsaspekte bei Intrusion Detection

Moderation: *Konrad Rieck*

Modellgenerierung und -validierung

Moderation: *Robin Sommer*

Neue Technologien

Moderation: *Ulrich Flegel*

Incident Management und Forensik

Moderation: *Bernhard Hämmerli*

Programm

Verwundbarkeiten und Malware

Moderation: *Ulrich Flegel*

Realisierungsaspekte bei Intrusion Detection

Moderation: *Konrad Rieck*

Modellgenerierung und -validierung

Moderation: *Robin Sommer*

Neue Technologien

Moderation: *Ulrich Flegel*

Incident Management und Forensik

Moderation: *Bernhard Hämmerli*

Programm

Verwundbarkeiten und Malware

Moderation: *Ulrich Flegel*

Realisierungsaspekte bei Intrusion Detection

Moderation: *Konrad Rieck*

Modellgenerierung und -validierung

Moderation: *Robin Sommer*

Neue Technologien

Moderation: *Ulrich Flegel*

Incident Management und Forensik

Moderation: *Bernhard Hämmerli*

Bitte Mobiltelefone **lautlos** schalten

SIDAR

Workshop-Unterlagen

- Namensschild
- Abstractsammlung
- Programm
- Teilnehmerliste (Stand: 11. Juli)
- Umgebungsplan
- Flyer:
  - DIMVA 2006

Gemeinsames Mittagessen: 12:30 – 14:00 Uhr

Adresse

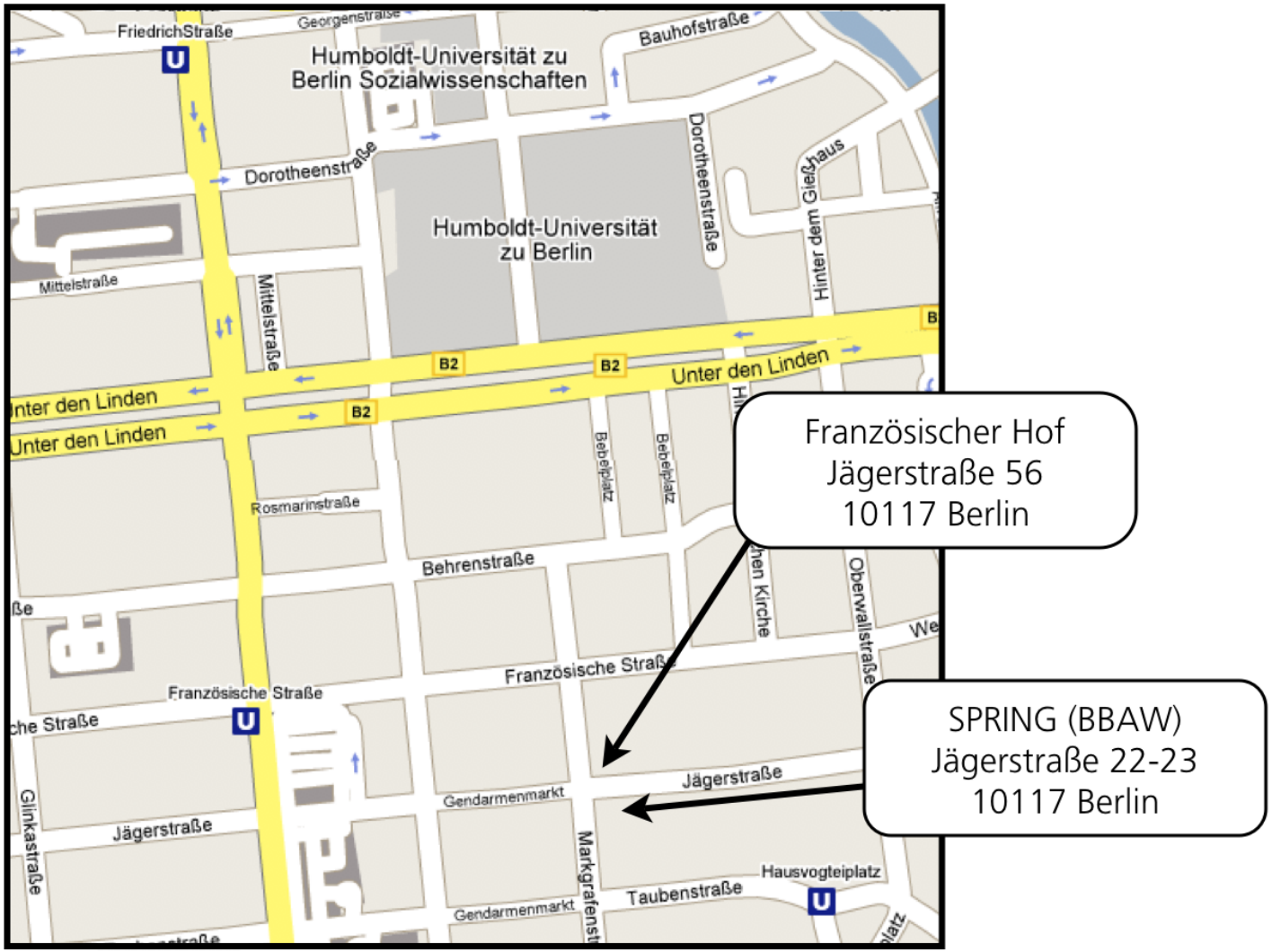
Französischer Hof
Jägerstraße 56
“direkt gegenüber”

Hauptgang mit Dessert 10,- EUR p.P., Selbstzahler

a) Schweinerollbraten mit saisonalem Gemüse und Kräuterkartoffeln
b) Gebratenes Zanderfilet mit Rahmspinat und Basmatireis
\+ Dessert: Rote Grütze mit Vanillesoße

Gemeinsames Mittagessen: Französischer Hof

Jägerstraße 56

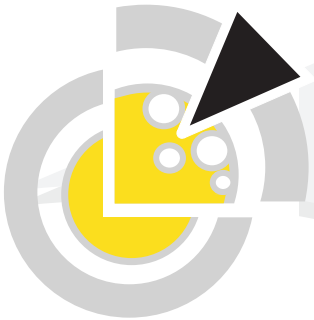


Rückmeldungen zur ersten SPRING

auch an: ulrich.flegel@udo.edu

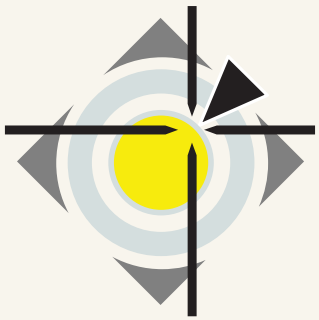
- Fortsetzung SPRING erwünscht?
- Gewünschter Turnus?
- Was soll in dieser Form beibehalten werden?
- Verbesserungsvorschläge?
- Freiwillige für lokale Organisation?

weitere SIDAR-Veranstaltungen



DIMVA 2006, direkt im Anschluß, 13./14. Juli, Berlin

- internationale Tagung
- Themen: Intrusion Detection, Malware-Bekämpfung, Verwundbarkeitsanalyse
- Hauptvortäge internationaler Experten
- Live-Übertragung CIPHER: internationaler Capture-The-Flag-Wettbewerb
- Rump-Session: Aktuelles und Amüsantes
- Spreeboot-Dinner mit Vortrag aus dem Bundesinnenministerium



IMF 2006, 18./19. Oktober, Stuttgart

- internationale Tagung
- Themen: Incident Management, IT-Forensik

Gemeinsamer Ausklang ab 22:00 Uhr

Adresse

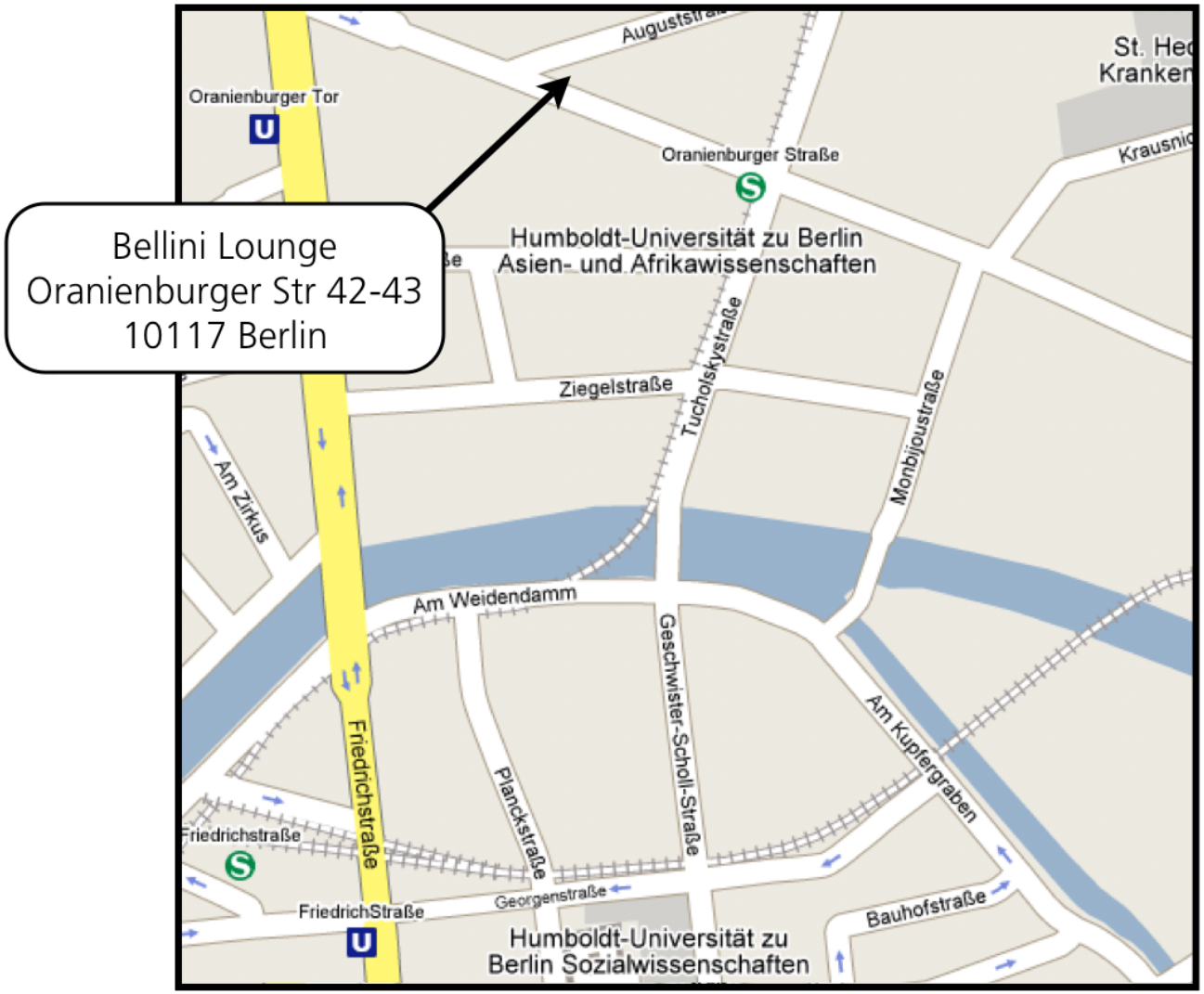
Bellini Lounge
Oranienburger Straße 42 – 43
U-Bahn-Haltestelle: Oranienburger Tor
S-Bahn-Haltestelle: Oranienburger Straße

Vorher: Empfehlenswerte Restaurants in der Nähe der Bellini Lounge

- Mirchi: Asiatische Crossover-Küche — Oranienburger Str. 50
- Amrit: Indische Küche — Oranienburger Str. 45
- Oranium: Internationale Küche — Oranienburger Str. 33

Gemeinsamer Ausklang: Bellini Lounge

Oranienburger Straße 42 – 43



Bleibt nur noch zu wünschen

Viel Spaß in Berlin
und
bei der DIMVA!

bzw.

Eine gute Heimfahrt!

Overview