



Das Deutsche Anti-Botnetz- Beratungszentrum

Cornelia Schildt

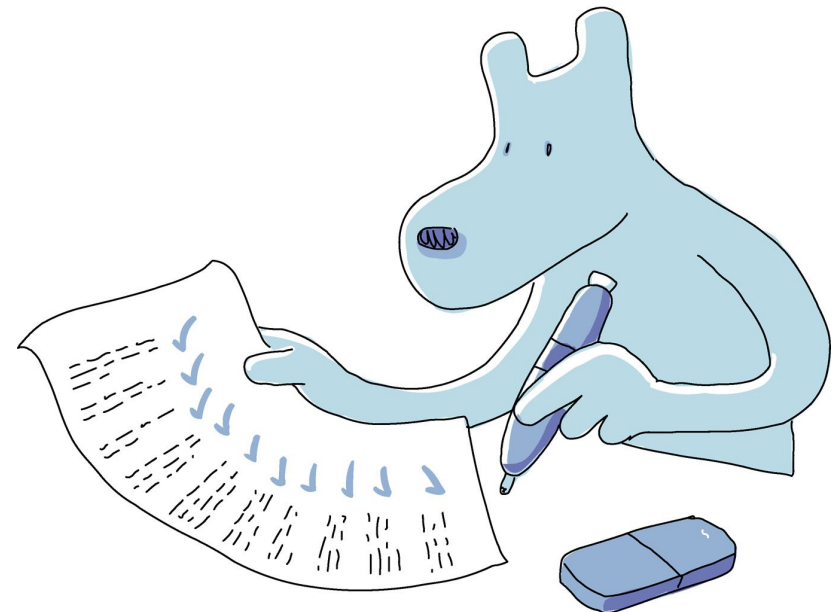
Bundesamt für Sicherheit in der Informationstechnik
Referat Internetsicherheit

ViS!T 7. - 8.9.2010 Bern



Agenda

- Aktuelle Situation
- Ziele des Anti-Botnet-Beratungszentrums
- Ablauf
 - Erkennung der Infektionen
 - Benachrichtigung der Kunden
 - Zentrale Webseite
 - DE-Cleaner und DE-Cleaner Rettungssystem
 - Telefonische Unterstützung
- Fazit





Aktuelle Situation

□ eleven:

- 100% Wachstum Spam über die letzten 12 Monate
- Typischerweise >95% der E-Mail an Unternehmen sind Spam
- Mehr als 20 Mio. verschiedene Adressen können weltweit allein Bots zugeordnet werden

□ Symantec:

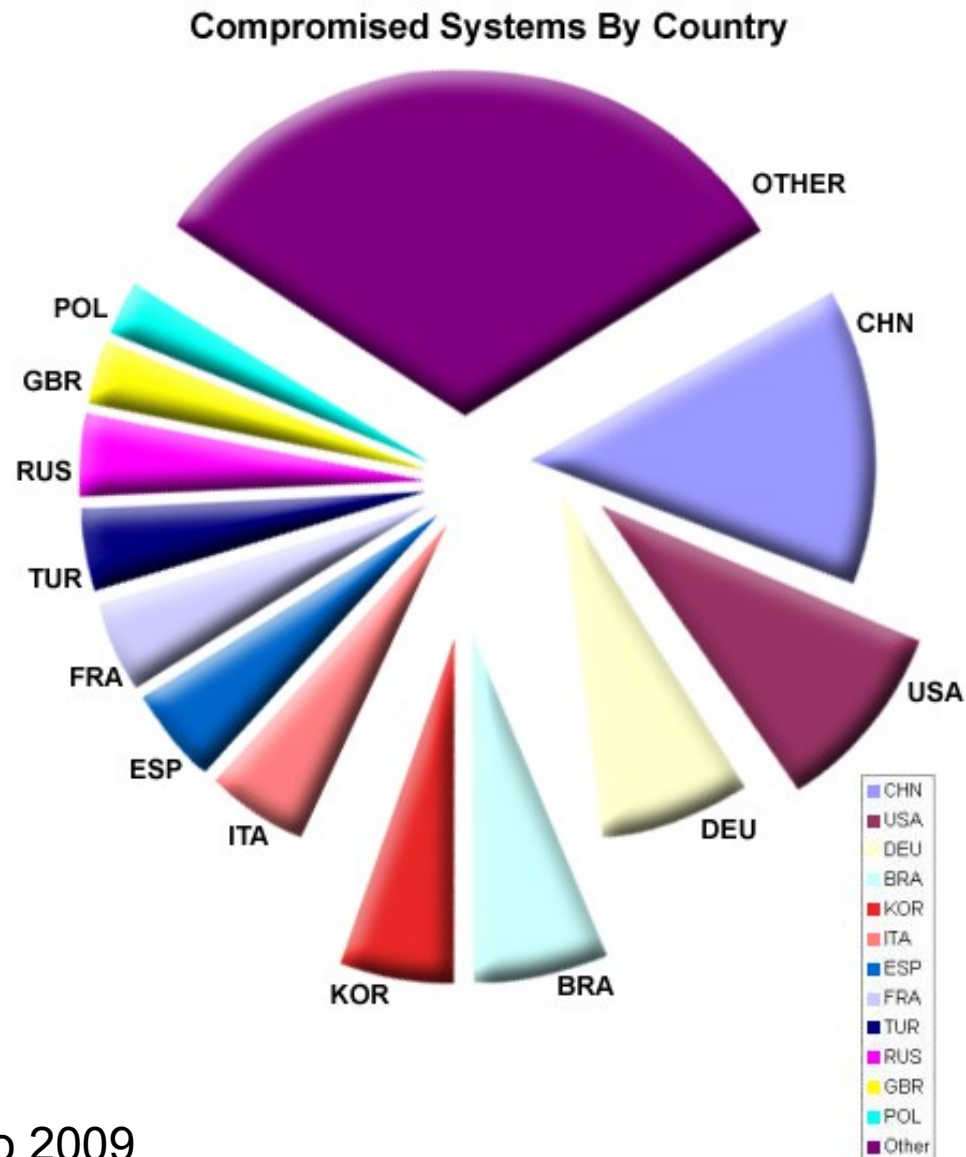
- 80% der Spams werden über Botnetze geschickt
- 13.000 Webseiten werden pro Tag infiziert

□ Trend Micro:

- Von 100 Mio. IP-Adressen
 - 80% der infizierten Rechner sind mehr als 30 Tage infiziert!
 - 50% der infizierten Rechner sind mehr als 300 Tage infiziert!



Länderverteilung





Spam Juli 2010

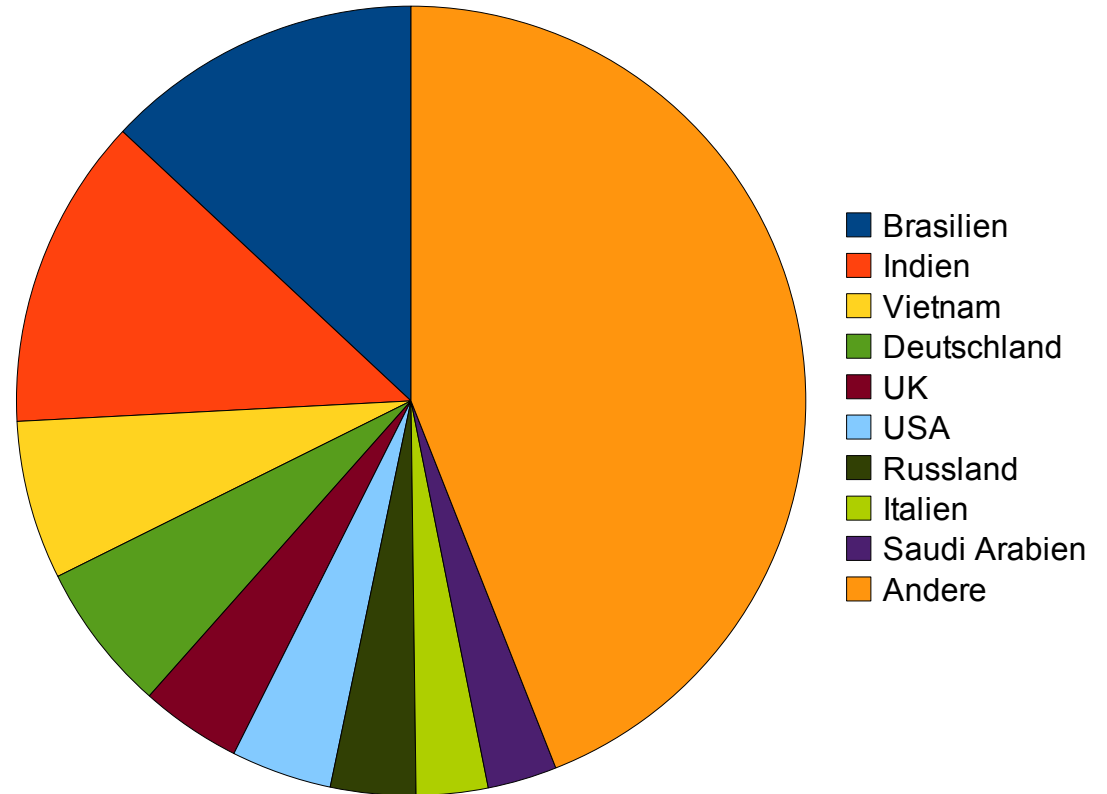
4. Platz
Deutschland

...

...

...

49. Platz
Japan



Quelle: BSI



Top 5 Bedrohungen durch Botnetze

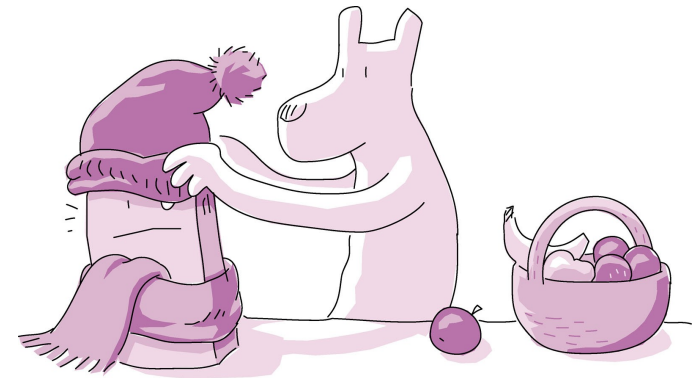
Bedrohung	2007	2009	Prognose
SPAM	↑	↑	↑
Identitätsdiebstahl	↑	↑	↑
DDoS	↑	↑	↑
Trojanische Pferde	↑	↑	↑
Spyware	↑	↑	↑

Botnetze sind schon jetzt sehr gefährlich und die Bedrohung wird weiter zunehmen.



Was kann der Nutzer tun?

- ❑ Empfohlene Schutzmaßnahmen auf Seiten der Nutzer
 - ❑ Anti-Viren-Produkte mit aktuellen Signaturen
 - ❑ Personal Firewalls
 - ❑ Automatische Systemupdates
 - ❑ Regelmäßiges Update von Anwendungen
 - ❑ Vorsicht beim Umgang mit E-Mail-Anhängen
 - ❑ Vorsicht beim Umgang mit Aktiven Inhalten
 - ❑ Gesundes Misstrauen
 - ❑ ...





Aber ...

- ❑ Maßnahmen haben nicht den gewünschten Erfolg
 - ❑ Benutzer sind überfordert
 - ❑ Benutzer wähnen sich in Sicherheit
 - ❑ Benutzer merken nicht, dass sie Teil eines Botnetzes sind

→ **Benutzer sind Opfer und werden gleichzeitig zum Täter ohne dies zu bemerken!**



Ziele des ABBZ

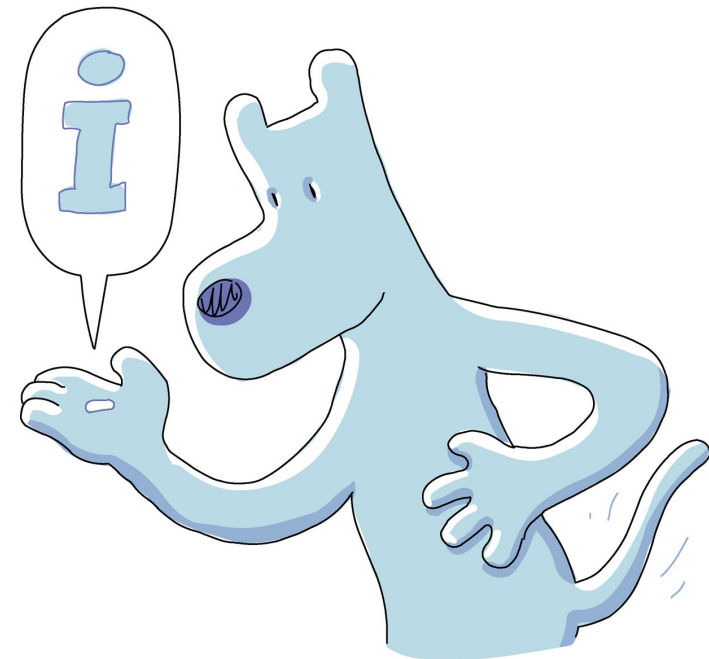
- ❑ Unterstützung der Benutzer bei der Desinfektion
- ❑ Bekämpfung der Botnetze
- ❑ Deutschland nicht mehr in der TOP 10

- ❑ Eco-Verband der deutschen Internetwirtschaft e.V baut Deutsches Anti-Botnetz-Beratungszentrum auf
- ❑ Bundesamt für Sicherheit in der Informationstechnik und Bundesministerium des Inneren unterstützen dabei



Vorgehen bei der Botnetzbekämpfung

- ❑ Erkennung der infizierten System
- ❑ Benachrichtigung der Benutzer
- ❑ Besuch der Webseite
- ❑ Download des DE-Cleaners
- ❑ Ggf. Unterstützung durch Call-Center
- ❑ Bereinigung des Systems
- ❑ Verhinderung der Neuinfektion





Erkennen und Benachrichtigen

- Infizierte Systeme werden durch Provider erkannt
 - Spamtraps
 - Honeypots
- Austausch der Informationen untereinander

- Benachrichtigung der infizierten Kunden möglich über
 - E-Mail, Post, Vorschaltseite, Browserplugin
 - **Keine Sperrung der Nutzer!**



Zentrale Webseite

□ Informieren

- Hintergrundinformationen zu Schadprogrammen, Botnetzen und dem Projekt

□ Säubern

- DE-Cleaner
- DE-Cleaner Rettungssystem-CD
- Weitere Tools wie Online-Scanner

□ Vorbeugen

- Maßnahmen zur Vermeidung von Neuinfektionen wie Updates, AV-Produkte,...

www.botfrei.de online ab 15.September 2010



DE-Cleaner

- ❑ Zusammenarbeit mit verschiedenen Herstellern von Anti-Viren-Programmen
- ❑ Standalone-Tool, das einfach zu bedienen ist
- ❑ Fokus auf Entfernung des Bots (im speziellen Top 10 Botnetze)
- ❑ Ersetzt das AV-Produkt nicht



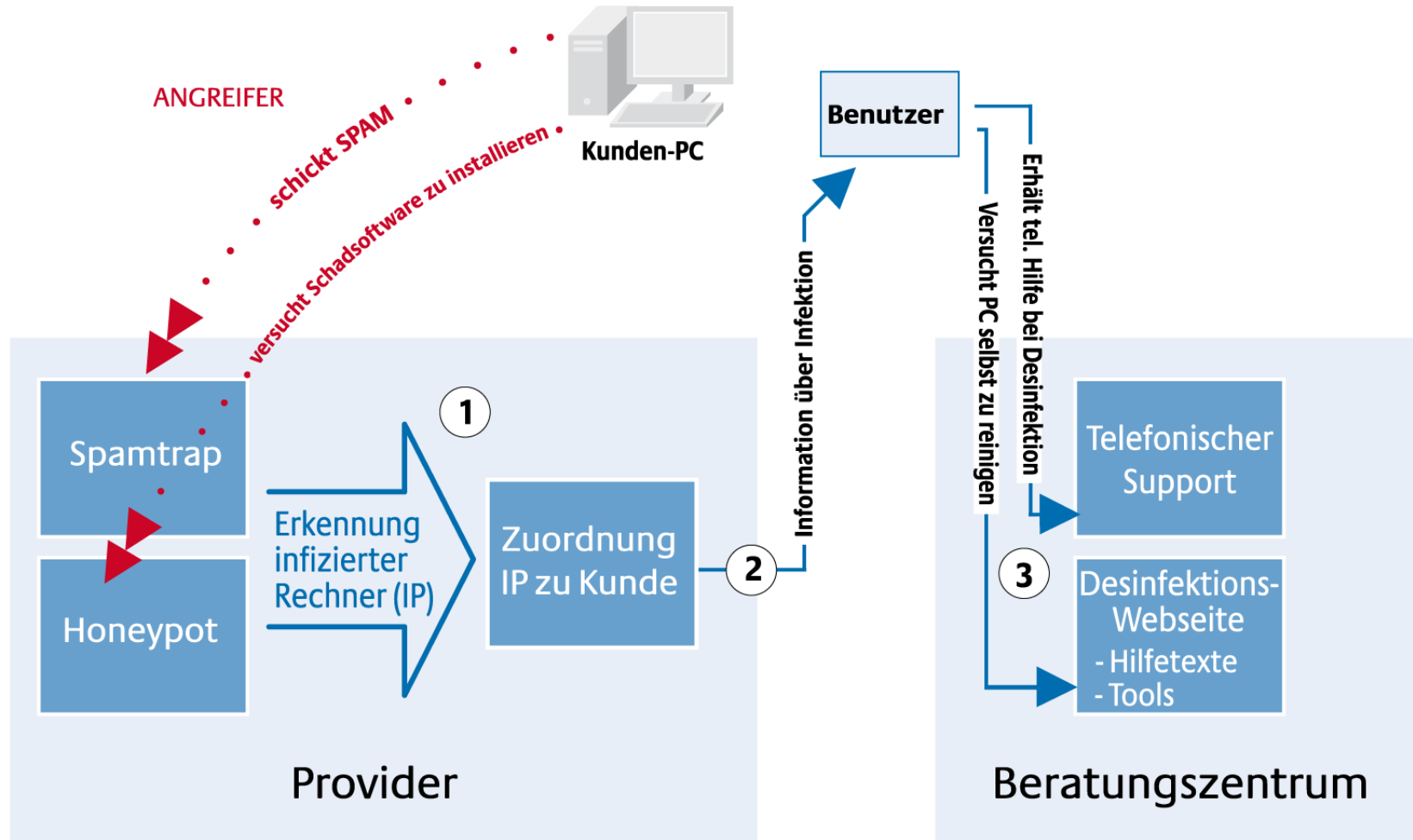
DE-Cleaner Rettungssystem

- Boot-fähige CD
- Kann so auch Schadprogramme entfernen, die tief im System stecken oder sich vor dem Betriebssystem tarnen
- Höhere Erkennungsrate
- Etwas komplexer als DE-Cleaner
- Unterstützt Signatur-Updates

- Kooperation mit ComputerBild (Heft-CD) und Avira



Ablauf der Beratung





Call-Center

- ❑ Benutzer, die alleine mit der Webseite und den bereitgestellten Programmen die Infektion nicht entfernen können
- ❑ Provider vergibt eindeutigen Voucher und Telefonnummer
- ❑ Benutzer kontaktiert Call-Center
 - ❑ 1st- Level-Support
 - ❑ 2nd -Level-Support
 - ❑ Geplante Servicezeiten: Mo-Sa 9-21 Uhr

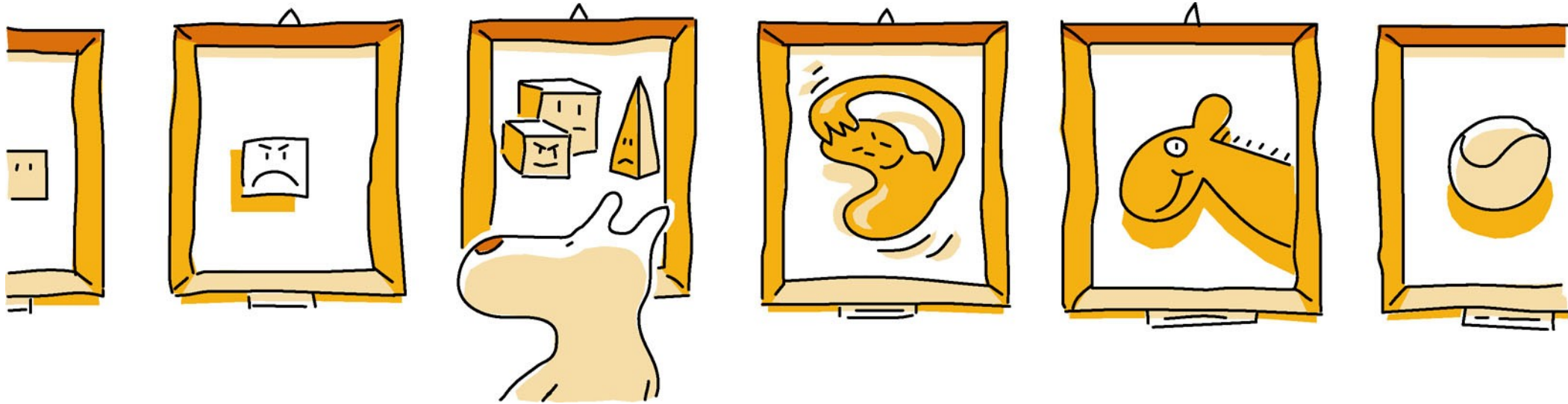


Fazit

- Projekte in anderen Ländern bereits erfolgreich
- Zusammenarbeit von Wirtschaft und Verwaltung
- Unterstützung der Benutzer in Deutschland erhöhen
- Kopplung mit Sensibilisierungsmaßnahmen



Fragen / Diskussion



Vielen Dank für ihre Aufmerksamkeit!



Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Cornelia Schildt
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5102
Fax: +49 (0)22899-10-9582-5102

cornelia.schildt@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

