antispameurope®

NUR GUTE NACHRICHTEN!

# Systemische Abwehr von Blended Threats

Eco AK Sicherheit
Köln, 5.5.2010

# Blended Attacks

# Blended Attack

- Definition:
  - Angriff auf die IT-Sicherheit, der mehrere verschiedene Methoden zur Ausbreitung und Erreichung seines Ziels benutzt.

# Verbreitungswege

- Typische Verbreitungswege von Malware
  - E-Mail
  - Web Server
  - Instant Messaging
  - Windows Shares
  - USB-Sticks
  - SW-Updates

antispameurope®

# Mechanismen

- Beispiele genutzter Mechanismen zur Erreichung der Ziele der Angreifer
  - Veränderung der Systemkonfiguration
  - Abschalten von Antivirus-Mechanismen
  - Verändern der Netzwerk-Konfiguration um die Installation und das Nachladen von Schutzprogrammen zu erschweren
  - Installation von Schadprogrammen zur späteren Ausführung
  - Nachladen von Schadprogrammen
  - Ausspähen lokaler Adressbücher
  - Infizieren von Shared-Folders
  - Öffnen eines Backdoor-Ports für Kommandos von außen
  - Automatische Verbindung mit Messaging-Service zum Austausch von Informationen

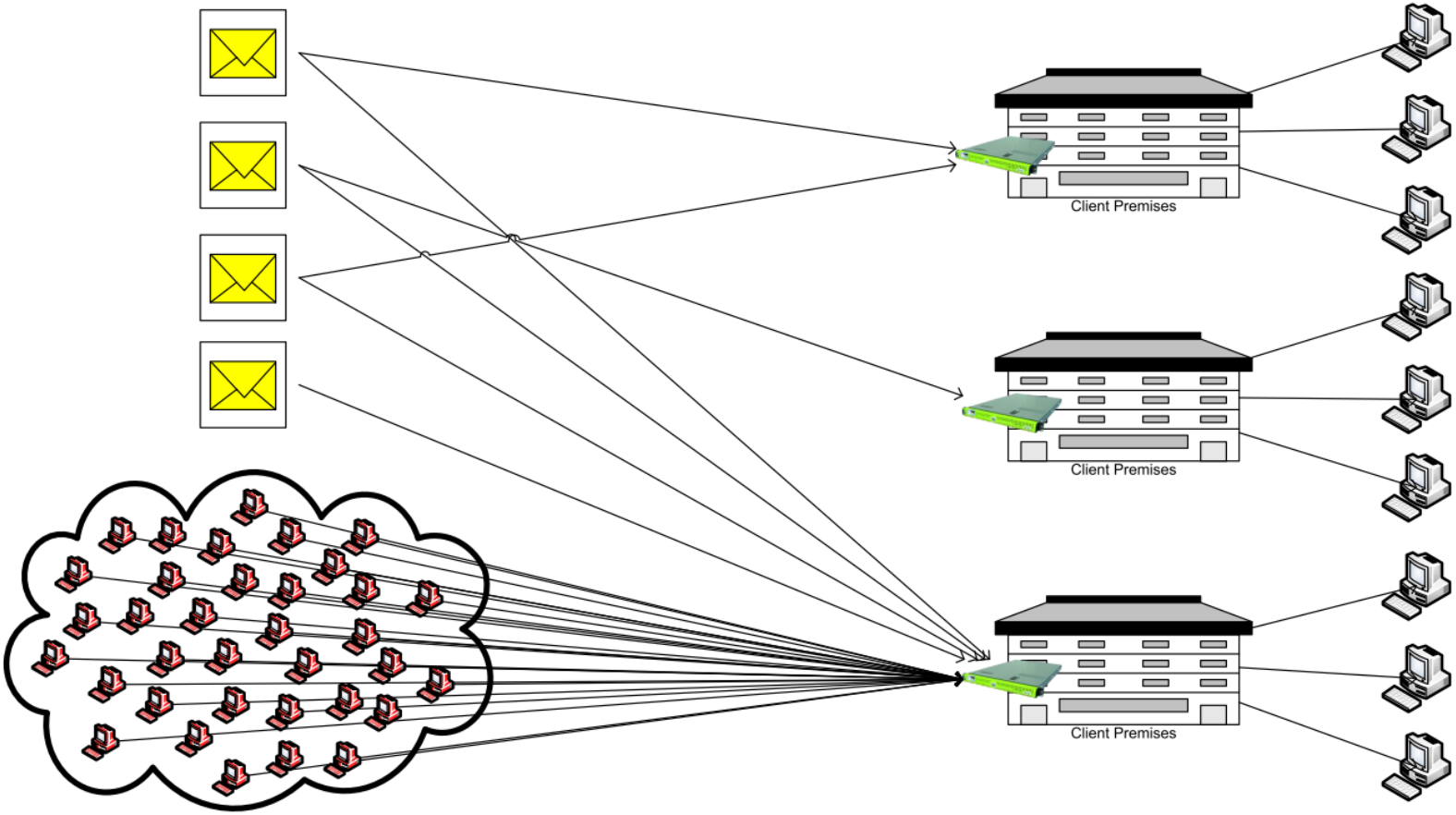
# Kombination von Mechanismen und Wegen

## Beispiel für Blended Attack

- Verbreitung von Spams mit URLs
- Aktivierung der URL durch Nutzer im Webbrowser
- Herunterladen von Schadcode, Installation eines Bots
- Umgehung der lokalen Sicherheitsinstanzen
- Bot meldet sich im Botnet an (z.B. per IRC)
- Auftrag aus dem Botnet an den Bot (IRC)
- Vorbereitung und Versand von Spams durch den Bot an Empfänger aus lokalen Adressbüchern

- Angreifer haben ihren Schwerpunkt längst in die Cloud verlegt!

# Botnet Attacke




Botnets nutzen die Cloud optimal
Singuläre Verteidigungsmaßnahmen sind vollkommen unzureichend

antispameurope®

# Problemstellung

- Es gibt zwar Schutzmechanismen für alle Verbreitungswege und Angriffs-Mechanismen
- Schutzmaßnahmen sind aber meist isoliert und können deshalb leicht umgangen werden
- Unnötige (redundante) Schutzmaßnahmen verursachen unnötige Kosten
- Klassische Installationen stehen massiven Attacken wehrlos gegenüber

antispameurope®

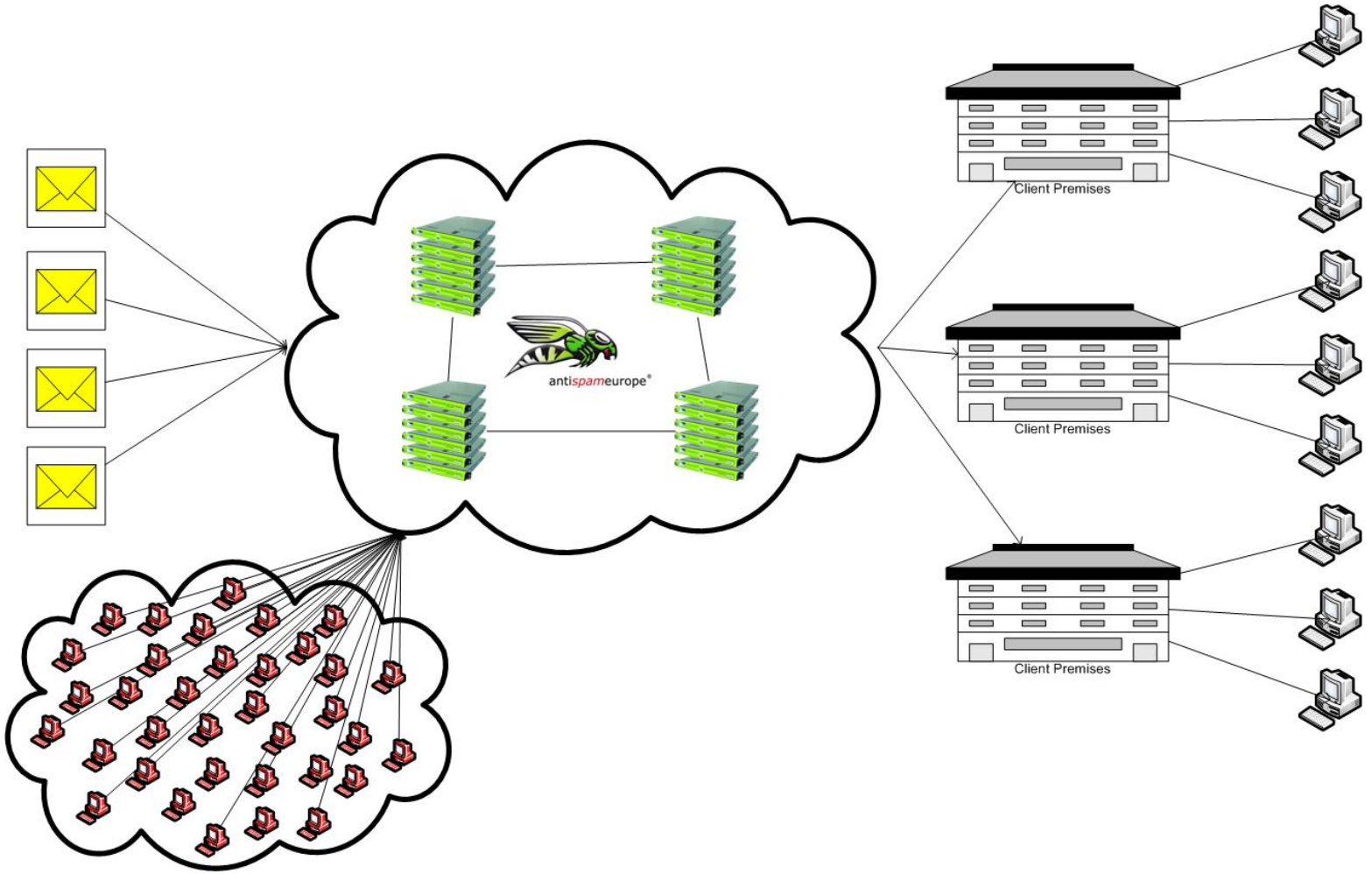
# Systemische Abwehr

# Systemische Abwehr

- Systemisch:
  - Ganzheitlich, das ganze System betreffend

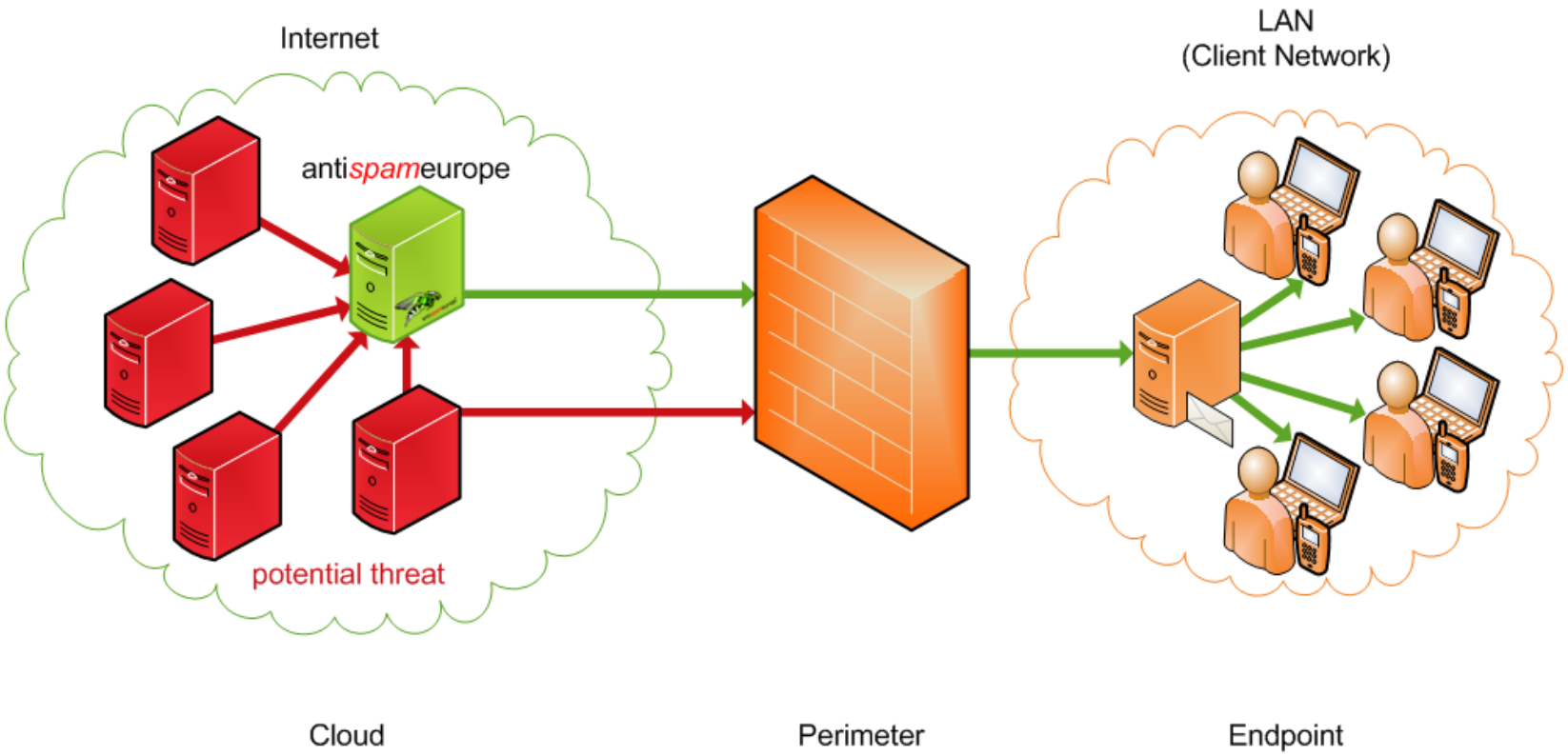
- Systemische Abwehr meint
  Abwehr von Bedrohungen
  durch gemeinsame, abgestimmte Aktion
  in einem System eigenständiger und
  voneinander unabhängiger Akteure.

# Cloud-based Security




Cloud-basierten Angriffen mit Cloud-basierten Lösungen begegnen

# Abwehrlinien

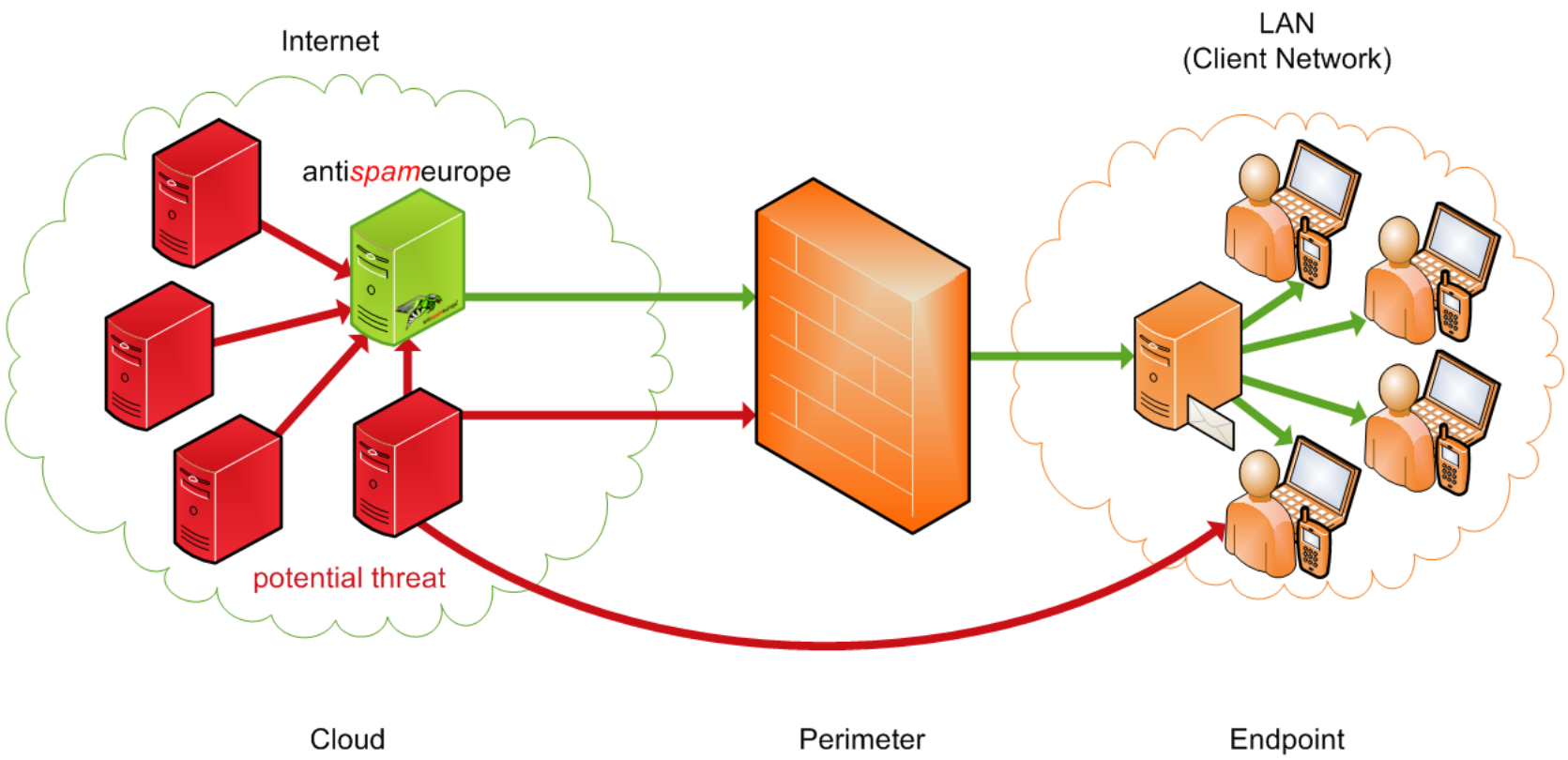



Vorgelagerter Schutz in der Cloud bietet zusätzliche Sicherheit

# Cloud-based Security: Vorteile

- Besserer Schutz vor Angriffen
  - Cloud-basierte Schutzmechanismen greifen, bevor die Bedrohung geschützte Bereiche erreicht
  - Schutzsysteme werden i.d.R. von Experten betrieben, rund um die Uhr
  - Administration von Schutzsystemen in tieferen Schutzebenen wird einfacher – weniger Fehlerquellen
- Reduzierte Kosten
  - Nutzung synergetischer Effekte durch Zusammenfassung der Anforderungen vieler Nutzer

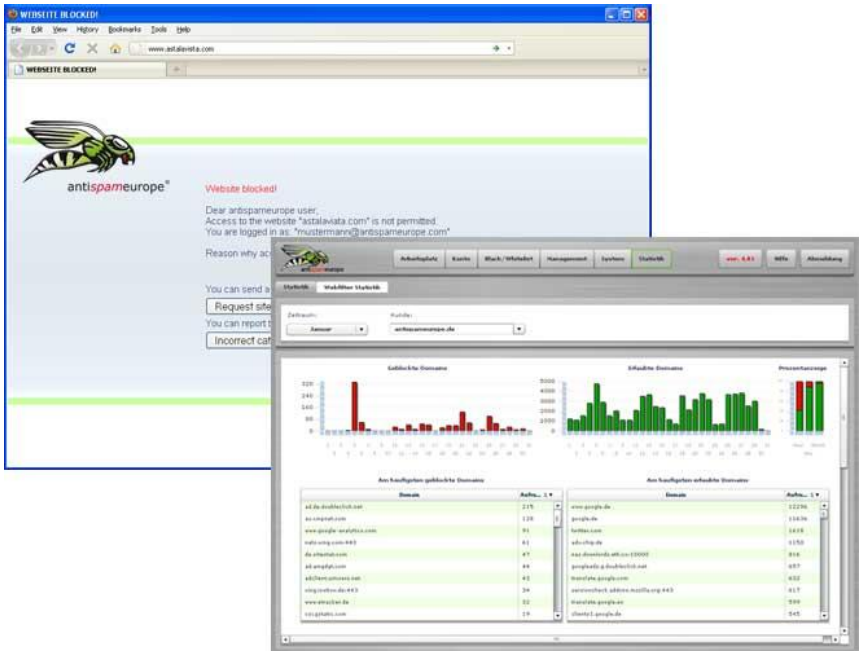
# Abwehrlinien




Vorgelagerter Schutz in der Cloud bietet zusätzliche Sicherheit ...
... löst aber nur einen Teil des Problems

# Austausch von Informationen

- Verschiedene Verbreitungswege:
  - Z.B. Sperren von URLs, die in Spam auftauchen, im Webfilter
    - Der antispameurope Web Filter Service nutzt eine Datenbank mit derzeit 8,8 Mio. Einträgen – generiert aus E-Mails
  - Z.B. Sperren von IP-Adressen mit bekannten Bots auch für Web-Traffic



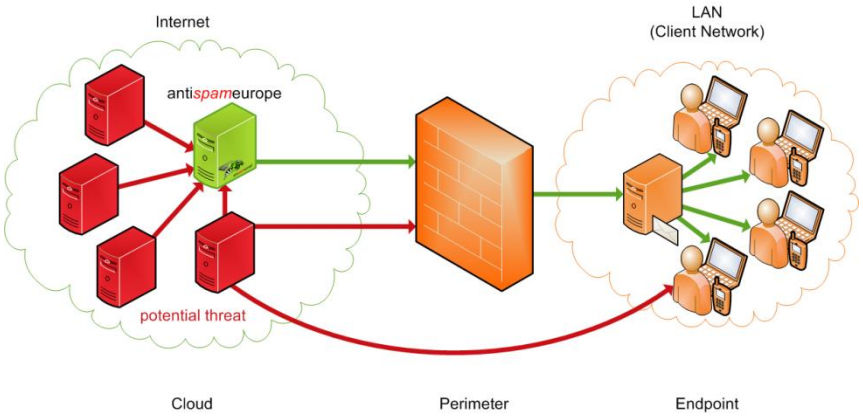
# Austausch von Informationen

- Herstellerübergreifend
- Über verschiedene Schutzebenen

- Beispiel: Zusammenarbeit von antispameurope und G DATA
  - Austausch von aus Spam gewonnenen Informationen
  - Nutzung der Ergebnisse in Produkten beider Anwender

# Ziel

- Ergo:
  - Nutzen aller Schutzebenen:
    - In der Cloud
    - Am Perimeter
    - Im Endpunkt
  - Zusammenwirken aller Schutzmechanismen
    - Austausch von Informationen in Echtzeit
    - Nutzen der Informationen aus verschiedenen Quellen
    - Gegenseitiger Schutz
  - Zusammenarbeit der Hersteller und Betreiber!



# Über antispameurope

# Über antispameurope

- Managed Security Services
  - Spam Filter
  - Web Filter
  - E-Mail Archiv
  - E-Mail Continuity
  - E-Mail Verschlüsselung
- Entwicklung der SW im eigenen Haus
- Betrieb über mehrere RZ in Deutschland
  - Wahlweise im RZ des Provider-Partners oder Endkunden
- Vertrieb über derzeit 180 Partner
  - Systemhäuser, ISPs und Hoster
  - in D, A, CH, IT, ES, FR, UK
- Über 4.000 Unternehmenskunden mit je1 bis 25.000 Mitarbeitern in 20 Ländern

# Mission und Ziele

antispameurope ist Premium-Anbieter Cloud-basierter IT Security Services

**Unsere Mission:**

- Gewährleistung perfekt sicherer Internet-Kommunikation unserer Kunden.

**Unsere Ziele:**

- Anhaltend hohe Zufriedenheit und Loyalität unserer Kunden
  - Höchste Qualitätsstandards
  - Performance, die Benchmarks setzt
  - Einfachste Nutzung
  - Umfassender Support
- Kontinuierliches Wachstum und eine führende Position in unseren Märkten
  - Ausbau des Produktportfolios
  - Ausbau des Vertriebsnetzes
  - Ausbau unserer Kundenbasis
  - Ausbau der internationalen Präsenz

antispameurope®

# Kunden

NIESMANN +BISCHOFF

AWO Bezirksverband Pfalz e.V.

Deutsche Umwelthilfe

LJN

HONOLD

GAGGIA

Saeco

HYMER

hameln pharma group

CAMTEX

NEUHAUS PARTNERS

caritas

Verlag für die Deutsche Wirtschaft AG

Sekretaerinnen.de
Sekretariat/Office & Korrespondenz online

FhG

EPCOS

LMC

Deutsches Rotes Kreuz
Kreisverband Ludwigsburg e.V.
Wir helfen weiter

KONICA MINOLTA

Fraunhofer Gesellschaft

High-Tech Gründerfonds

YENI RAKI

SieMatic

Deutsches Institut für Bautechnik DIBt

BAUHAUS

bfw hamm

THIELERT

Konrad Adenauer Stiftung

WITZENMANN
managing flexibility

WEENER
PLASTIC PACKAGING GROUP
IDEE DESIGN PRODUKT

# Kontakt

Oliver Dehning

antispameurope GmbH

Am Listholze 78

30177 Hannover

Tel.: +49 – 511 – 260 905 – 0

www.antispameurope.com

dehning@antispameurope.com