

# Wir über uns



## AGe-EDV - Wer ist das ?

Der Firmenname bildet sich aus den Initialen meines Namens - Andreas Geck



Ich bin seit über 10 Jahren Netzwerk- und Systemtechniker und verantwortlich für Netze mit bis zu 2000 PCs und rund 40 Servern.

Dabei kommen alle heute gängigen Techniken zum Einsatz, vom NT4.0-Server bis hin zum Windows 2003 Active Directory, Microsoft Exchange, Firewalls, VPN, Virens Scanner samt zentralem Management, IPS-Lösungen usw.

Vor allem heterogene Landschaften mit Windows und UNIX/LINUX sind sicherheitstechnisch immer wieder eine Herausforderung - aber eine lösbare!

Das Logo mit der Möbius-Schleife ist übrigens das perfekte Symbol für den IT- und vor allem den Security-Bereich. Kaum ist man "am Ziel", muss man die gerade geschaffenen Strukturen auch schon wieder überdenken, weil es etwas Neues gibt.

IT allgemein und IT-Security im Speziellen sind einfach niemals "zu Ende"...

Da auch mein Wissen Grenzen hat, arbeite ich in speziellen Bereichen mit entsprechenden Experten zusammen. Für den Kunden gibt es aber immer nur einen Ansprechpartner und Lösungen aus einer Hand.

Neben dem Bereich IT-Security engagiert sich AGe-EDV auch noch in vielen anderen Bereichen, so u.a. auch bei der Virtualisierung von Hardware.

Wenn Sie also alte Hardware ablösen wollen, aber das Betriebssystem so gar nicht auf einer modernen Maschine laufen will oder wenn Sie eine preisgünstige Testumgebung aufbauen möchten, sind Sie bei uns genau richtig. Unsere Erfahrungen mit Virtualisierungstechniken von Beginn an sprechen für sich.

Wenn Sie mehr erfahren wollen, schauen Sie sich doch einfach die Webseite [www.age-edv.de](http://www.age-edv.de) an.

# Kontakt aufnehmen



## Telefon/Fax

Telefon: (0700) 00 AGE EDV  
(0700) 00 2 4 3 3 3 8

Fax : (0201) 877 62 71

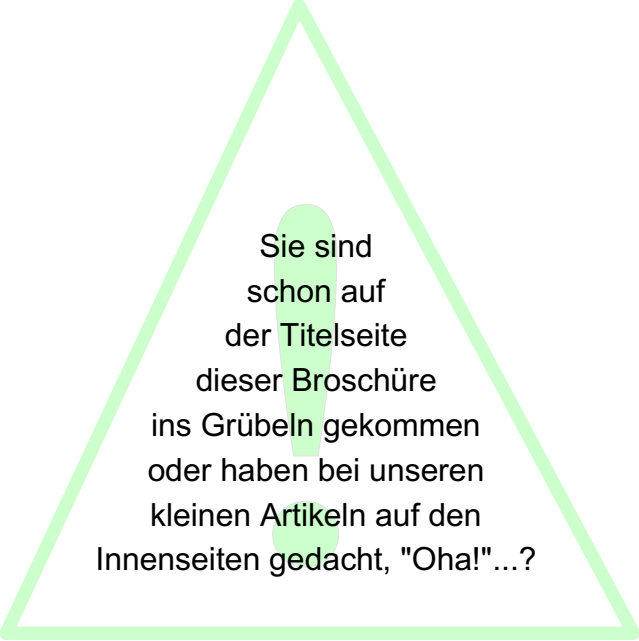
## Post

AGe-EDV Andreas Geck  
Niederdingstraße 10  
45147 Essen

## Internet

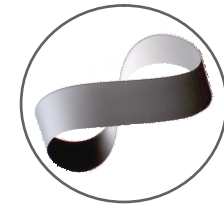
Homepage: [www.age-edv.de](http://www.age-edv.de)

E-Mail : [security@age-edv.de](mailto:security@age-edv.de)



Sie sind schon auf der Titelseite dieser Broschüre ins Grübeln gekommen oder haben bei unseren kleinen Artikeln auf den Innenseiten gedacht, "Oha!"...?

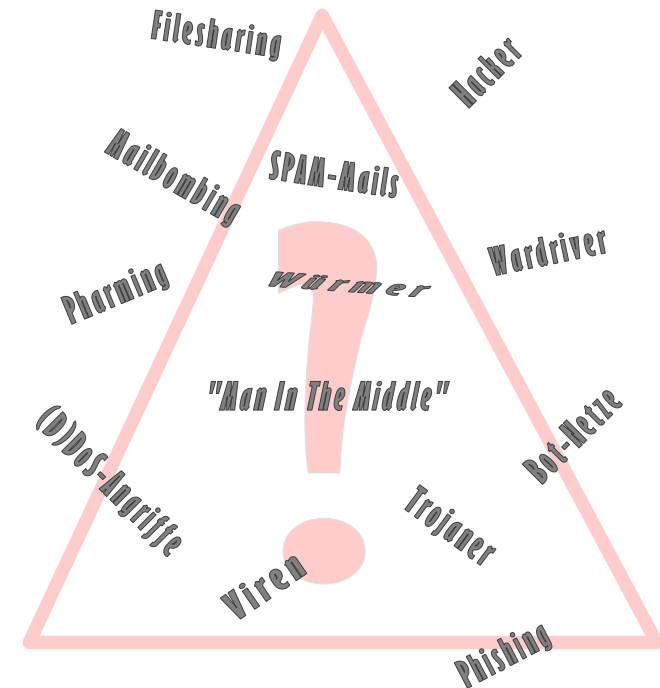
**Sprechen Sie uns an - wir teilen unser Wissen mit Ihnen !**



# AGe-EDV Andreas Geck

Ihre Netzwerk- und Sicherheits-Spezialisten

**Sind Sie sicher, dass Ihr Netzwerk sicher ist ???**



**Bedrohungen und Störungen Ihres Netzwerkes wirkungsvoll begegnen**

# Bedrohungen



## Bedrohungen von außen

Dies sind die wohl bekanntesten Bedrohungen, die auch immer wieder durch die Presse gehen.

- Viren, Würmer, Trojaner, Dialer, CallBack-Anrufe
- Phishing, Pharming
- Bot-Netze und (D)DoS-Attacken
- Hacker

Fast jedes Unternehmen ist mittlerweile in der Situation, dass bestimmte Daten von extern zugreifbar gemacht werden sollen oder sogar müssen. Seiten für Partner, Kunden und Lieferanten, aber auch die Anbindung der eigenen Außendienst-Mitarbeiter sind hier nur einige Beispiele, wo potentielle Gefahren lauern.

Wenn solche Schritte gegangen werden, ist ein gutes und umfassendes Sicherheitskonzept unumgänglich!

## Bedrohungen von innen

In vielen Fällen werden die Bedrohungen, die im Inneren des eigenen Netzes entstehen, nicht gesehen oder als vernachlässigbar angesehen.

- "Tote" Useraccounts / fehlende Kennwörter
- nicht gesperrte Konsolen
- frei zugängliche Netzwerkdosens
- ungesichertes DHCP
- Verwendung von WLAN
- Verhalten der Benutzer

Durch diese und noch viele andere Dinge entstehen Sicherheitslücken, die Externe nutzen können, um auf Ihre Unternehmensdaten zugreifen zu können.

**Denken Sie einmal nach, wo in Ihrem Unternehmen solche Bedrohungen lauern könnten... Sie werden bestimmt einige Punkte finden - und wir als Security-Experten zeigen Ihnen bestimmt noch viele Weitere!**

# Risiken



## Daten-Verlust

Der wohl schlimmste Schaden für ein Unternehmen ist der Verlust von Daten, z.B.

- Stammdaten (Kunden, Lieferanten)
- Kaufmännisch (Rechnungen, Mahnungen)
- E-Mails
- Geschäftskorrespondenz

Zum Einen können ggf. gesetzliche Vorgaben nicht mehr erfüllt werden, andererseits können Kunden und Lieferanten nicht mehr zufriedengestellt werden.

## Image-Verlust

Können Sie sich vorstellen was passiert, wenn Ihre Kalkulationsdaten in die Hände von Kunden oder Konkurrenten fallen? Leider passiert so etwas immer häufiger, weil Benutzer zu unvorsichtig oder unbedarft mit Ihrer Büro-Software umgehen!

Außerdem - kann es etwas Peinlicheres geben, als dass interne Dokumente nach außen gelangen (z.B. der Meinungs-austausch über bestimmte Kunden/Zulieferer)?

## Zeit- und Geld-Verlust

Selbst wenn Sie bei einem Datenverlust noch ein Backup in der Schublade (oder vielleicht besser im Tresor) haben, bedeutet ein Recovery auf jeden Fall immer den Ausfall von Arbeitszeit und evtl. sogar das Versäumen von Fristen (Lieferungen, Zahlungen). Der schlimmste Fall dabei ist der Ausfall von Rechnern in der Produktions-Steuerung. Stillstand ist hier purer Verlust!

**Erkennen Sie Risiken wieder? Malen Sie sich einige dieser Szenen gerade für Ihr Unternehmen aus? Wir helfen Ihnen, Risiken individuell zu bewerten und geeignete Maßnahmenpläne zu erarbeiten.**

# Lösungen



## Sicherheits-Analysen

Wir analysieren Ihr Netzwerk, Ihre Server und PCs auf Schwachstellen und erarbeiten mit Ihnen Lösungen auf Basis dieser Analysen. Im Folgenden finden Sie einige der häufigsten Ansatzpunkte.

## Malware-Bekämpfung

Wir planen mit Ihnen und/oder für Sie eine passende Anti-Malware-Strategie. Diese umfasst z.B.

- Viren- und Spywareschutz auf Servern
- Viren- und Spywareschutz auf PCs/Notebooks
- Zentrales Management der Virens Scanner

## IDS-/IPS-Systeme

Unter dem Begriff "Intrusion Detection System" und "Intrusion Prevention System" werden Lösungen zusammengefasst, die Hardware- und Software-basierend dafür sorgen, dass Anomalien und unerwünschte Dinge in Ihrem Datennetz gemeldet oder automatisch geblockt werden. So können sogar neue Würmer oder Exploits für Sicherheitslücken vom System erkannt werden, ohne dass dafür Updates eingespielt werden müssten.

## Patch-Management

Der "Microsoft-Patchday" ist sicherlich einer der bekanntesten Tage in der IT-Welt. Damit Sie sicher sein können, dass auch Ihre Systeme immer mit den aktuellen Sicherheits-Updates ausgestattet sind, erarbeiten wir mit Ihnen Lösungen für das Patch-Management in Ihrer IT-Umgebung.

## Benutzer-Sensibilisierung

Der "Otto Normal-User" ist natürlich kein IT-Fachmann. Daher müssen Benutzer über Gefahrenpotentiale aufgeklärt werden. Verhaltens-Regeln im Umgang mit PC, Internet und Co. helfen in vielen Fällen, Risiken zu vermeiden ("Behavioural Guidance").

- Erstellung von Dienstanweisungen
- Schulung der Benutzer in IT-Sicherheit
- Aktive Ansprache der Benutzer bei Fehlverhalten

## Absicherung Ihrer Systeme

Systemabsicherung geht weit über die Funktionen hinaus, die "offensichtlich" sind - lassen Sie sich überraschen...