

# Monitoring von Windows Systemen

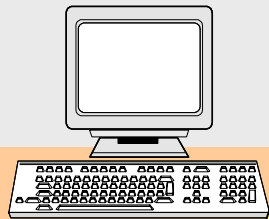
Michael Wirtgen

NETWAYS Nagios Konferenz 2006

Nürnberg, 21.09.2006

# Häufige Fragen

- Kann ich Windows überwachen?
- Wie kann ich Windows überwachen?
- Was ist der beste Weg, das beste Werkzeug...?

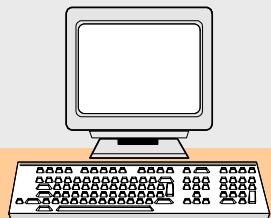


Nagios

*Hier geschieht ein Wunder...*



Windows



Nagios



Windows

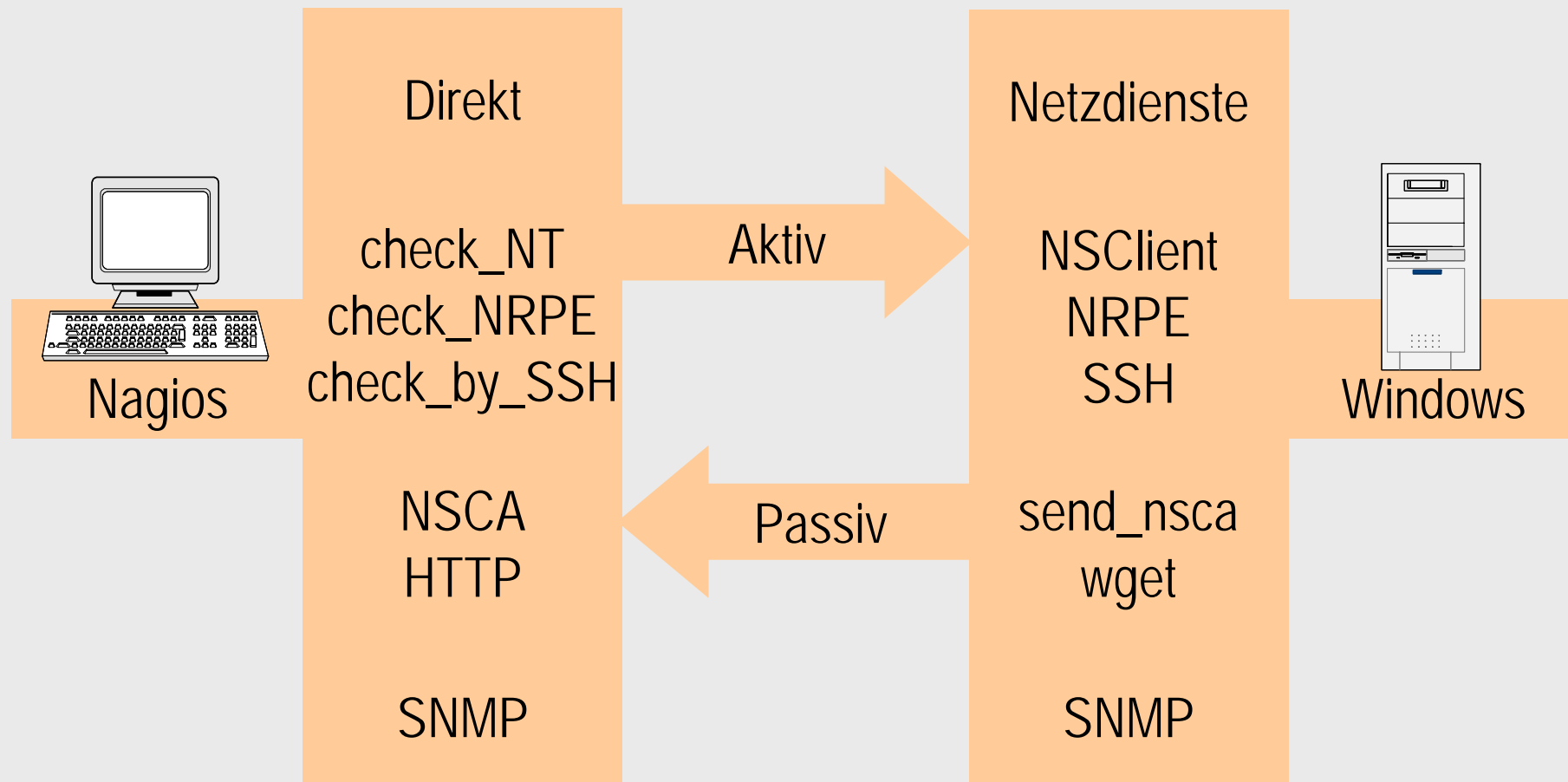
# Komponenten

- Abfragesysteme
- Plugins
- Windows Besonderheiten

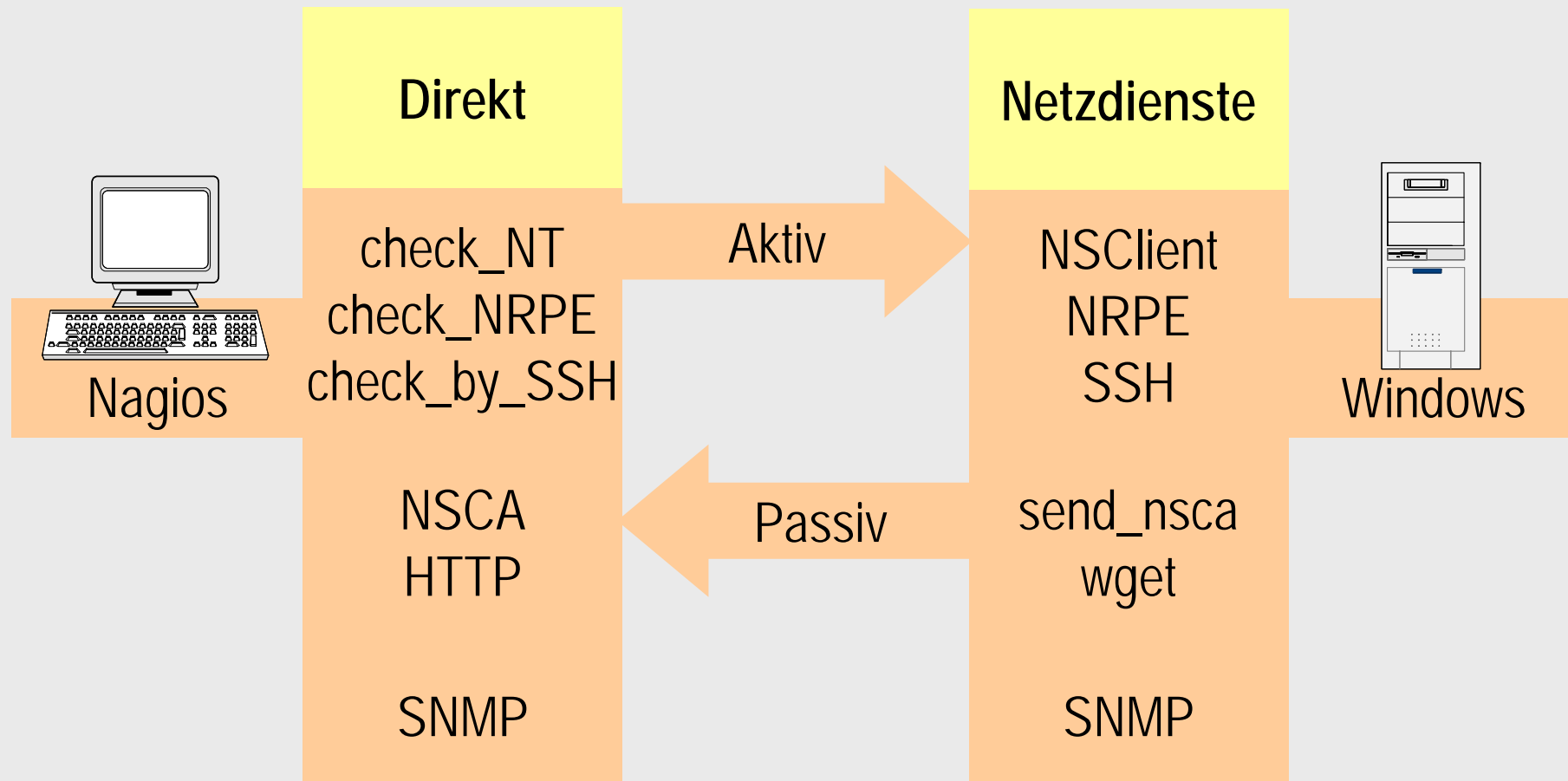
# Abfragesysteme

- Direkt
- Aktiv
- Passiv
- SNMP

# Abfragesysteme



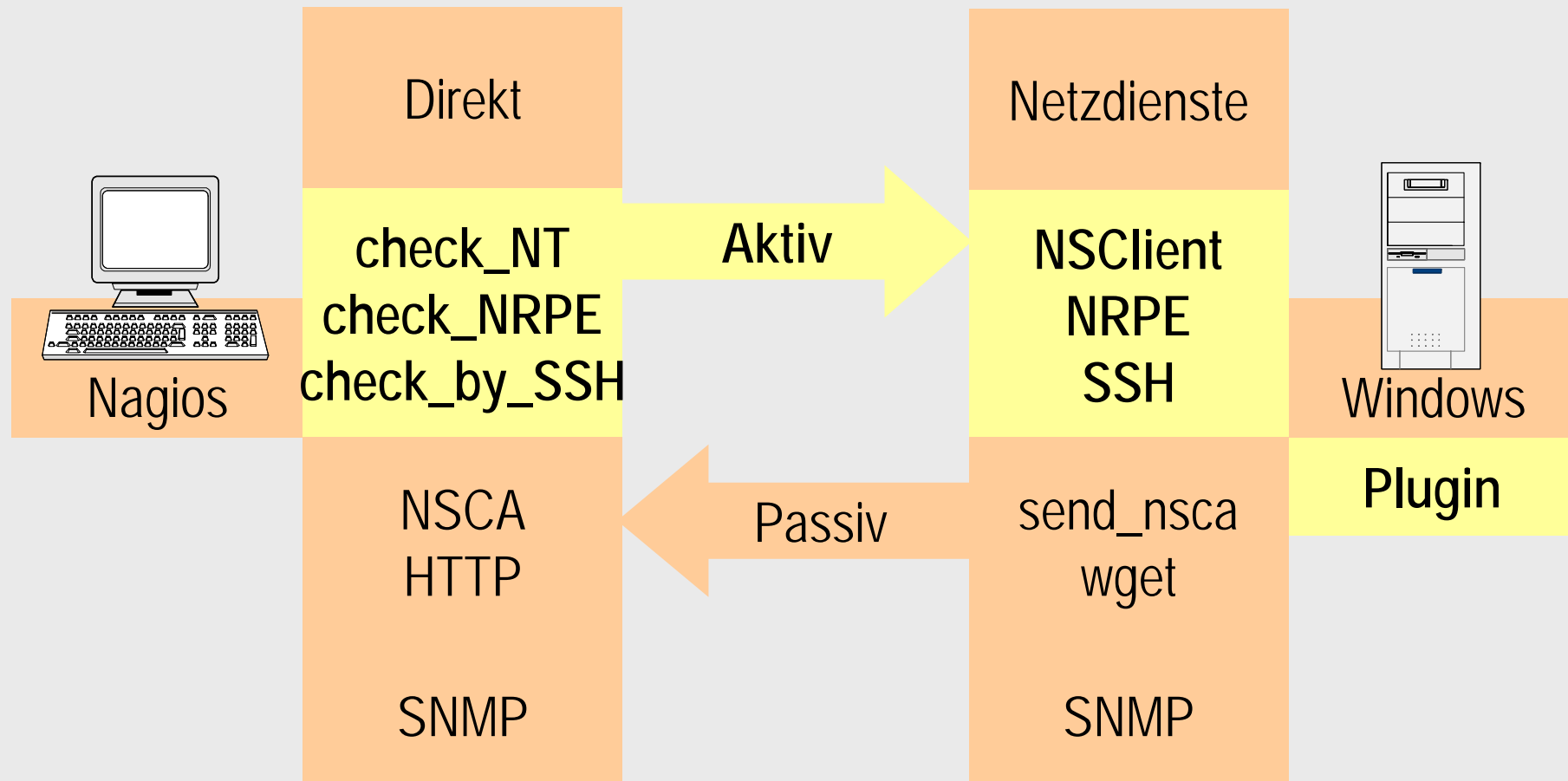
# Abfragesysteme - Direkt



# Abfragesysteme - Direkt

- Nagios
  - check\_tcp
  - check\_http
  - andere
- Windows
  - Netzwerkdienste
- Einfache Konfiguration
- Keine Systeminformation

# Abfragesysteme - Aktiv



# Nsclient

- Nagios
  - check\_nt
- Windows
  - pnsclient
  - nc\_net
  - nsclient++
- Interne checks
- Keine Plugins
- Einfache Konfiguration
- Geringe Erweiterbarkeit

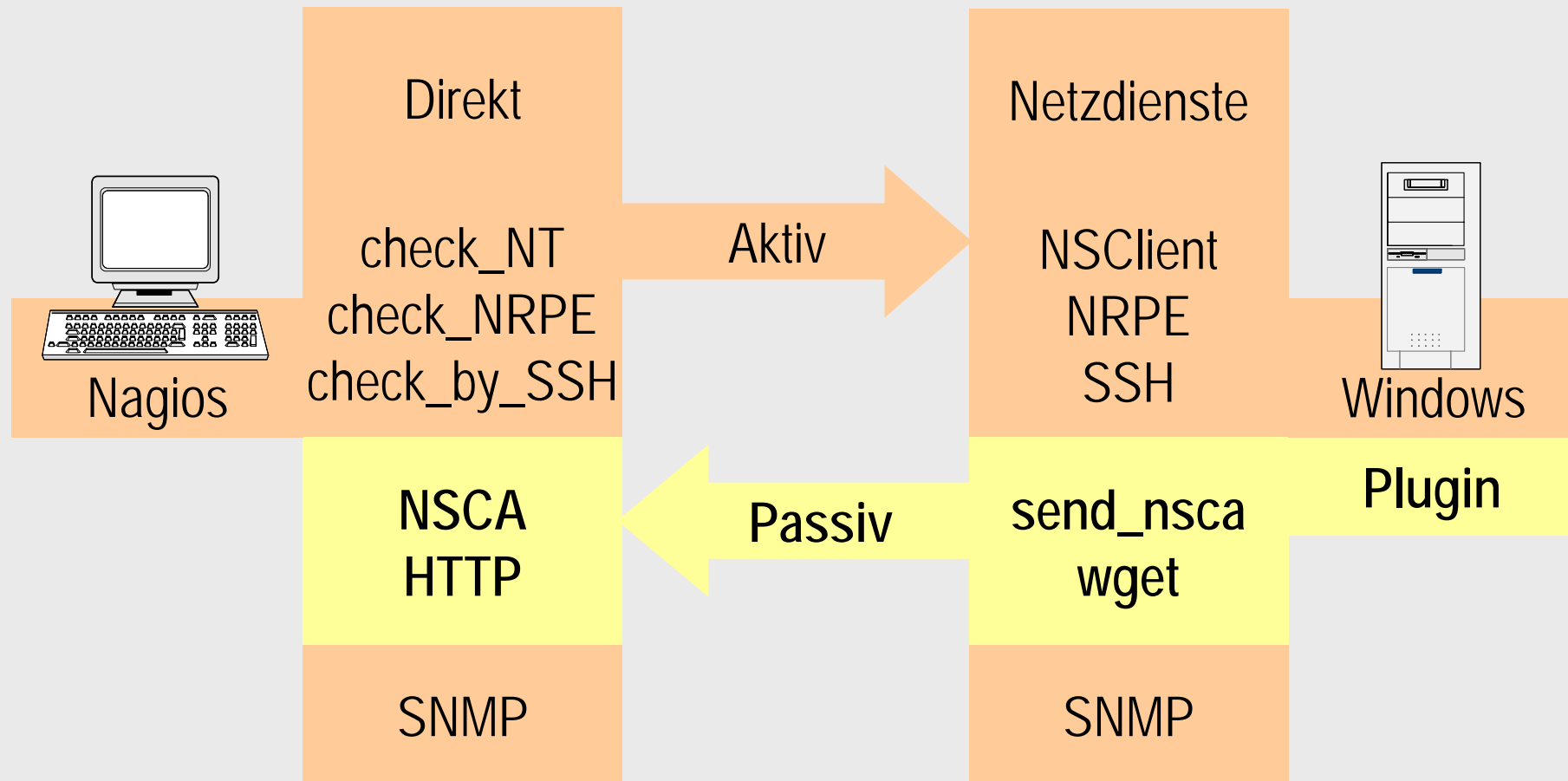
# NRPE

- Nagios
  - check\_nrpe
- Windows
  - nrpe\_nt
  - nsclient++
- Keine internen checks
- Plugin Konfiguration
- Volle Erweiterbarkeit

# SSH

- Nagios
    - check\_by\_ssh
  - Keine internen checks
  - Plugin Konfiguration
  - Teils eigene Userverwaltung
  - Volle Erweiterbarkeit
- Windows
    - Freesshd
    - WinSSHD
    - Andere

# Abfragesysteme - Passiv



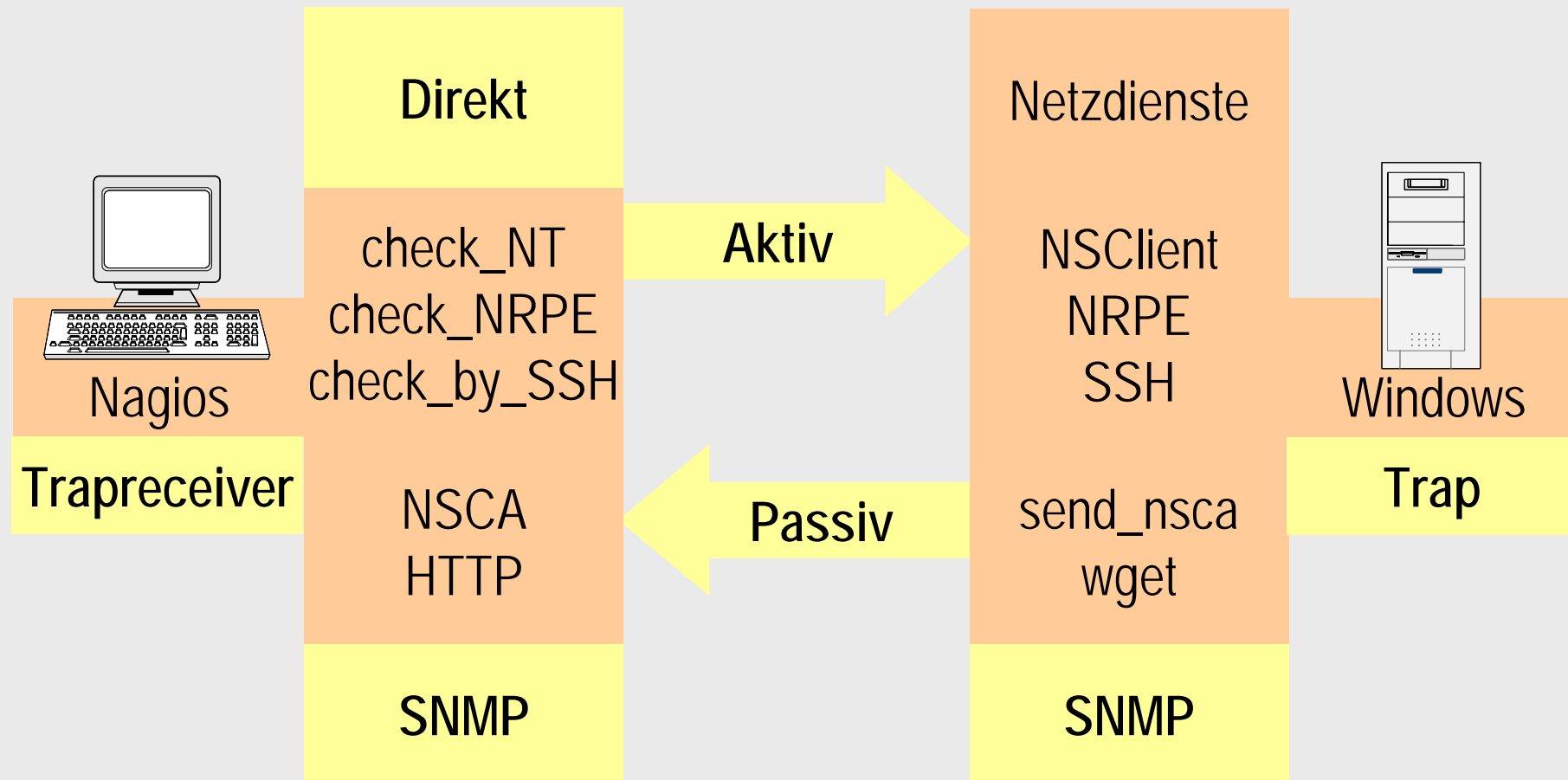
# NSCA

- Nagios
  - NSCA
- Windows
  - Send\_nsca\_win32
- Quellen
  - Eventlog (Evtrig)
  - Dienste (Wiederherstellen)
  - Perfmon
  - Hardwaremonitore

# HTTP

- Nagios
  - HTTP (cmd.cgi)
- Windows
  - wget

# Abfragesysteme - SNMP



# SNMP

- Direkte Checks via `check_snmp`
- Ereignisse als Traps versenden

# Plugins

- Zahlreiche Windows Plugins
- Kein „offizielles“ Repository
- Nagiosexchange

# Plugins

- CMD / Batch
- PERL
- Exe
- VBscript
- Beliebige andere...

# Windows Besonderheiten

- Administration immer noch GUI-lastig
  - Es geht (fast) immer auch anders!
- Eventlog
  - Evtsys
  - Snare
  - evtrig

# Windows Besonderheiten

- Dienste
- Performance Counters
  
- Exchange
- IIS
- SQL

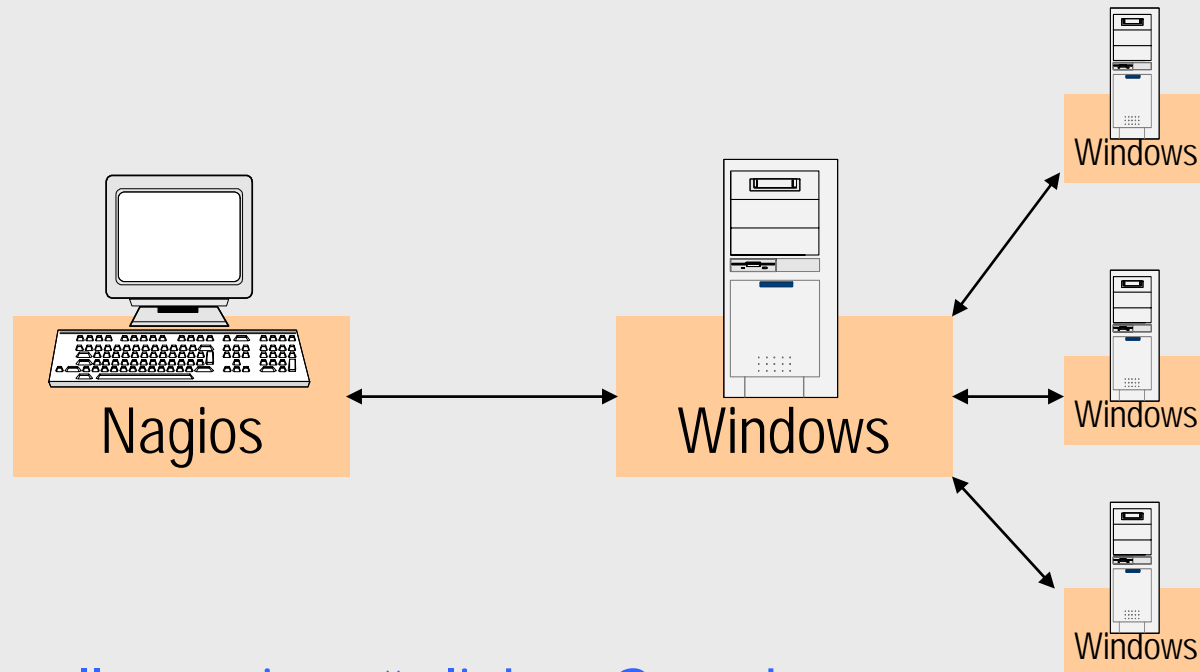
# Ideen für die Praxis

- Eventhandler
- Indirekte Checks
- Tools

# Eventhandler

- Eventhandler sind auch nur Plugins
- Häufig schon vorhanden
- Einfach, aber nützlich:
  - *C:> net start spooler*
- Eskalationsplan erstellen

# Indirekte Checks



- Firewall nur ein möglicher Grund
- Zentrale Administration der Plugins
- Domain basierte Aufgaben
- Abhängigkeiten definieren!

# Tools

- MS Utilities
- evtrig
- netsh
- iisreset
- wget
- pstools
- Cygwin
- SpeedFan

# Rückblick

- Kann ich Windows überwachen?
- Wie kann ich Windows überwachen?
- Was ist der beste Weg, das beste Werkzeug...?

**Ihre Fragen?**

**Vielen Dank für Ihre  
Aufmerksamkeit!**

# Monitoring von Windows Systemen

Michael Wirtgen

NETWAYS Nagios Konferenz 2006

Nürnberg, 21.09.2006