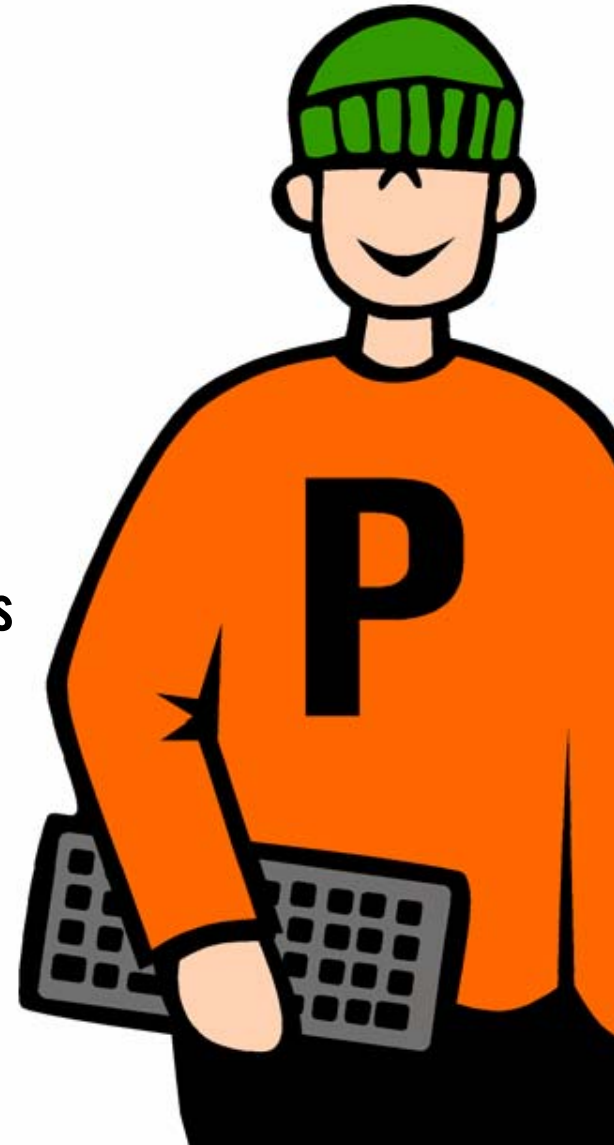




DIRK PAESSLER

## Securing Your Online Business Success With Network Monitoring

European Shareware Conference 2004, Strassbourg



# Overview

## Securing Your Online Business Success With Network Monitoring

- The needs of the sample Shareware Company „Big P Solutions“
- Network diagram of „Big P Solutions“
- Sample Events and their handling - based on real life samples
- Analyzing historical monitoring data - based on real life samples
- Monitoring is not enough! Be prepared!
- Top 5 reasons to monitor your network
- Getting started with freeware products from Paessler



# Sample Shareware Company „Big P Solutions“

## Big P Solutions

- creates and sells shareware software
- Since >90% of marketing and sales is conducted online, the business success depends totally on the reliability of the server systems involved

## Systems involved in business transactions

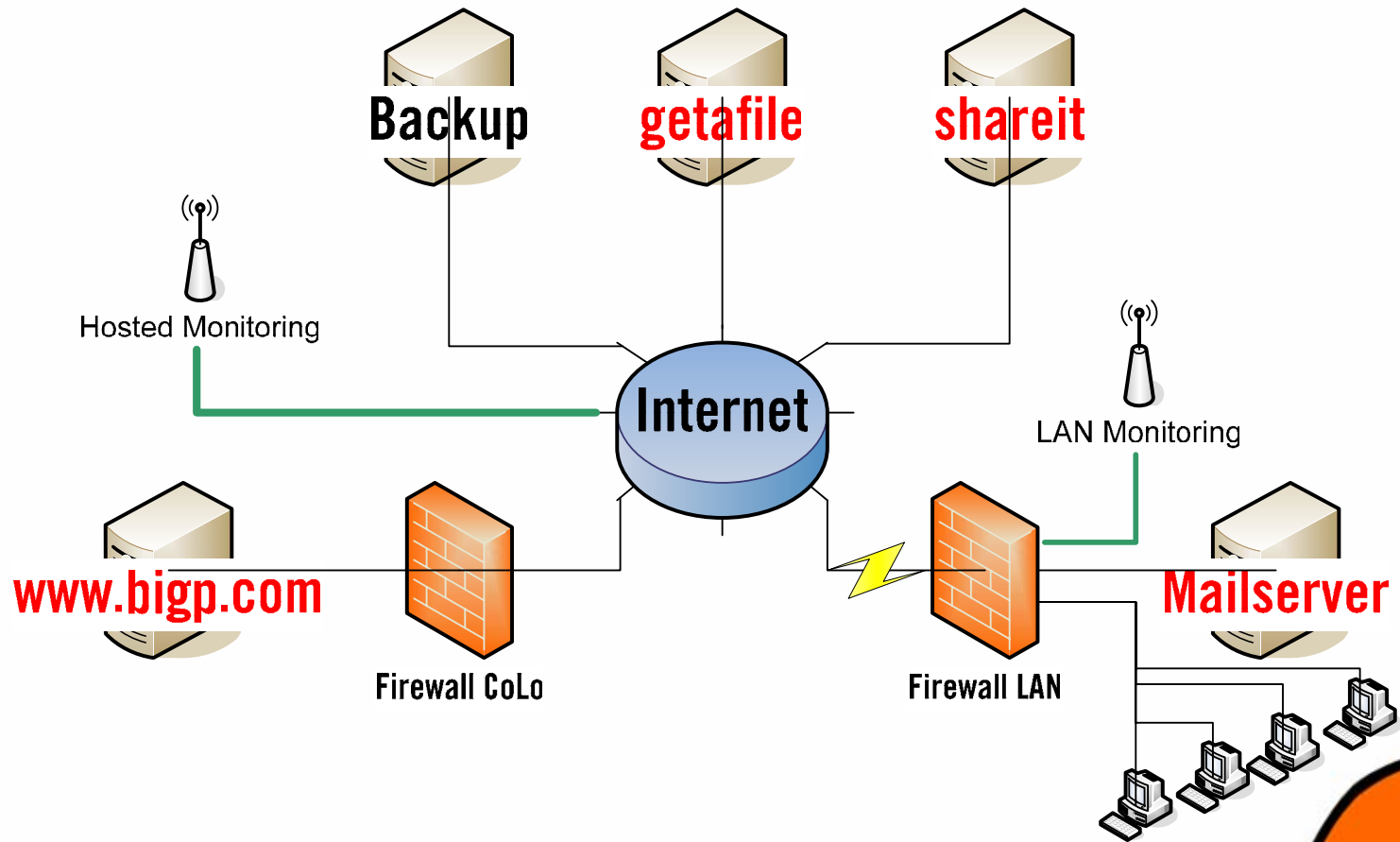
- **Web server:** [www.bigp.com](http://www.bigp.com)
- **Online shop:** hosted by [www.shareit.com](http://www.shareit.com) (Element 5)
- **Download URLs:** hosted at [www.getafile.com](http://www.getafile.com)
- **Leased line:** connects office LAN with the Internet (with firewall)
- **Mail server:** located in the office LAN

## Redundancy/Backup Systems

- **Backup web server:** [www2.bigp.com](http://www2.bigp.com)
- **Backup mail server:** [mail2.bigp.com](http://mail2.bigp.com)



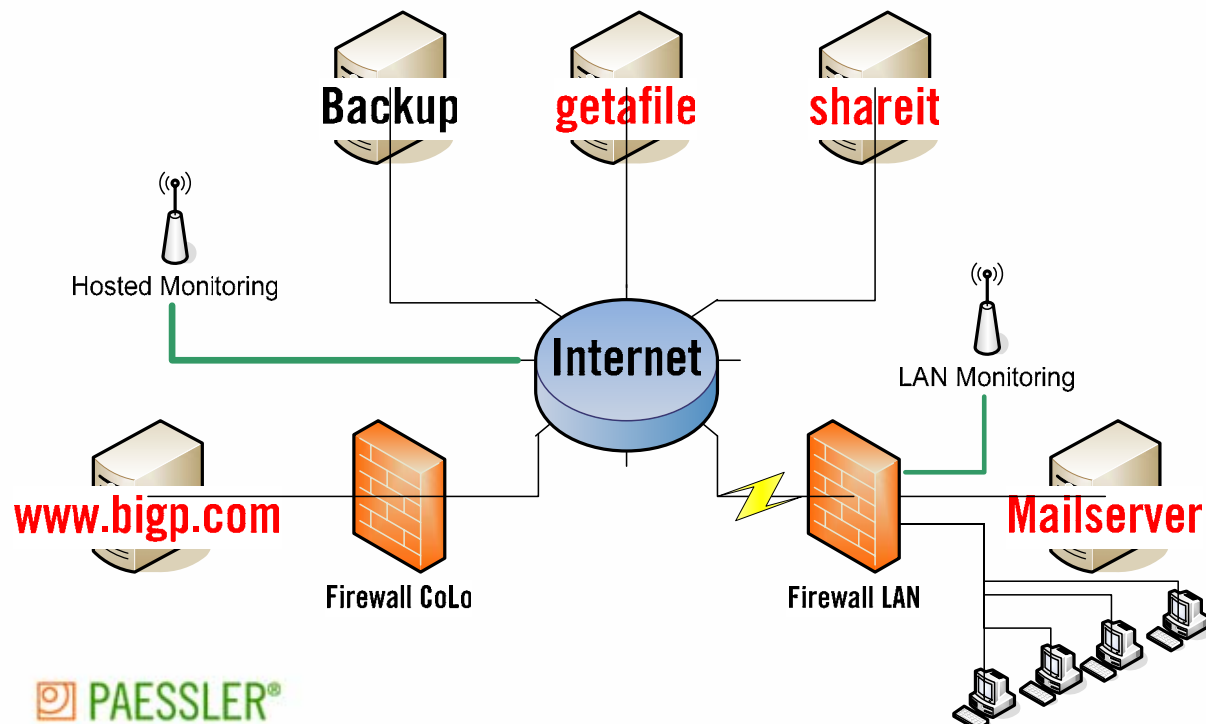
# Big P Solutions - Network Diagramm



# Big P Solutions – Network Monitoring Setup

## Sensors to monitor

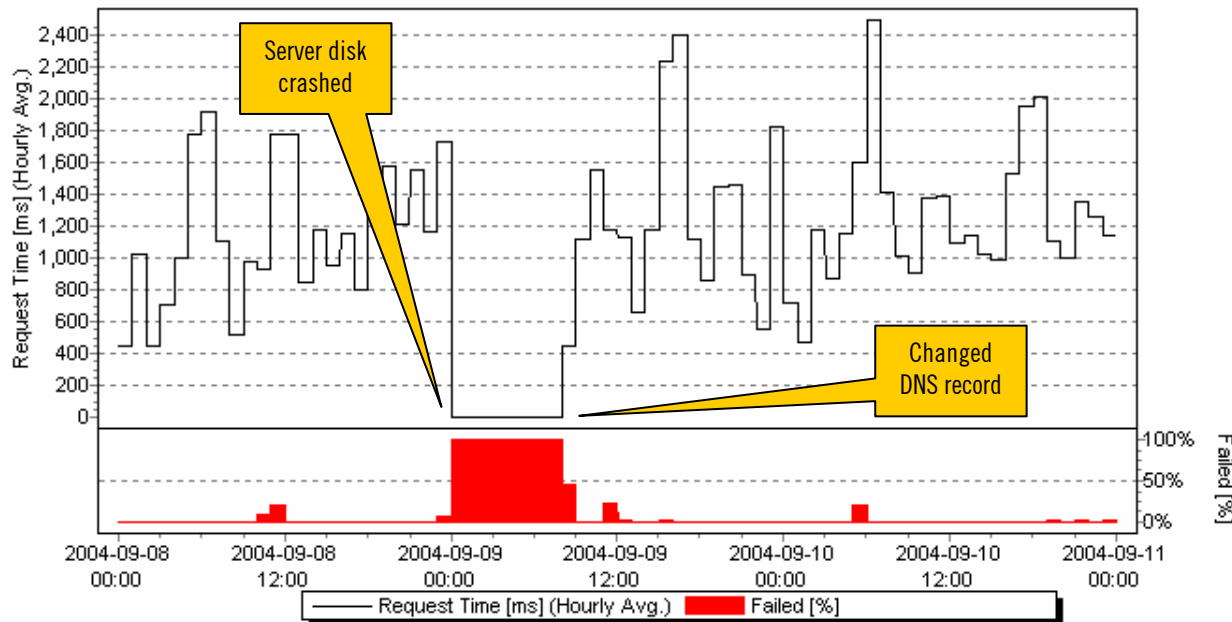
- **PING:** All servers, routers, etc. (also several „hops“ on the main TCP/IP routes)
- **HTTP&HTTPS:** web server, ShareIt\*, getafile\*, backup website, provider's website\*
- **SMTP&POP3:** primary, secondary mail server
- **Traffic&Bandwidth:** web server, leased line
- **Custom:** e.g. trial key generator CGI, server disk space, mail queues, etc.
- Use common sense when configuring sensors on other company's servers. Keep CPU and bandwidth usage to a minimum!



# Sample Events and Their Handling

## Notification 1: www.bigp.com is down (HTTP connect failed)

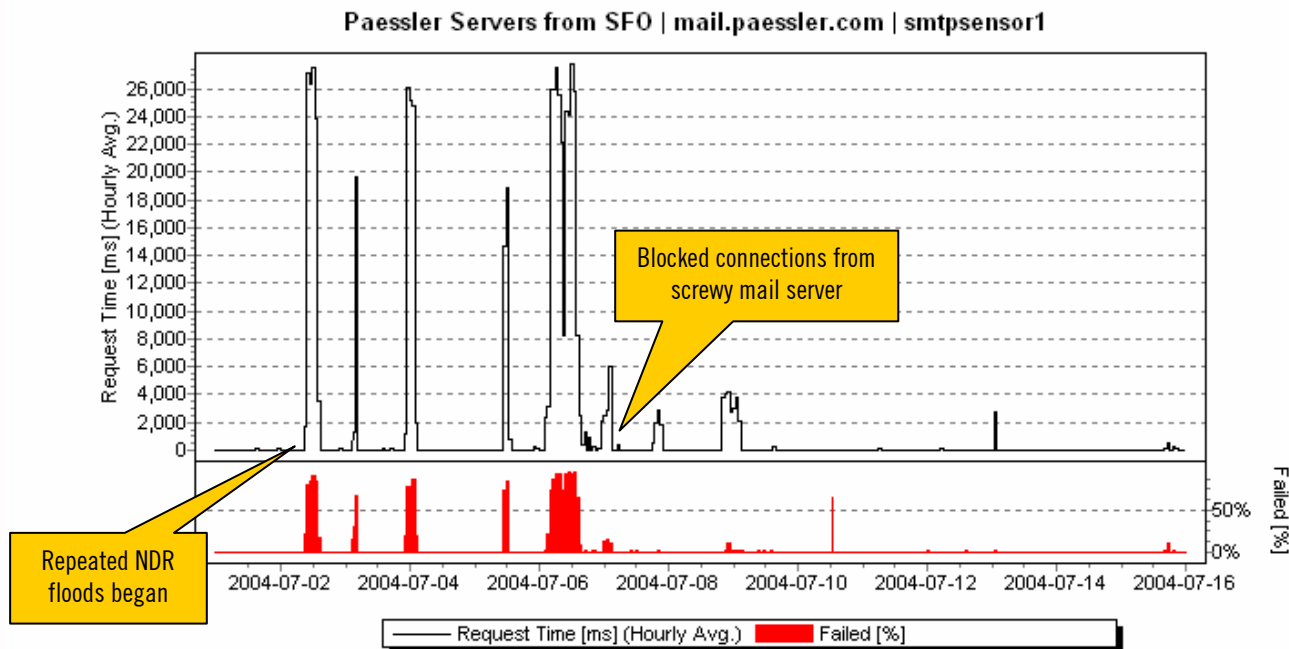
- You receive a notification via email, SMS, soundfile, popups, etc.
- Since you also monitor routers/hops en-route and your provider's site, you know right away whether there is just a general network problem or a problem with your server
- You discover a severe hard disk crash of the main web server
- => You re-route traffic to your backup systems (via DNS)



# Sample Events and Their Handling

## Notification: mail.bigp.com is down (SMTP timeout)

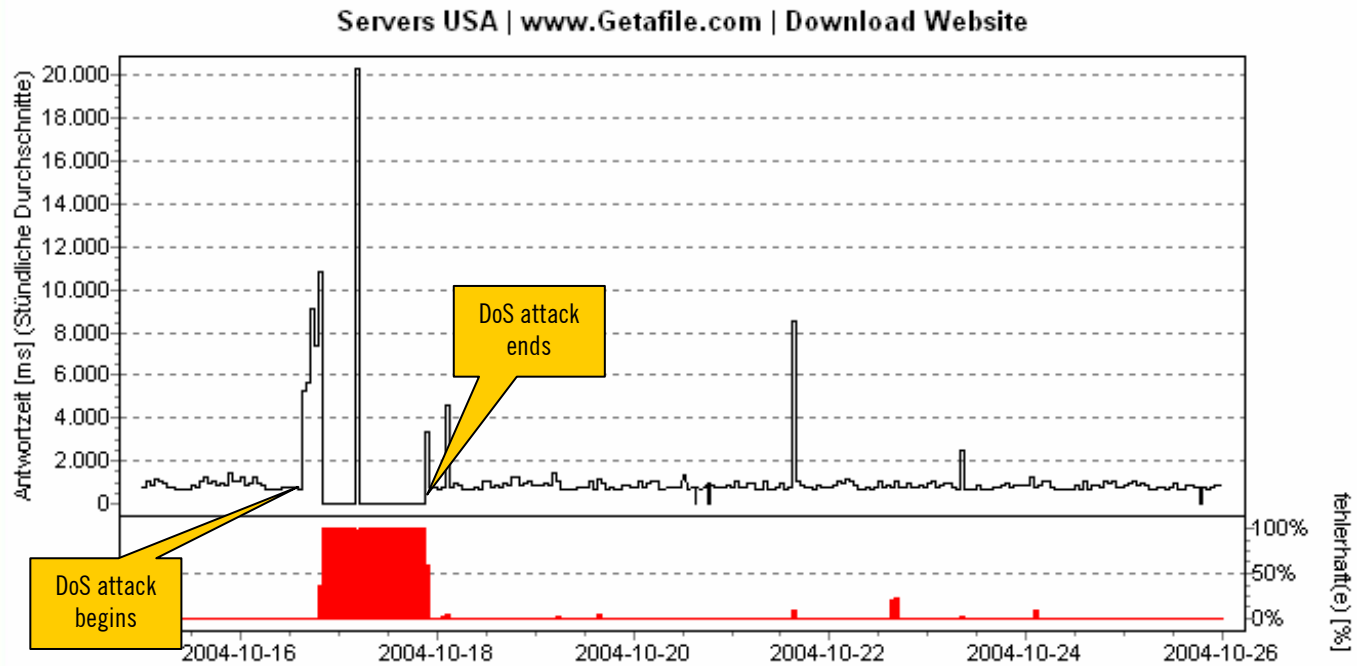
- You receive a notification via email, SMS, soundfile, popups, etc.
- All other network sensors report a green light
- You check the mail server and discover that you receive an insane number of bogus non-delivery reports due to worm activity
- => You deny SMTP connections from the screwy mail server



# Sample Events and Their Handling

## Notification: [www.getafile.com](http://www.getafile.com) is down (PING failed)

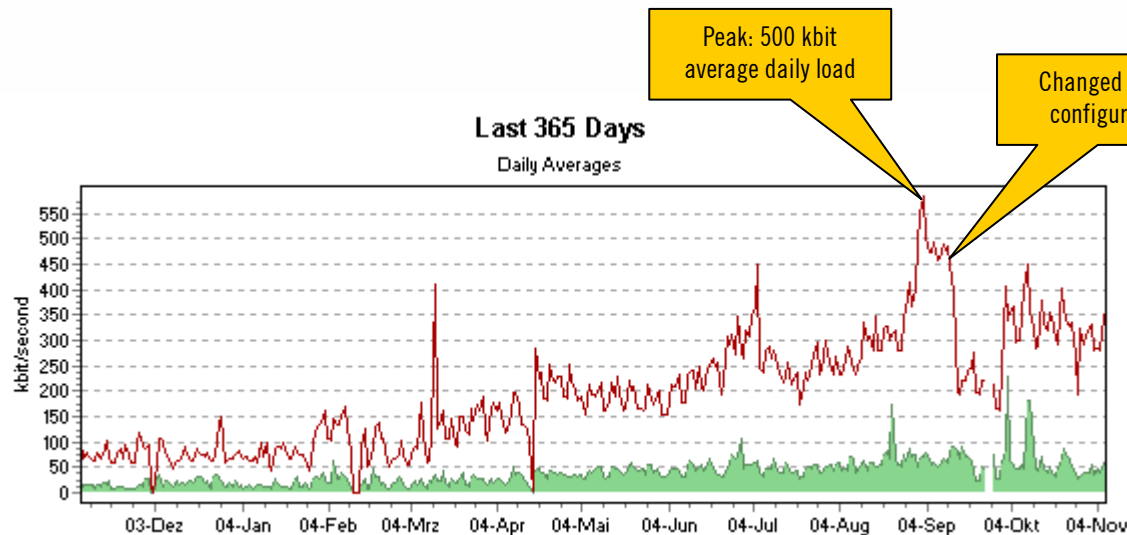
- You discover that [www.getafile.com](http://www.getafile.com) does not answer
- => You re-route all downloads to your backup download server
- What actually happened: DoS attack against [www.getafile.com](http://www.getafile.com)



# Analyzing Historical Monitoring Data

## Sample 1: Leased Line Bandwidth Usage

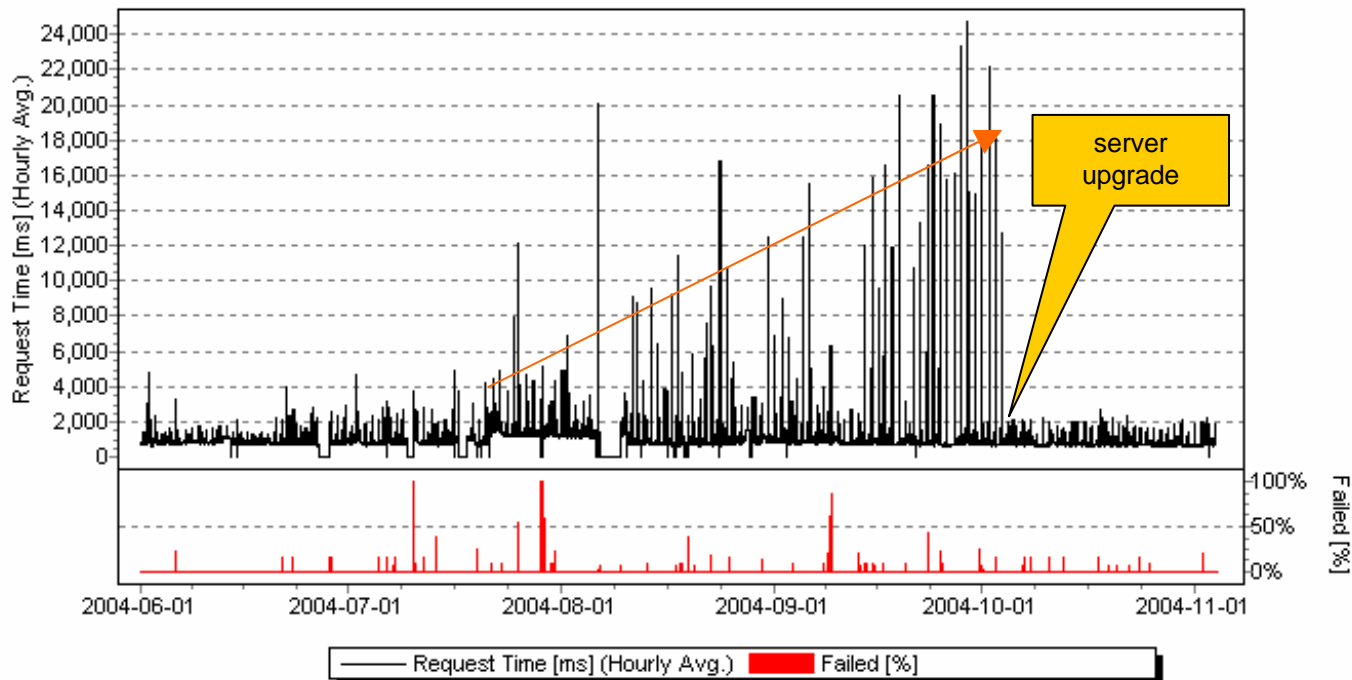
- Usage of the 1 MBit line of Big P solutions' office was steadily growing
- Early September users began experiencing slow Internet access
- Reconfiguration of various servers considerably reduced traffic
- => Upgrade to the more expensive 2 Mbit line could be delayed



# Analyzing Historical Monitoring Data

## Sample 2: Overloaded Web Server

- Due to rising traffic the speed of a script based website deteriorated
- => Decision to upgrade hardware mid September
- => New hardware solved problems early October



# Monitoring is not enough! Be prepared!

## Steps To Secure Your Online Business Success

- Identify the servers/system that are mission critical for your business
- Set up monitoring for these systems (hosted solution or „run-your-own“)
- Try to use advanced monitoring (e.g. scan for „productname“ in homepage)
- Set up backup systems (hot redundancy) that can be kicked in immediately
- Prepare disaster recovery plans
- Have one person on standby 24/7 (to receive notifications via SMS etc.)



# Top 5 Reasons to Monitor Your Network

**There are various reasons to monitor your network&servers**

1. **Secures your turnover – because you will know about problems literally within one minute and you can take immediate action**
2. Gives you a chance to switch to your redundancy systems
3. Know about performance bottlenecks before your customers find out
4. Long term performance data gives you a chance to plan and implement upgrades (e.g. new server hardware, leased lines) without the need for hectic solutions
5. Control whether your provider meets your service level agreement

**Customers turn to your competitor if your website is slow (>5-10 seconds load time) or even fails!**



# Get Started With Freeware Products from Paessler GmbH

## IPCheck Server Monitor (Up/Downtime Monitoring Software)

- Freeware version monitors up to 3 sensors
- Free Download from [www.paessler.com](http://www.paessler.com)

## IPCheck Server Monitor (Hosted Monitoring Solution)

- Free Account monitors up to 2 sensors
- Sign up at [www.ipcheck-server-monitor.com](http://www.ipcheck-server-monitor.com)

## PRTG Traffic Grapher (Bandwidth Monitoring Software)

- Freeware version monitors e.g. bandwidth usage of your DSL line
- Free Download from [www.paessler.com](http://www.paessler.com)

