PROGNOST
Intelligence on Duty

PROGNOST® system security

Closing ports has prevented 100% of all attempted intrusions of PROGNOST® systems

PROGNOST Systems puts great emphasis on a successful protection against pc intrusions.

As a first step, all ports the Mircosoft operating system uses, have been closed. These Windows default ports (e.g. for webbrowser, netmeeting, file sharing) are the open doors world-well-known parasits as "Blaster32" or "Sasser" use for intrusion.

The **PROGNOST® communication module** is client/server-technology and uses only 10 out of 65,535 total ports. As a comparison: a regular office pc uses approx. 1,000 default ports. The number shows it all: PROGNOST® systems have 99% less open security holes.

Alert message of Blaster32-virus in 2003. Billions of pc`s and networks have been infected. The virus used port 135 (Windows default port) to invade into the pc.

The **PROGNOST® protocol** is proprietary with checksum calculation, unique header-ID and 128 bit encryption. Additionally, each transmitted data packet is checked and will be ignored (not only rejected) if it does not meet the security restrictions.

Connections for remote access are created solely via encrypted ISDN-, modem lines, or VPN-tunnels. In contrast to to service packs, patches and antivirus scanners which have to be updated weekly to follow the latest intrusions, the **PROGNOST® system security concept** offers the highest possible security levels. Varmints do not find any means of entry for instrusion.

- Maximum reduction of ports used for highest security against intruders
- Proprietary PROGNOST® protocol, CRC-check, unique header-ID for maximum security
- Up to 196 bit encryption
- Minimized system updates with servicepacks, patches or virus scanners
- Secure remote access via RAS gateway, VPN or internet

PROGNOST Systems GmbH, Daimlerstr. 10, 48432 Rheine, Germany
Phone: +49 (0)59 71 - 8 08 19 0 Fax: +49 (0)59 71 - 8 08 19 42
info@prognost.com