

# The Truth about Intrusion Detection

- Buzzword of the marketing department?
- Light at the end of the tunnel?

**Marc Heuse, nruns,  
Germany**

<marc.heuse@nruns.com>

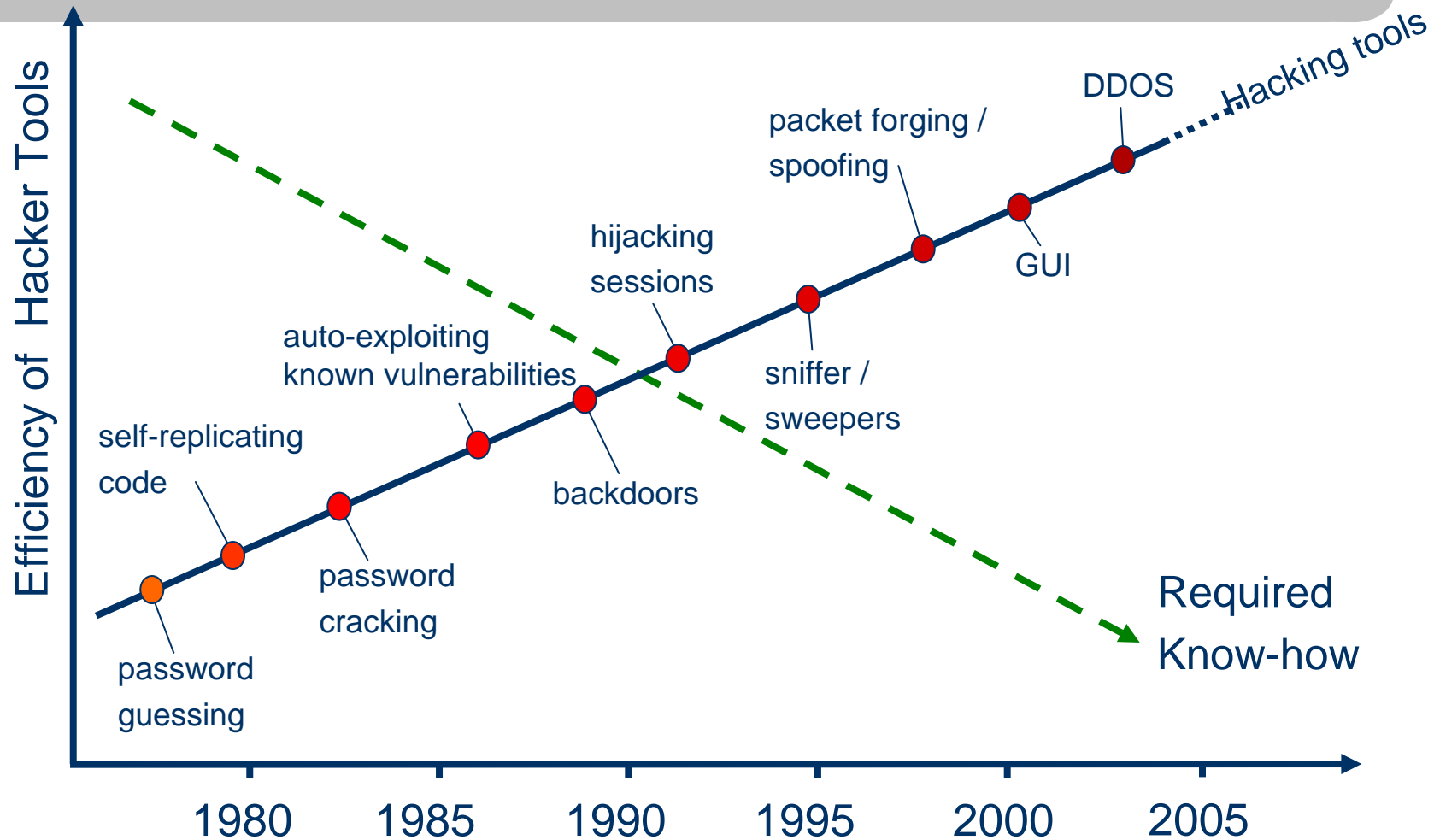
# I am: Marc Heuse

- Doing in-depth IT-Security since 1996
- Project Manager and Security Expert at nruns, Germany (Full time position)
- Founded the SuSE Security Team in 1998, today Security Advisor at SuSE/Novell (SuSE Linux) (part time position)
- Company History:
  - Unisys (Head of IT-Security Services Germany), KPMG (Head of IT-Security Services Germany), Deutsche Bank (Firewall Engineer)
- Specialities:
  - Network, UNIX, Network Pentests, Webapp Pentests
  - Risk Analysis, Risk Management (EAL, CRAMM etc.), BS7799
  - Old School: Wardialing, Wardriving, Lock Picking & Co.

# Contents

- Intrusion Detection – Why?
- Types of Intrusion Detection
- Pro and Contra
- Management, Consolidation and Correlation
- The Future of IDS
- The Reality IDS
- Recommendations

# User friendliness of Hacker Tools



# Hacker Profiles

Criminal  
Energy

Classic  
Insider

Industrial Espionage  
Secret Agencies  
Professional Hackers

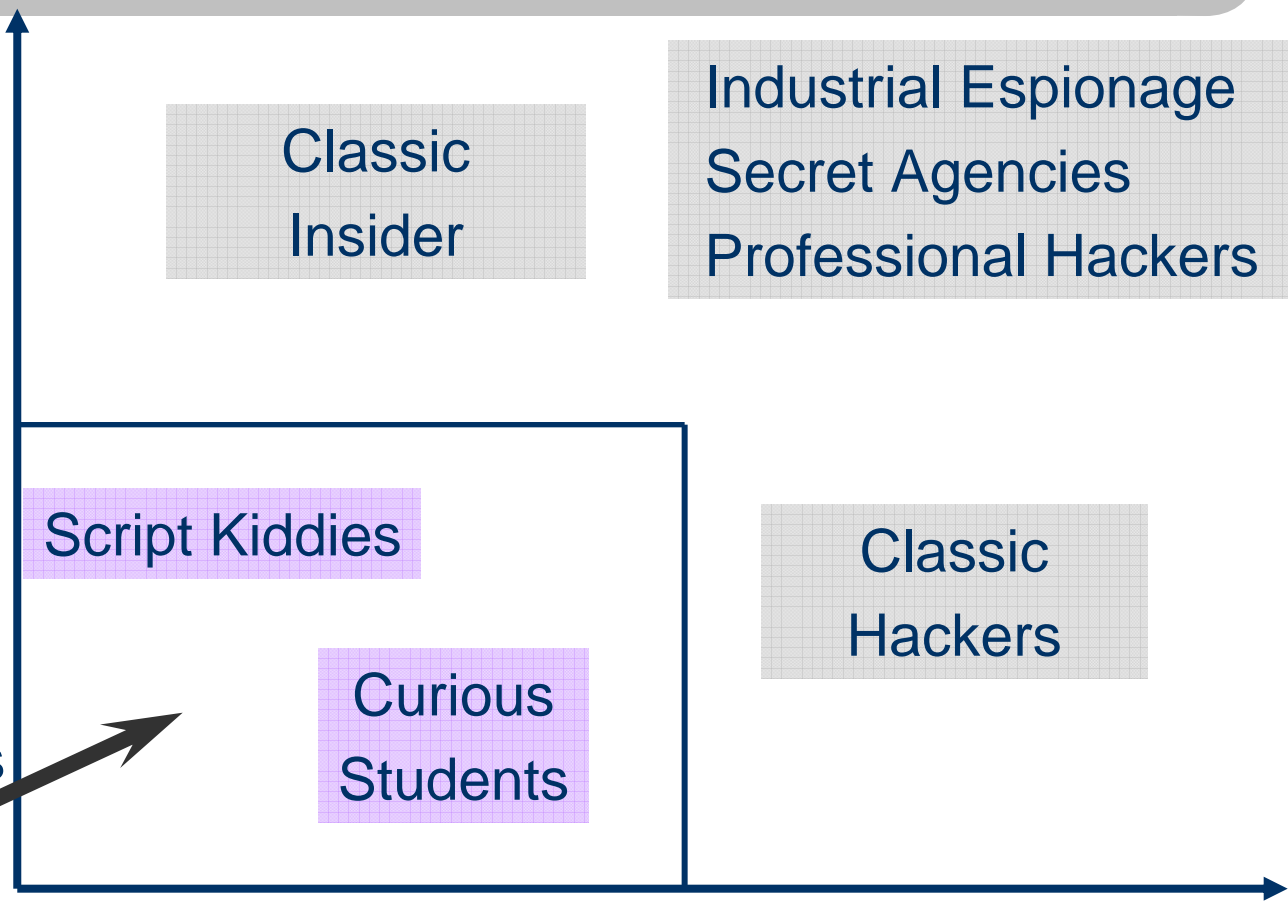
Script Kiddies

Classic  
Hackers

Curious  
Students

Only these cases  
become known!

Know-how



## Who in the Audience ...

- ... has implemented Network IDS and in operation?
- ... has more than 5 events per day with these?
- ... has detected internal staff scanning the network?
- ... has detected a successful intrusion which would have not been detected otherwise?
- ... Has made an ROI calculation for the IDS implementation?

# The Current Market Landscape

- There is only hype and marketing around the IDS topic – but no critical voices
- A discussion about the usefulness is not being made
- The discussion about implementing IDS or not in a company is just done by money and operation

# The Goal of this Talk

- Show Arguments Against IDS
- Create a Discussion about the usefulness of IDS
- Enable an open and per-case decision process on the usefulness and efficiency

# Intrusion Detection Types

- Network IDS
- Host IDS
- Honeypots

# Network Intrusion Detection Systems

- Monitor the network traffic
- Detection Techniques:
  - Search for data patterns (like a virus scanner)
  - Statistical analysis of the network traffic characteristics do detect anomaly or new kinds of traffic (*high false alarm rate, therefore not used within commercial products*)
  - Anomaly Detection in Protocol Data (*Only implemented in a few N-IDS systems, only few protocols supported*)

# Network IDS

- Note:
  - Current N-IDS data might not be used in court as evidence as only offending packets are stored, not the whole session. Therefore the „Chain of Evidence“ is missing. This depends on your laws. Check them out.

# Host Intrusion Detection Systems

- Monitor a single computer
- Detection Techniques:
  - Monitor log files (Syslog/Eventlog) about attack signatures
  - Monitor critical system files about tampering
  - Anomaly detection on application behaviour (*new since 2003, only in two products so far*)
  - (*Anomaly detection of user behaviour – might be implemented in 2006 in H-IDS or Desktop Firewall Produkts*)

# Honeypots

- Networks or systems, which are put in place to be hacked – to detect and analyse attackers
- ... won't be handled in this presentation because of no value for corporations, but rather academics and researchers:
  - Costs for HW and SW of the systems
  - Efforts for installation, configuration and operation
  - Exhaustive monitoring mechanisms required
  - Must be „advertised“ on the network to be recognized as interesting targets
  - ... => very bad cost/benefit calculation for a corporation

# Pro and Contra Network IDS

- PRO
  - Monitors many systems at once (cost and resource efficient)
  - ...
- CONTRA
  - If now or only parts of attack traffic flows by the N-IDS, attacks can't be detected
  - New/unknown attacks can not be detected (*mostly true*)
  - Attackers can prevent detection of their attacks by changing the attack data and traffic flow
  - Encrypting Attacks prevent detection 100% (Web SSL/HTTPS)
  - **A good (= comprehensive and timely) patch management is more efficient than a Network IDS**

# Contra Network IDS

- N-IDS add to the security risks!
- They have buffer overflows like all other software (already seen in ISS, Dragon, NFR, ...)
- A tight security design for a N-IDS network therefore is mandatory!

# Pro and Contra Host IDS

*Only a Host IDS with Anomaly Detection is worth it's name*

- PRO
  - Good detection rate of unknown attacks
  - ...
- CONTRA
  - Requires H-IDS agents on every system which has to be monitored, therefore they cost:
    - Licenses (Money)
    - System resources
    - System stability
  - High effort and expensive for vendors to support multiple platforms and versions, therefore only very few platforms are supported
  - An attacker can – in theory – disable an H-IDS protection/detection before it can send an alarm

# Requirements for an IDS

	Host IDS	Network IDS
Detect known attacks	Yellow	Green
Detect unknown attacks	Yellow	Red
Central management & monitoring	Green	Green
Little performance losses	Yellow	Green
Little stability losses	Yellow	Green
Few false alarms	Yellow	Yellow
High success rate	Yellow	Green
IDS difficult to circumvent	Green	Red

# Central Management & Consolidation

- A central management is mandatory for the deployment of IDS in a corporation
- Most of the management systems allow grouping of events, and ignoring uninteresting events
- Only very few IDS management systems can incorporate event messages from third party security products (Firewalls, Routers/Switches, Anti-Virus etc.)!

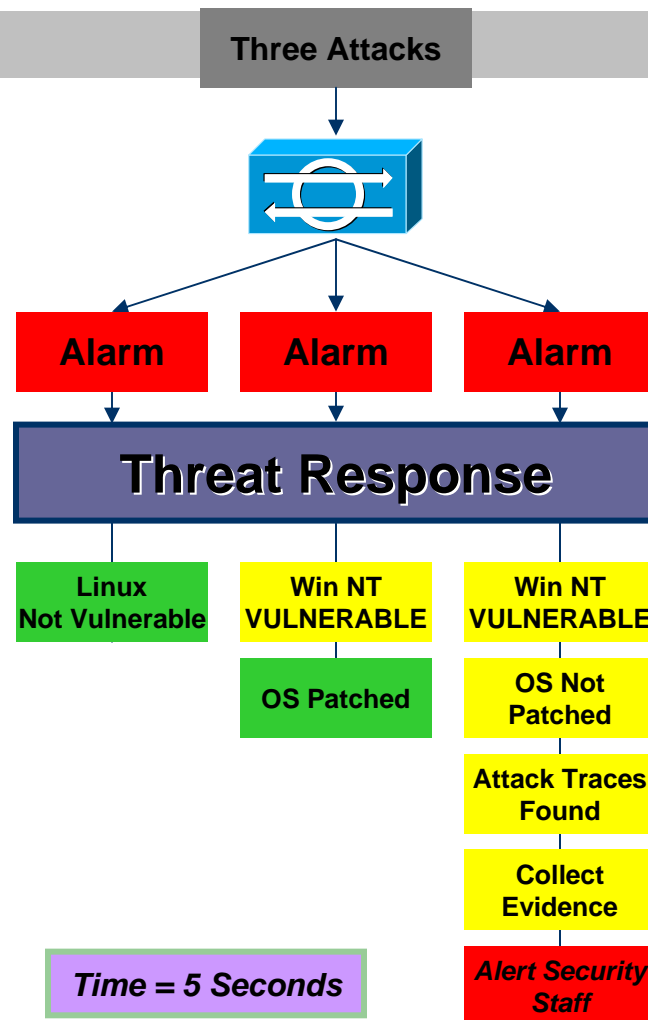
# Correlation of Events

- IDS without correlation uses up too much staff
- An „attack“ mit Nessus shows 300+ events on a mangement station, after correlation only 1
- Only very few vendors currently offer correlation modules, and even fewer are good enough
- Only very few correlation modules come with predefined useful correlation scenarios and can be expanded

# The Future

- Automatic User Identification, Attacker Tracing, Evidence Capturing on Systems and patching systems (***partially possible today, completely 2005+***)
- Prevention (Inline IDS) (***few products today, rest 2005***)
- Intrusion Prevention integrated in Firewalls (***2006+***)
- Heuristic (***2007+***)
- Integration in a central security management (***2005-2006***)
- Integration in a central IT operation management (***2005***)

# Threat Response



1. An Attacker starts an attack on several web servers of a company
2. The IDS Systems detect the attacks
3. A Threat Response Systems analyses the events in real-time

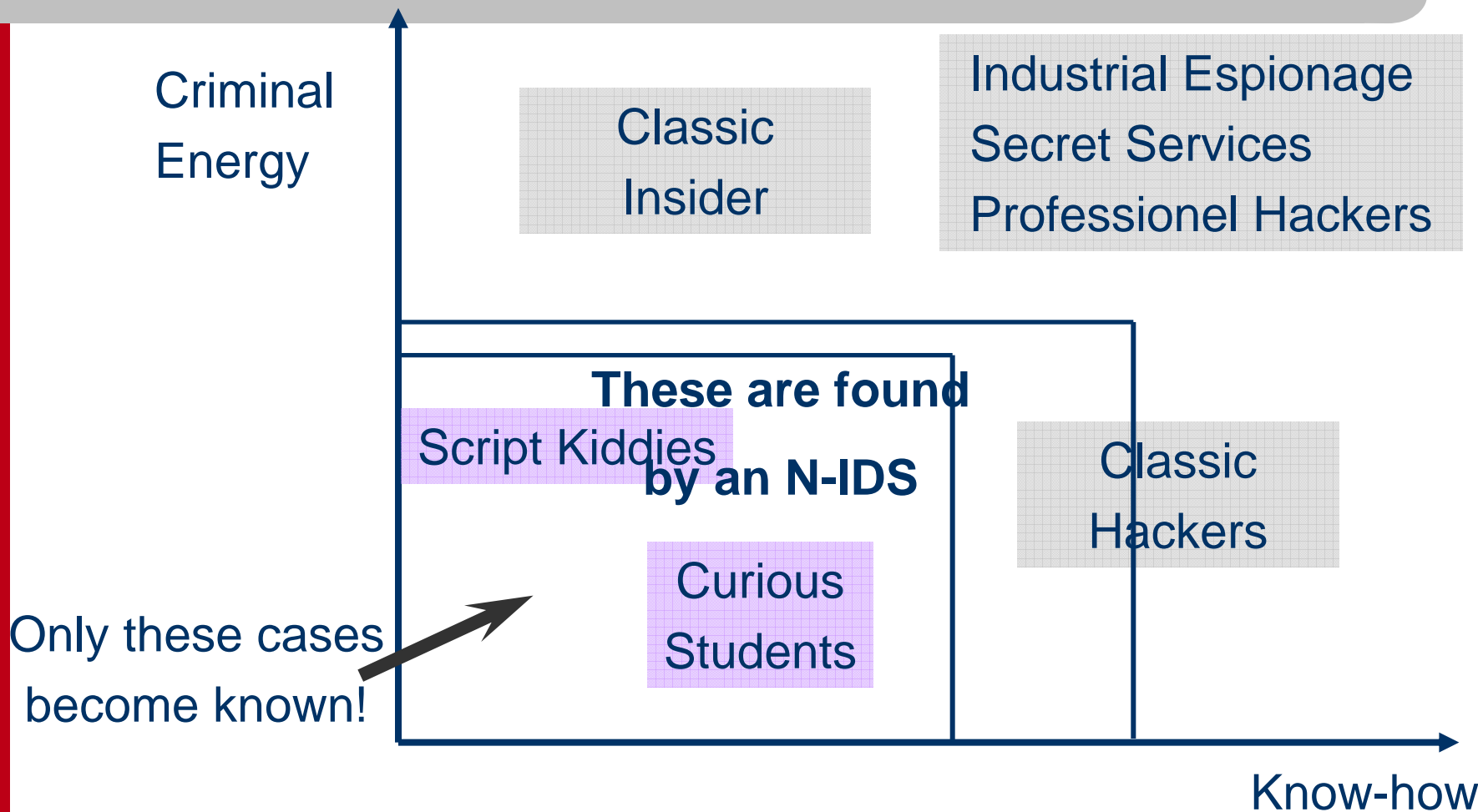
Evaluation if the attack was successful:

1. Is the operating system affected?
2. Is the operating system patched?
3. Do attack signatures exist on the target?
4. Save all logs and data which could be evidence
5. Alarm the administrators

# The Reality of IDS

- The current state of technology is not comprehensive enough
  - They detect only known vulnerabilities  
Means: Patches exist, which – if installed – protect the systems. N-IDS therefore just shows inefficiencies in patch management!
  - Correlation features are partially there, however a company must develop their own rule set. This requires lots of knowledge (which is not there) and lots of effort
- General problems of IDS:
  - The fine configuration takes a lot of time (money), however without it the false alarm rate is too high
  - Additional staff for monitoring the IDS is required, this too costs money

# Hacker Profiles (revisited)



# So what to do?



# Recommendations (1/2)

- Develop a sound protection strategy first!!
  - What has to be protected against whom/what?
  - Does a host and/or network IDS protect the resource against the attack scenarios?
  - ***IDS should always be an additional protection mechanism! Filtering, hardening, patching and system monitoring are more important!***
- Products should just be selected from the „Big Players“
  - Intrusion Detection is a big field – host, network, management, consolidation, correlation – on multiple platforms...
  - Only the big players are able to offer the full products spectrum and features interoperable and cross platforms
    - Symantec, **ISS**, Cisco, **McAfee**
    - Sadly open-source makes no sense here ☹

## Recommendations (2/2)

- N-IDS should only be implemented after:
  - Protocol anomaly detection is working with good success rates
  - The consolidation and correlation modules are shipped with lots of predefined rules
  - *Expect this begin/mid of 2005*
- Define a tight security design for N-IDS systems to prevent taken-over systems to be used as hops!
- Only select an H-IDS, that uses an efficient anomaly detection (Currently only Cisco and McAfee)
- Use H-IDS on security critical system (and just there)
- Without a central management system which does consolidation and correlation IDS makes no sense

# And Don't Forget the PROCESSES

Detection Mechanisms  
(e.g. IDS, Firewall Monitoring, etc.)



Define and establish  
Incident Handling  
and Escalation Procedures



Define Forensical Procedures,  
train and test them

# Your Contact



**Marc Heuse**  
Security Expert

**n.runs** GmbH, Zimmersmühlenweg 62, D-61440 Oberursel  
phone +49 6171 699 – 0, fax +49 6171 699 – 199  
marc.heuse@nruns.com, [www.nruns.com](http://www.nruns.com)  
mobile: +49 160 989 259 41

**Cell Phone No in Manila this week: 09266244427**

**Thank you for your attention!**

Now is time for your  
questions!