CyberSecurity4Rail

October 4th · Hotel Thon EU · Brussels

Are your services protected against cyber criminals?

This Conference will prepare you!
Secure networks for collaborative services

Mick Haynes
Technical Director, Hit Rail
Why are networks a major risk?

VPN private mesh network

VPN Gateway

Internet

Typical Business networks internal VPNs or simple LANs
Typical business network(s)

- Some private LANs
- Some private VPNs for larger users
- One main firewall to internet
- Lots of employees working from PCs, phones and tablets over wireless
- Employees using PCs over local LAN (with secure wireless)

Small Businesses
- Laptops with wireless and PC based firewall
Internet

- Ubiquitous
- Attacked continuously
- Fast but with uneven performance
- Fundamentally insecure
VPN Gateway

- Hit Rail's secure pipe for internet connections
- IPSec tunnel with backup
- Part of SLA
- Monitored and secure
HERMES Private
VPN

- **Meshed** private rail network
- Rail users make two connections to a private Point of presence
- Rail users have specific firewall policies to ensure no unknown connections or traffic is presented
- **Guaranteed** service levels
- Targeted at **mission critical** services
Why are networks a major risk?
The HERMES VPN
cyber security shields

- A single internet gateway
- Software and virus detection
- Highest level of cyber security maturity
- Continuous review and improvement plan
- Comprehensive counter measures against threats
- Proactive incident recovery processes and plans for all known incident types
- Abnormal behaviour automatically detected and alerted
- All assets protected
- Traffic monitoring
- All incidents recorded and analysed
- No EMAIL
- Only “private” addresses used
- A perfect record
Components of the Hermes VPN
Cyber Security Shield

- Ability to control traffic entering the network
- Measurement
- Monitoring

A single @ internet gateway
Components of the Hermes VPN
Cyber Security Shield

Services are protected and monitored

Best practice virus protection on all potentially vulnerable connections

Software and virus detection
Components of the Hermes VPN
Cyber Security Shield

Highest level of Cyber Security Maturity Model

We follow US and European CSMMs
Components of the Hermes VPN
Cyber Security Shield

All incidents recorded and analysed

• Both Hit Rail and users have a process
Components of the Hermes VPN
Cyber Security Shield

- Only “private” addresses used
- NAT an essential requirement of the architecture
- No DNS
Components of the Hermes VPN
Cyber Security Shield

- Continuous review and improvement plan

- The Hit Rail team covers roles monitoring possible threats and possible modifications to all of our protection techniques.
Components of the Hermes VPN
Cyber Security Shield

Comprehensive counter measures against threats

- Access lists
- Limited ports
- Valid source and destination combinations
- Encryption
- Traffic pattern monitoring
- Back ups and automatic re-routing
Cyber Security Shield

Proactive recovery from incidents

- Automated recovery using back up links
- Tested and documented recovery scripts and data
Abnormal behaviour automatically detected and alerted

Components of the Hermes VPN
Cyber Security Shield

- Monitoring sudden excessive activity
- Monitoring loss of activity
- Monitoring loss of connectivity
Components of the Hermes VPN
Cyber Security Shield

- Email and similar risky traffic is not allowed across the network

No email
Components of the Hermes VPN
Cyber Security Shield

All assets protected

- All nodes have good physical security
- Heros and central site secured
- Customers follow the best security practices
Components of the Hermes VPN
Cyber Security Shield

Traffic monitoring

- IP accounting is on all routers
- The data is collected centrally and used to understand patterns of use
- Each traffic type uses a dedicated IP address and is collected to provide application levels volumes
- The variability is understood both within 24 hours and by day of the week and to understand seasonality
Components of the Hermes VPN
Cyber Security Shield

A perfect record

- For over 25 years
- Will be 20 years into the future
Which services justify consideration for network segmentation?

- Operational Services e.g. TSIs
- Rail Technical Services e.g. Scada and ERTMS
- Commercial Services
- General IT Services Email, Business Data
Which are the critical services?

- Control systems including signalling
- Scada networks
- Sales services both passenger and freight
- Infrastructure monitoring
- Communication RU ↔ IM
- International Communication for international services
- Web sites
- Customer communications
What are the different attack types?

- Operational Services e.g. TSIs
- Rail Technical Services e.g. Scada and ERTMS
- Commercial Services
- General IT Services
  - Email, Business Data
- External or Internal Physical Access
- Hackers
- Ransomware
- Viruses/Malware
- Denial of Service (incl. DDoS)
It can’t affect me!

What about?

Operational Services e.g. TSIs

Commercial Services

General IT Services
Email, Business Data

Rail Technical Services e.g. Scada and ERTMS

Hackers

Browser hacked

Ransomware

Viruses/Malware

Denial of Service (incl DDOS)

External or Internal Physical Access

Mobiles

Home Working

Wireless
VPN Costs

Usage per month

Typical Costs per month

400 €

50 MB

USERS 5

Usage per month
VPN Costs

**Typical Costs per month**

- 1.500 € for USERS M
- 400 € for USERS S

**Usage per month**

- 50 MB
- 1.000 MB
VPN Costs

Typical Costs per month

- 1.500 € (50 MB)
- 400 € (1.000 MB)
- 1.000 € (200.000 MB)

Usage per month

- USERS S
- USERS M
- USERS L
### Typical Costs per month

- **1.500 €**
- **400 €**
- **50 MB**
- **1.000 MB**

### Risk Cost

- **Loss of key services (>$1M per day)**:
  - Operations
  - Sales

- **Partial interruption of services (>$100K per day)**:
  - RU ↔ IM connection
  - International connection
  - Client services
  - Business services

- **Reputation (between €10K and €500K per incident)**:
  - Data breach
  - Internal sabotage
Risk Cost

- Loss of key services (>€1M per day)
  - Operations
  - Sales

- Partial interruption of services (>€100K per day)
  - RU↔IM connection
  - International connection
  - Client services
  - Business services

- Reputation (between €10K and €500K per incident)
  - Data breach
  - Internal sabotage
Risk Cost

- **Loss of key services (>€1M per day)**
  - Operations
  - Sales

- **Partial interruption of services (>€100K per day)**
  - RU↔IM connection
  - International connection
  - Client services
  - Business services

- **Reputation (between €10K and €500K per incident)**
  - Data breach
  - Internal sabotage

### Network Costs
€'000 per annum

### Volume
(MB/month)

### Potential risks costs

<table>
<thead>
<tr>
<th>Volume (MB/month)</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>200</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>400</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>1000</td>
<td>10000</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>2000</td>
<td>20000</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>5000</td>
<td>50000</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
<td>10000</td>
<td>100000</td>
</tr>
<tr>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
</tr>
</tbody>
</table>

### Medium risks

<table>
<thead>
<tr>
<th>Volume (MB/month)</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>200</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>400</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>1000</td>
<td>10000</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>2000</td>
<td>20000</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>5000</td>
<td>50000</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
<td>10000</td>
<td>100000</td>
</tr>
<tr>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
</tr>
</tbody>
</table>

### Large risks

<table>
<thead>
<tr>
<th>Volume (MB/month)</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>200</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>400</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>1000</td>
<td>10000</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>2000</td>
<td>20000</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>5000</td>
<td>50000</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
<td>10000</td>
<td>100000</td>
</tr>
<tr>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
</tr>
</tbody>
</table>

### Reputational risks

<table>
<thead>
<tr>
<th>Volume (MB/month)</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>200</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>400</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>1000</td>
<td>10000</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>2000</td>
<td>20000</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>5000</td>
<td>50000</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
<td>10000</td>
<td>100000</td>
</tr>
<tr>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
</tr>
</tbody>
</table>

### ROI

<table>
<thead>
<tr>
<th>Volume (MB/month)</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>200</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>400</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
<td>500</td>
<td>5000</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>1000</td>
<td>10000</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>2000</td>
<td>20000</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>5000</td>
<td>50000</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
<td>10000</td>
<td>100000</td>
</tr>
<tr>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
<td>&gt;200000</td>
</tr>
</tbody>
</table>

### Loss of key services (>€1M per day)

- Operations
- Sales

### Partial interruption of services (>€100K per day)

- RU↔IM connection
- International connection
- Client services
- Business services

### Reputation (between €10K and €500K per incident)

- Data breach
- Internal sabotage
Risk Cost

Saving one incident per year will give a return on investment

Network Costs
€'000 per annum

Volume
(MB/month)
To summarise

Now you know the answers to:

- What is a VPN?
- What are your cyber security risks?
- How does a VPN provide protection?
- Which services are critical?
- Typical VPN costs?
- What could be a business case?
Any questions?