A Shared Approach to Information Security

24th September 2009
Matthew Cook

- Network and Security Manager for Loughborough University
- Managing ESISS initiative
- JANET Contracted Trainer
- Author of multiple Technical Guides/courses
- Invited speaker over 50 events in 10 years
- Personally discovered vulnerabilities in: HP Insight Manager, ExLibris Aleph/MetaLib and Cisco AnyConnect VPN/ASA platform
Agenda

- History
- Geography
- Service Drivers
- Service Catalogue
- Network Based Anomaly Detection
- Reputational Monitoring
- Example Feedback Received
- How to find out more information
History

- Shared Services concept
- HEFCE expressions of interest
- Response by Richard Smeeton
- Feasibility Study [October 2007 – May 2008]
  - Led by Tony Brookes
  - Collaboration between six East Midlands Universities
- HEFCE pump primed service
- Service delivery award to Loughborough University [April 2009]
Geography – JANET(UK)

JANET Regional Networks

[Map of the UK with regions highlighted in different colors, each representing a specific network or region.]
Geography - EMMAN
Service Drivers

- Strong support from EMMAN community
- Individual requests from other academic institutions
- Feedback from JANET CSIRT events
- UCISA Directors ‘Top Ten Concerns’

- Organisations are broadly facing the same challenges which do not provide distinct competitive advantage.
Network Based Anomaly Detection

Campus Network Anomaly Detection Service [Per MAN/RNO]

Management, report generation and queries

Device Status

Optional Syslog feeds

Optional Active Mitigation

Optional NAC Integration

ESISS Domain

Management Console - SMC

Netflow Collector - XE-2000

University Domain

HTTPS

Local Services

EMMAN

Internet

University Site

Proactive monitoring of Network Flows by ESISS

Optional management access for local staff
Requires JAVA, plus ports 80/tcp, 443/tcp, 49000/tcp and 49001/tcp
Network Based Anomaly Detection

Campus Network Anomaly Detection Service [Per Site]

ESISS Domain
- Management, report generation and queries
- Firmware updates
- Device Status
- Optional Syslog feeds

University Domain
- HTTPS
- HTTPS
- SNMPv3

Local Services
- Time Synchronisation
- NTP
- Optional Active Mitigation
- Shun et al.
- Optional NAC Integration

Management Console - SMC
Netflow Collector XE-2009
EMMAN
Proactive monitoring of Network Flows by ESISS
Internet
Netflow Collector XE-1000
University Site
All flows kept on site, only queries traverse Internet.
Netflow Data from one or more routers (6,000 fps)

Optional management access for local staff
Requires JAVA, plus ports 80/tcp, 443/tcp, 49000/tcp and 49001/tcp
Reputational Monitoring

- THE: “University fails to use its own language guidelines in its publications.”
- Pinsent Mason: “Domain hijacking/squatting”
- Guardian: “University hosting illegal DVDs”
- Twitter: “I’ve failed to do any work today, due to network outages!”

- Internet based reputational is critical
## Reputational Monitoring from ESISS

**Organisation:** Loughborough University

**Overall Health indicator:**

### Test Mechanism Summary

<table>
<thead>
<tr>
<th>Test Mechanism</th>
<th>Description</th>
<th>Weight</th>
<th>Most Recent Score</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Page Search</td>
<td>Checking the name &quot;Loughborough University&quot; against homepage URL</td>
<td>0.9</td>
<td>1</td>
<td>2009-09-09 02:34:02</td>
</tr>
<tr>
<td>[edit parameters]</td>
<td><a href="#">More info...</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webcam Finder</td>
<td>Network visible webcams</td>
<td>1.0</td>
<td>1</td>
<td>2009-09-08 18:15:08</td>
</tr>
<tr>
<td>[edit parameters]</td>
<td><a href="#">More info...</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Proxy Servers</td>
<td>Open Proxy Testing</td>
<td>1.0</td>
<td>1</td>
<td>2009-08-25 16:48:52</td>
</tr>
<tr>
<td>[edit parameters]</td>
<td><a href="#">More info...</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JANET RBL presence</td>
<td>Check Lboro Hosts for RBL entries</td>
<td>1.0</td>
<td>1</td>
<td>2009-09-08 20:45:02</td>
</tr>
<tr>
<td>[edit parameters]</td>
<td><a href="#">More info...</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check for banned words</td>
<td>Look for banned words in Loughborough University</td>
<td>0.5</td>
<td>-2.498e-16</td>
<td>2009-09-09 04:23:10</td>
</tr>
<tr>
<td>[edit parameters]</td>
<td><a href="#">More info...</a></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example Feedback Received

Feedback on security notifications:

“Thanks for this - it's just the kind of helpful message that explains the problem, and the solution, in sufficient plain English for those who are not adept at IT Security to understand and respond to quickly.”

Feedback on Information Security consultancy:

“There's been a great buzz here since your visit and we're all fired up now with loads of actions having been suggested already, so the visit was an absolutely resounding success - many thanks again.”
How to find out more information

- Website: http://esiss.ac.uk/

- Email: esiss@emman.net

- Or chat afterwards with myself…