Lazy Management of a Secure Gateway

System Administration Miniconf
Tuesday, 25th January 2010
LCA2011, Brisbane, Australia

Mark Suter
Senior Gateway Engineer
Unisys Australia Pty Limited
Prefer going to great effort to reduce overall energy expenditure? That's my kind of Laziness. Add some Perl-ish Impatience and Hubris and you have a good description of my current workplace.

This talk is a "How we do things" walk-through of my workplace with most of the focus on what works for us, minus some detail to keep the security people onside ;)

My workplace is a secure gateway for a large government client. It has many different types of devices all forming part of a managed response to the risks we face in connecting to the world.

Of course, I'll mention the Wiki that I presented on last year but this time with more about how it fits into our workplace and almost nothing on the wiki itself.
Click to add an awesome title

• Click to add an awesome outline
Laziness is the quality that makes you go to great effort to reduce overall energy expenditure. It makes you write labor-saving programs that other people will find useful, and document what you wrote so you don't have to answer so many questions about it.

http://c2.com/cgi/wiki?LazinessImpatienceHubris
Secure Gateway?

• Government Client
• Large internal network
• Many B2B links
• Let people work with protection and audit.
• PSM / ISM / IRAP
High Level Architecture

- Primary and Secondary Sites
- Over 200 pieces of kit
- Multiple redundant traffic paths
- Single point of entry/exit
- Extensive Monitoring
Customer Common Services

• Web Browse, including content filtering
• Internet Email (SMTP), including anti-spam
• DNS: Public, Gateway, Business Partners, etc
• Business Partner Connections
  • 20 + links to Business Partners
  • Specific data requirements
  • Failure closes borders (Airports and Cruise Ships)
• Secure File Transfer (drop box w/ automation)
• Remote Access VPN Solutions (collect them all!)
What we do (1/2)

• Firewall Administration
  • Multiple Vendors

• IDS/IPS Administration

• Router/Switch Administration

• Linux Administration (DNS, NTP, Logging, etc)

• Log Analysis
  • Including Anomaly Detection

• System Monitoring and Reporting
What we do (2/2)

• Incidents, Problems and Changes
• External Hosting Infrastructure
  • Reverse Proxies
  • SSL Decryption
  • Anti-virus Checking
• Web (XML) Messaging Gateways
• Documentation
• Certification
Documentation
Openness

• Very good relationship with customer
• Saves a huge amount of time
  – e.g., B2B “Link Documents”
• Un-needed secrecy **hurts** Security
Firewall Rulesets

• Live Rules
• Exports into Subversion (web viewable)
• Wiki versions of B2B “Link Documents”
Naming and Addressing

• IP Plan
• Multi-split DNS
• Public space but with many “private” ranges and a lot of NAT :( 
Web Browse: what we use

- Blue Coat ProxySG Appliances
- SSL Intercept aka “Man in the Middle”
- Blue Coat Web Content Filtering
- Blue Coat Anti-virus appliances
Email: what we use

- Axway Mailgate SMTP Appliances
- Very strong tagging/policy capability
- Anti-spam
  - IP Reputation Filtering
  - SMTP checks (good behaviour)
- Approx 100,000 legitimate emails per day
- About 7% spam count (user web-based digests)
- > 80% connections rejected
Email: Anti-spam

Traffic Volume

Accepted and Rejected by Percentage

|       | Accepted 1506199 (18.86%) | Rejected 6481934 (81.14%) |

Rejected Mail by Type

<table>
<thead>
<tr>
<th>Defense</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHA</td>
<td>21148</td>
<td>0.33%</td>
</tr>
<tr>
<td>DoS</td>
<td>19211</td>
<td>0.30%</td>
</tr>
<tr>
<td>DNSBL</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>General</td>
<td>1130156</td>
<td>17.44%</td>
</tr>
<tr>
<td>Manual</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>IP Reputation</td>
<td>5311419</td>
<td>81.94%</td>
</tr>
</tbody>
</table>

Traffic Volume

Count/HR

- Accepted
- Rejected
Passwords

• Many different types of devices
• Many of each type of device
• Separate credentials per trust zone
• One central KeePassX file
Monitoring (1/2)

• Cacti – Capacity Planning
• Nagios – Everything okay right now?
• NetFlow – historical “tcpdump”
Monitoring (2/2)

- SourceFire – IPS/IDS
- Logs – syslog-ng /archive/yyyy-mm-dd/
- ArcSight – SIEM
Questions?

This presentation is at http://zwitterion.org/talks/