**September 25th 2012**

**Security Breakout Group Notes**

Aim: to discuss

* Security of the OpenHIM
* Securing the registries – how do we limit public access but make web access available to those who need it

We need to ask – what happens if the data is compromised?

What are the policy and regulatory issues? What is the security?

To consider:

* access to data – both read and write access
* Asset may be – the data, the data quality, performance, reputation,
* Threats – asset could be stolen, attack paths (hacking)
* What are the counter measures to the threats?

RC described the AS-IS situation now:

HIM installed in NDC – exposes API over https using basic authentication with a self-signed certificate on mule server

At the APPLICATION LEVEL

At OpenMRS and RapidSMS use a username and password to access

1. Web service calls - From HIM to registries only http

* CR has session key
* FR has basic authentication
* SHR has basic authentication
* TS is in public domain

2. Web application per registries

* Has a username and password to login
* All UI are http
* Terminology Service – DTS-Editor has https and the other interface has http – is read only at thisend

***AT HOST LEVEL***

* SHR and CR are on physical boxes
* Rest are on virtual machines

If we do not have control over physical security then must assume it is a public place

NEED:

* a third party to come in and evaluate by doing an audit and provide recommendations

(find out if government of Rwanda has it’s own service to do this)

* to have host-based intrusion detection on your machine for detection
* to develop checklist further for use AND to manage and monitor system

***Short term tasks – basic plan in place***

* Switching all to https
* Block ports on the server
* Install packages to protect servers
* All registries should have same procedure
* Certificate – either signed internally by Daniel(MoH) or buy a certificate from a third party such as Verisign or GoDaddy (This should include a certificate for OpenMRS between clients and server). Recommend – 3rd party certificate

The obvious weak spot is at client- OpenMRS – 450 facilities with full access and only password protection - People will always share passwords so must decide on a usage policy

Client certificate will be most secure but has high management overhead and therefore cost

Think that SHR and CR need higher level of security although someone else must identify what the requirements are. It is not for us to decide but must have ability to deal with it.

TO DO –:

* Certificate should be signed by Daniel Murenzi rather than Ryan
* MOH should get a “proper” certificate to sign with
* Lock IPs with access to APIs
* Lock ports on each box
* Must find out what policies are in place at the NDC – aim to develop a document for RHEA that aligns with this and get it signed off at as high a level as possible – Can propose more detailed policy if not there in existing policy
* Must identify person responsible for system security / component security
* Must find out if government of Rwanda has its own service to do security audits
* Read up on ISO 27000 and also the SUBSA model
* Find out about usage policy and/or help to define one
* Set up an activity log for each registry to monitor what is going on

***BACKUPS AND DISASTER RECOVERY***

* How far back in time should you need to recover to?
* What intervals should you be doing this? Daily, weekly, monthly
* How long do you keep backups for ?
* Must define a policy for this and get sign-off
* Need an off-site virtual machine to handle backups
* Can keep snapshots with a simple script
* Do database dumps
* Current plan – to have a Backup server to send backups to within the MOH – bandwidth btw them should be sufficient.
* Remote storage needs the same security level as live system otherwise must consider encryption of data before sending it to backup server - Recommend - Better to store data backups unencrypted if the physical security is very good
* Process to restore – must rehearse the restore and ensure it is recoverable
* Also need a fall-back system / mirror system
* Separate snapshot of system plus data backups
* Must be aware of the problem of propagation of errors from image on VM, but still much faster and cost effective to use virtualization
* Must build procedures into support policies for system administration teams
* Consider a communication strategy: how do we tell users when the system is up or down - SMS notifications one option