

Session 33: OpenMRS Security

Facilitators: Isaac and Ian

Brief

Members present :

Sarah Bostan
Ben Ajwant (KenyaEMR)
Isaac Sears
Herbert
Keziah
Rabindra Bista
Simon Savai
Zainabe Dada

Discussions

Two lenses: Development perspective and implementers perspective

Ben Ajwang: We've kind've felt that things were secure enough with Ubuntu rather than Windows, but we've been working on a cloud implementation and running into some security concerns (partitioning / data access), defining the correct roles, security of data in transit or at rest.

Q to Ben: What cloud provider are you using? Azure. Data needs to remain in country and this is possible with Azure. Wide APN, encrypted at the application layer.

One of the biggest problems that comes up is that what is considered security best-practices depends on infrastructure and technology that may not exist everywhere in the world. For instance, two-factor authentication relying on, e.g., smart phones vs SMS. It's a struggle to balance security, not just with usability but also low resource environments.

How are security recommendations implemented on-the-ground? RBAC (role-based access control); within the facility, each person has a role, but sometimes different users might need to perform a specific task. This results in a loosening of security rules.

Superuser Role: allows the user to be able to do everything. Feel like this role needs to be assigned to at least one user at each site, but then they might have more access than we typically be comfortable with.

Feature request: Ability to create a user able to create new users and assign them roles without having to make them a superuser.

Permissions are perhaps too granular, which makes it hard to properly define roles. Definition of roles requires manual effort on the part of implementers.

Administrator role without *full* permissions. A proper system administrator role. (Create and manage users, upgrade system, update indexes, etc.)

Password controls! (Restricting common passwords; password security metrics; shared passwords)

What does your update process look like?