CiviProxy

CiviCRM Enhanced Security Architecture

SYSTOPIA
Organisationsberatung

Björn Endres,
SYSTOPIA

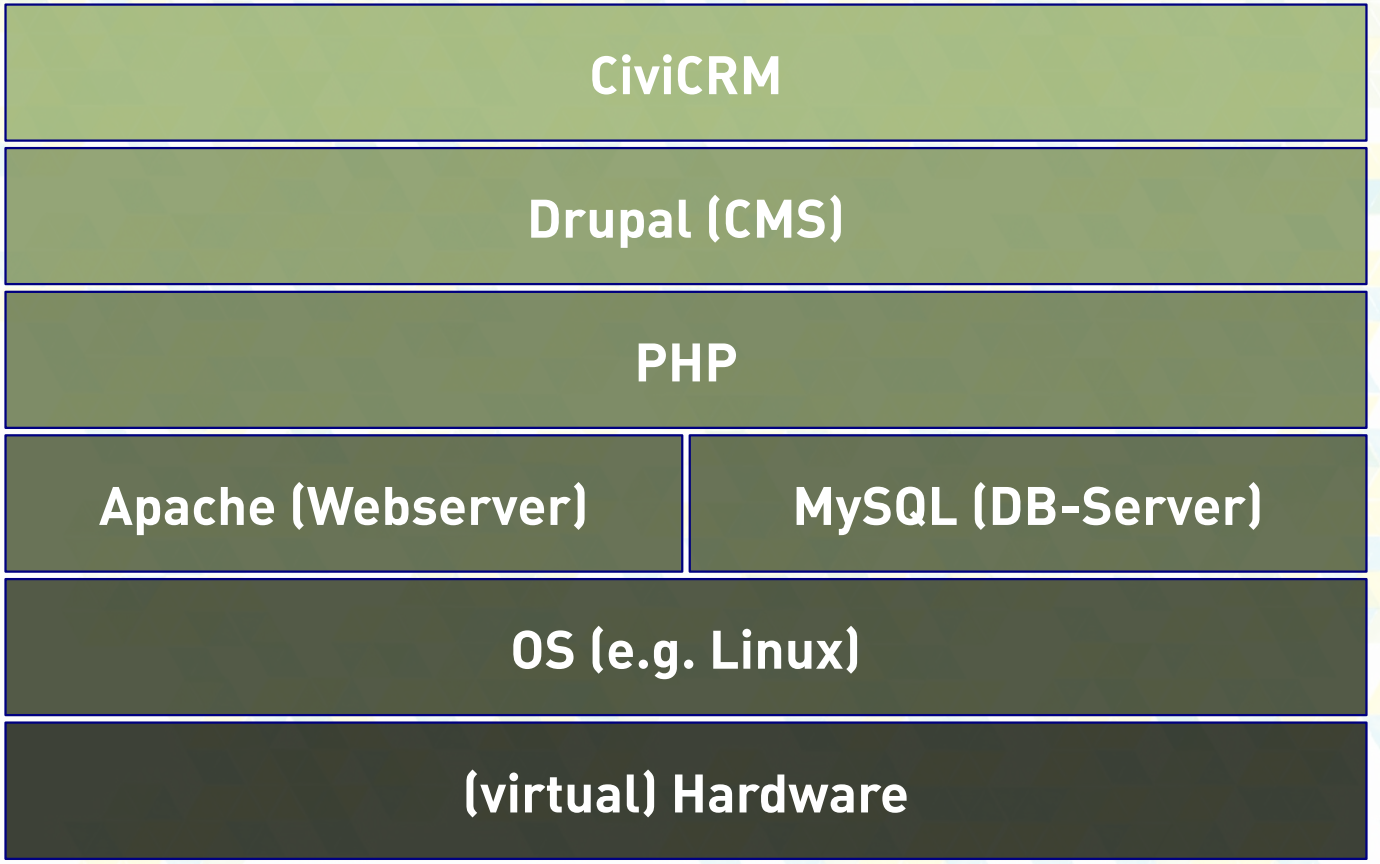
Why?

- System complexity increasing
- New first-choice way to harm your organisation
- State-funded surveillance
- Hacking tools easy-to-use and widely available

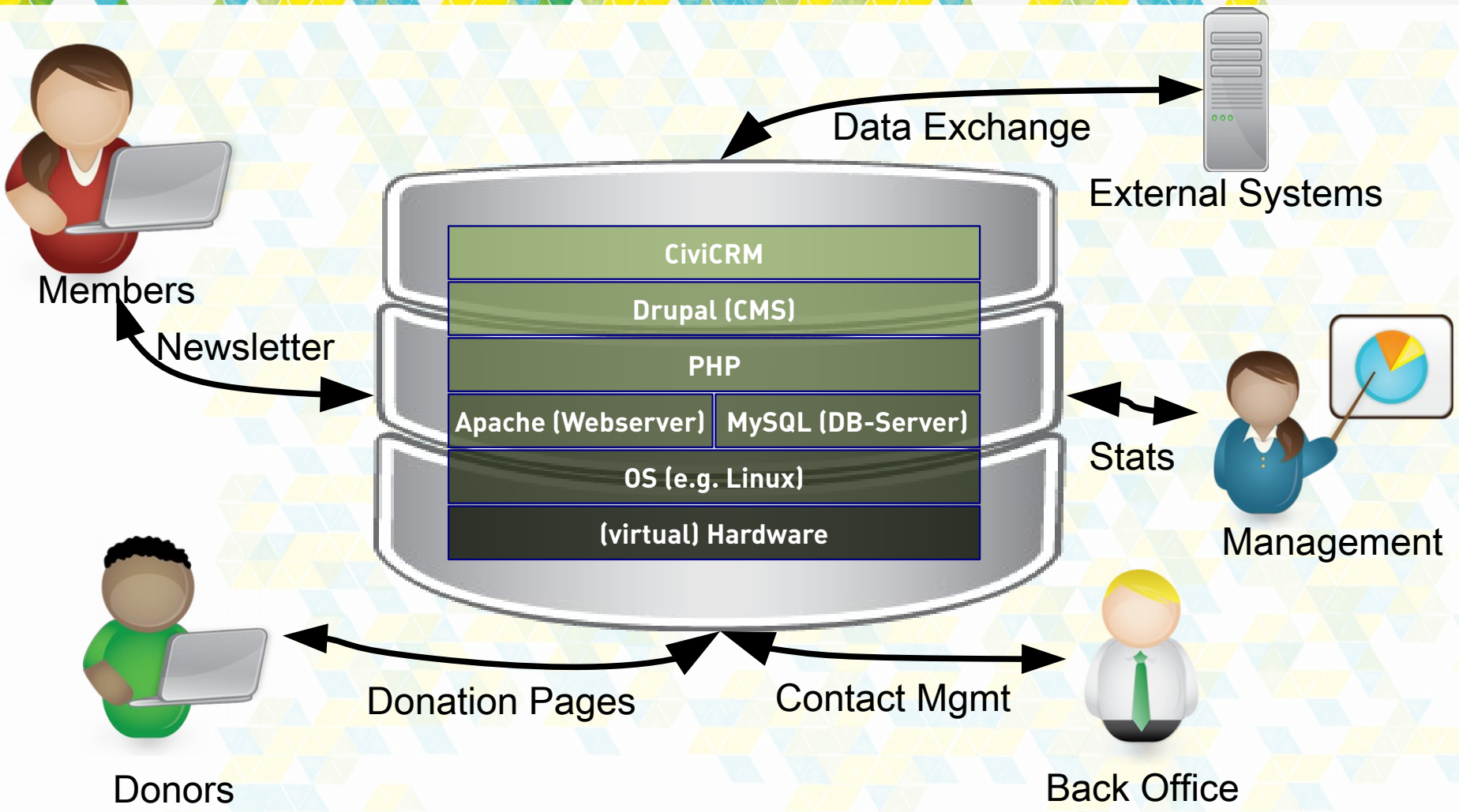
Agenda

- CiviCRM Security Threats
- Application Firewalls
- CiviProxy
- Live Demo
- Discussion

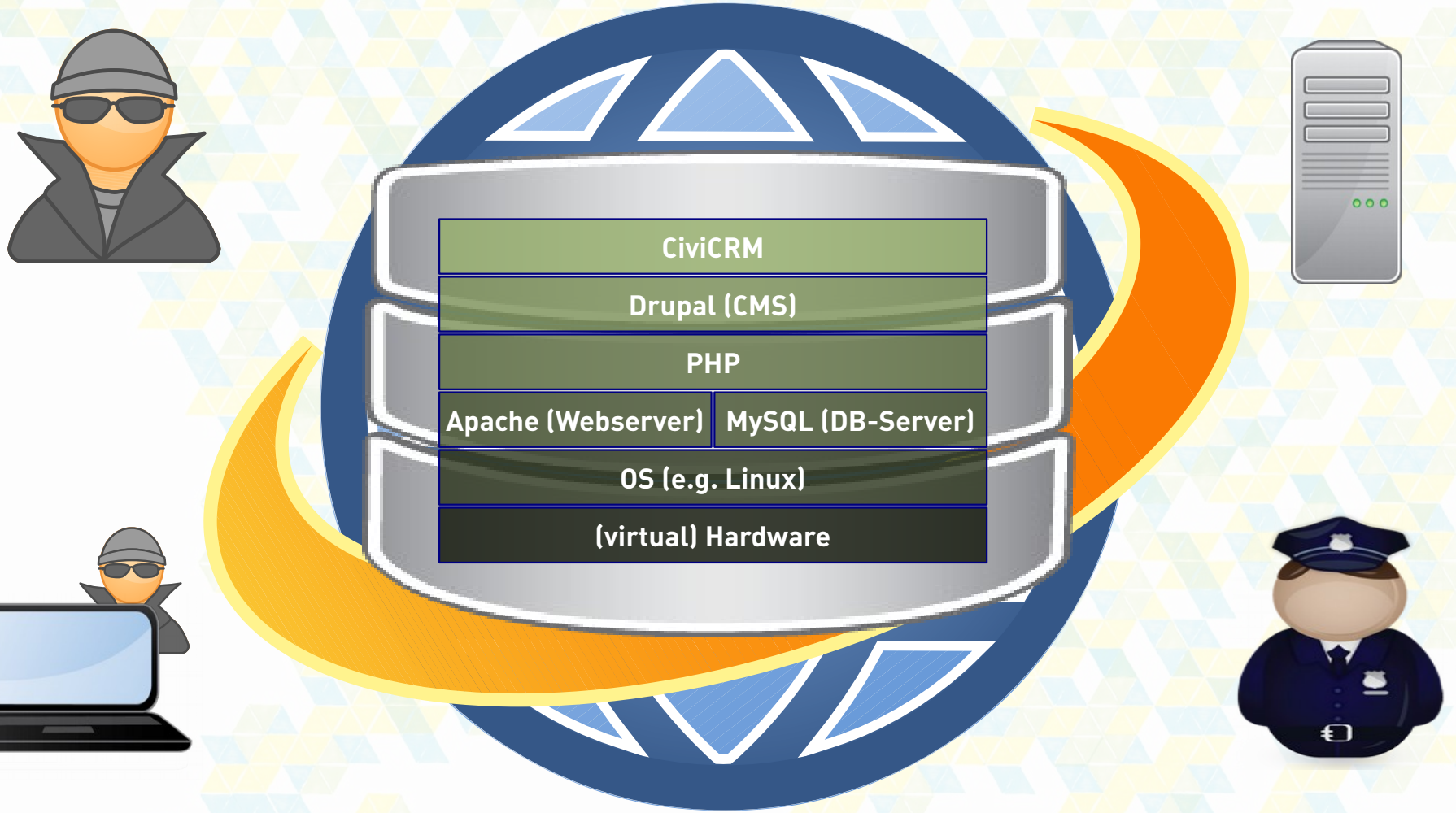
CiviCRM Architecture



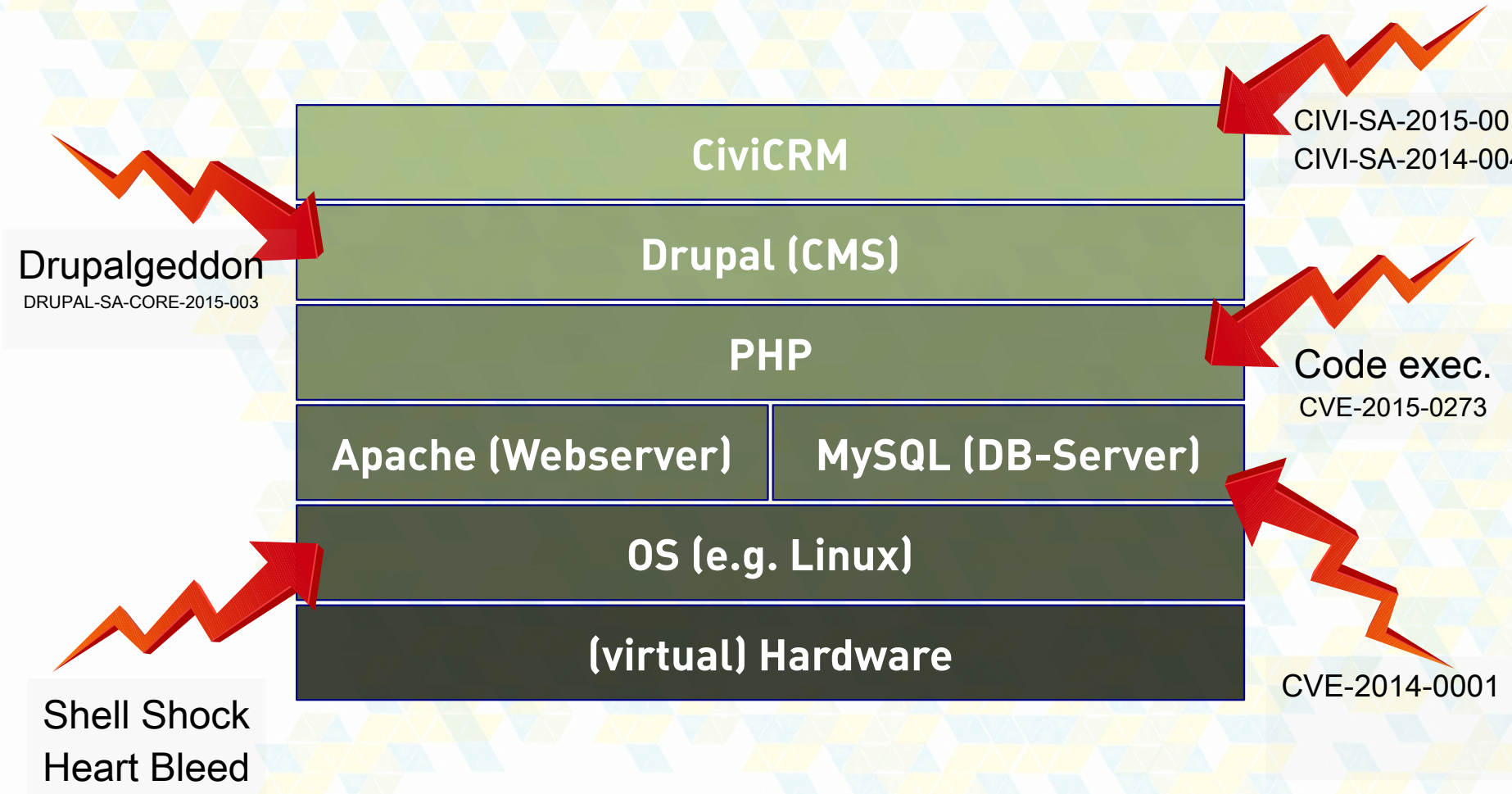
CiviCRM Architecture



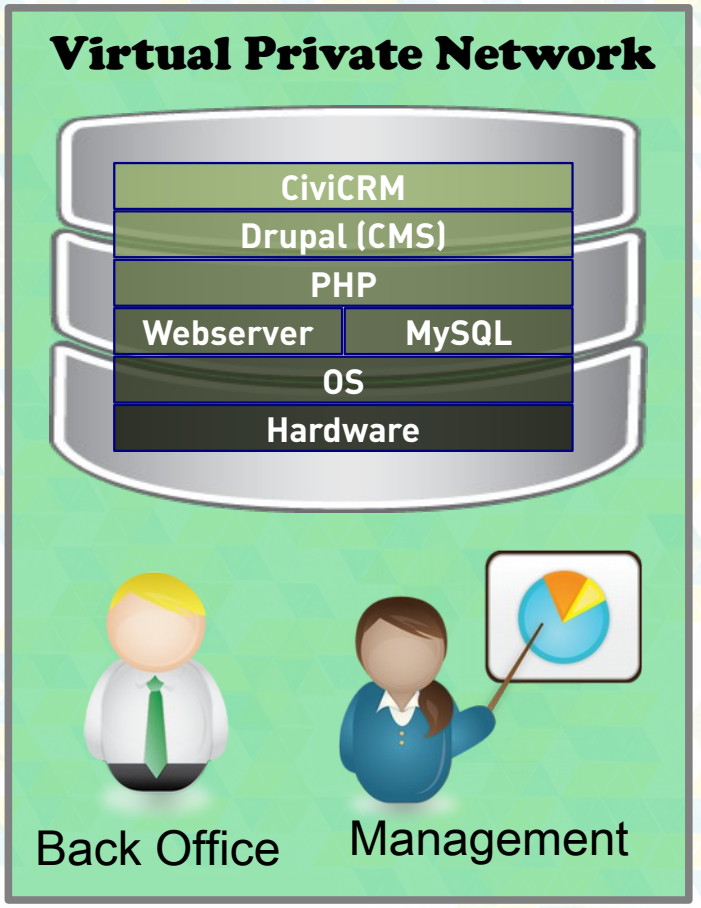
CiviCRM Security Threats



CiviCRM Security Threats

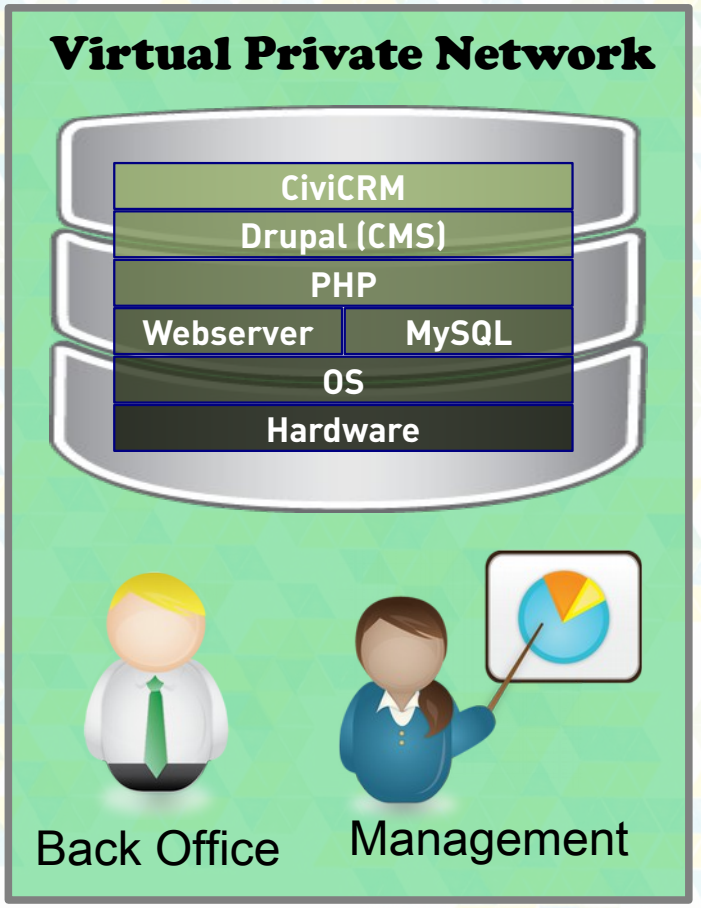


CiviCRM Virtual Privacy



CiviCRM Virtual Privacy

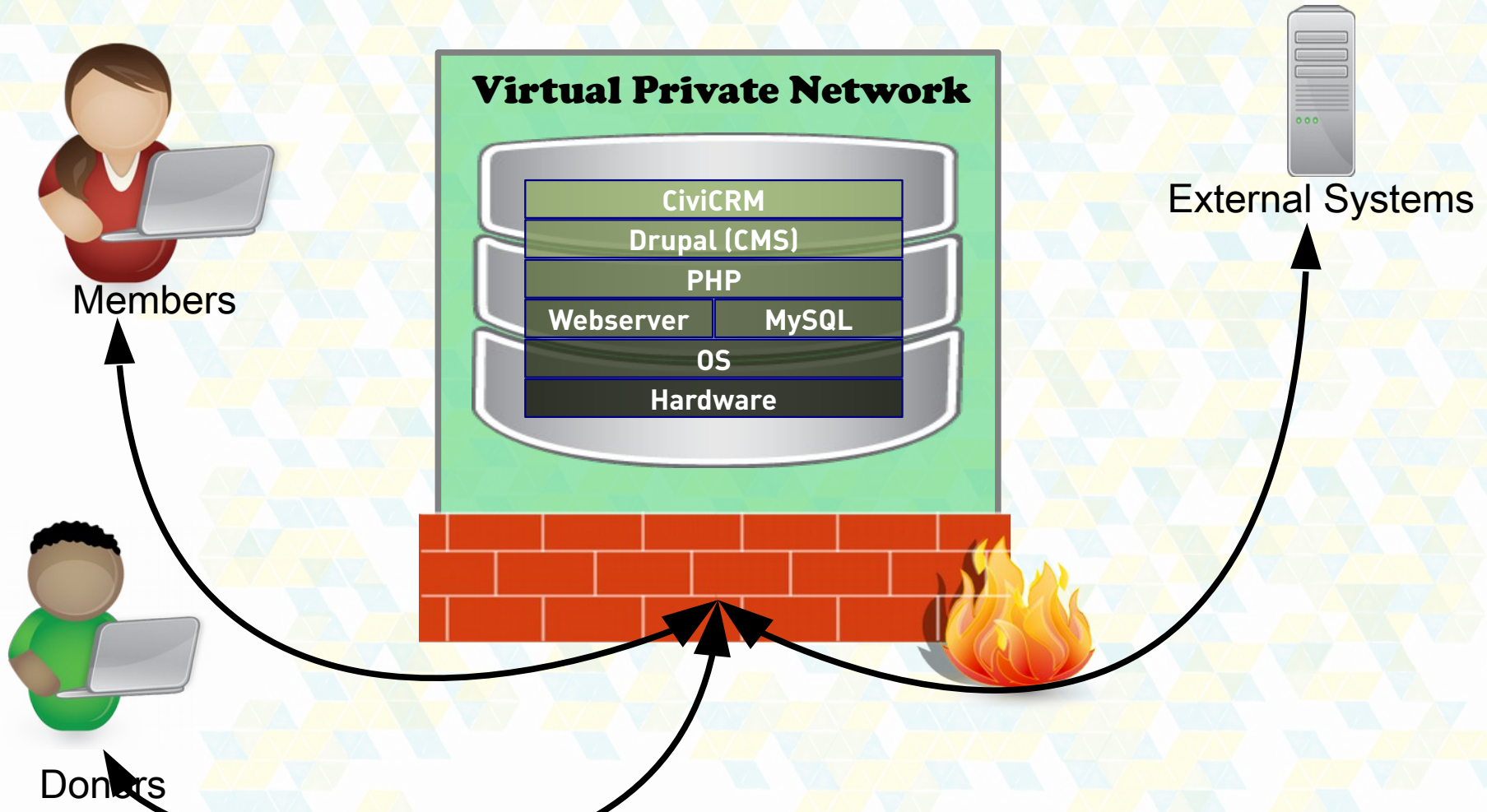
Members



External Systems

Donors

CiviCRM - Firewall



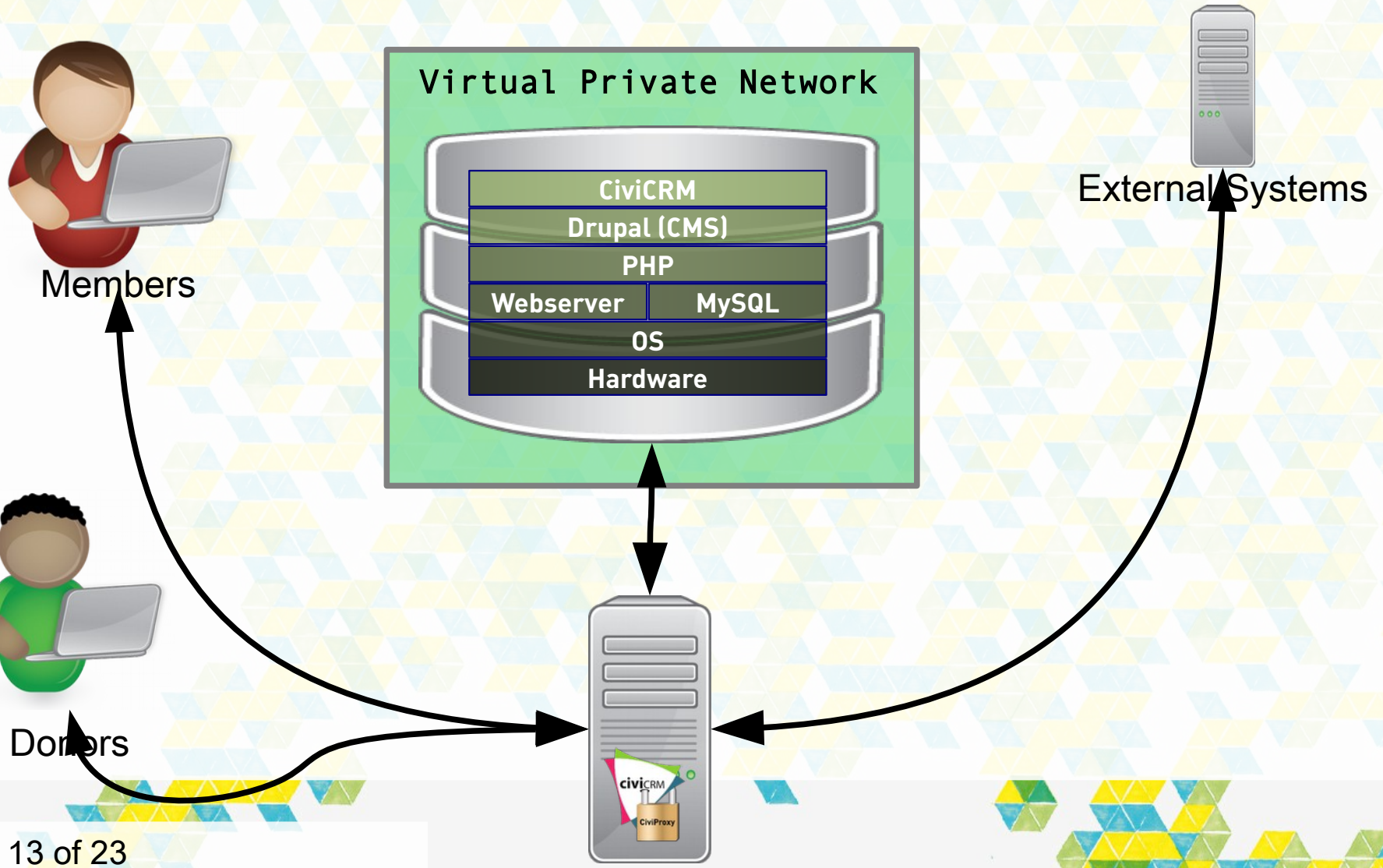
Application Firewalls

- Filter the traffic to / from the server
- Behaviour defined by a set of rules
- Various Open Source options available

Application Firewalls

- Tradeoff between number and precision of rules
  → the more precise the rules, the harder to maintain
- Tendency to be too lax, not to obstruct donor interaction

Alternative: CiviProxy



CiviProxy

CiviProxy Mission:

- Security proxy designed for CiviCRM
- But: keep it simple!
- Whitelisting (instead of blacklisting)
- Strict parameter sanitation
- Add / enable only the desired features.

CiviProxy

CiviProxy Implementation:

- Set of very simple PHP scripts
- Can be simply uploaded to any managed server or web-hosting service

CiviProxy

Managed hosting has its perks:

- High security standards
- Inexpensive
- Huge bandwidth, well connected
- “Shields” your network from unnecessary traffic

CiviProxy

What it can do (atm):

- Serve (cached) newsletter resources
- Serve (cached) static newsletter
- Handle newsletter sign on / off
- Full REST API
- Flooding / DOS filters*

*) commissioned, but not implemented yet

CiviProxy

What it can **not** do (yet):

- Donation / membership / event / petition pages
- Drupal Webforms
- Self service dashboard
- Profiles

CiviProxy

Feature: “Mailings”:

- CiviProxy caches all resources
- Pass on all “open” and “click-through” events
- Comes with a CiviCRM extension to automatically “mend” all URLs in outgoing mails

CiviProxy

Feature: “API”:

- API backbone of communication with other systems.
- Simply define entity and action to allow, and define sanitation rules

CiviProxy

Demonstration

AF vs. CiviProxy

- extensible
- established
- hard to set up
- hard to maintain
- API extension hard
- input sanitation complex

- predefined functions
- newly developed
- easy to set up
- easy to maintain
- API extension easy
- input sanitation built-in

CiviProxy

Discussion

Interested? Contact us: info@systopia.de