GRNET NOC

How we try to avoid getting pwnd

{ikakavas,kargig}@noc.grnet.gr

Sane security policies

Debian Linux

Good balance between features and stability

Has its own security team backporting patches

~3+3 years of support per release→enough for us to upgrade

Very responsive community→You are not alone!

Sane security policies

OS Updates

3 maintenance windows each week

Serious security updates can bypass maintenance windows if needed

Use orchestration to automate updates per service type or per project

No unattended updates (yet…)

Sane security policies

Services

Listen/Bind only on needed interfaces/IPs

Don’t run as root (duh!)

Don’t run multiple/unassociated services on the same host / compartmentalize risks

We own our L1, our datacenters...but we use TLS as much as possible, even for intra-DC connections.

Sane security policies

Firewalling

No external appliances, firewalling happens on _every_ host + router ACLs

Default INPUT policy DROP

Cannot SSH from one machine to another

Firewall rules managed by puppet exported resources

staging/testing/demo environments use even stricter firewall policies

Sane security policies

SSH/sudo access policy:

- NO access unless REALLY necessary (user account == potentially root)
- No SSH with root account allowed (duh!)
- SSH only allowed from specific IP ranges for specific users/groups (managed by puppet)
- Users don’t have passwords, just password protected SSH keys (different from their LDAP password!)
- Password-less sudo to get root
- Root access with password only through local/IPMI console (IPMI IP ranges are very very firewalled)

Sane security policies

Web applications:

Audit custom code before going live, ok ok..not aaaaalways

Use Debian package versions for web applications

Restrict plugins used, register for update notifications, update frequently

Don’t use pirated plugins/software→More harm than good.

Sane security policies

Monitoring

Icinga checks whether firewall is applied for every host, whether puppet runs, etc

Logs sent to multiple destinations (remote syslog, ELK, etc)

Dashboard for anomaly detection on hosts

Sane security policies

Procedures

Write down each step needed when someone joins/leaves the company

Contact US!

Are you interested in joining GRNET ?

Contact us at {ikakavas,kargig}@noc.grnet.gr

Or take a look at https://grnet.gr/en/company/career-opportunities/