Your VE's provide internet access to other private networks or what ?

I manage a server where i use the setup i'm talking about, because i live in Europe too

I don't think that exposing a HN that is running only the ssh daemon to internet is a great security risk. Maybe i'm wrong but i'm using such setup for four months now and i didn't have any incidents regarding the HN. Besides the normal dictionary attacks on the ssh daemon which i block using public key auth (a normal thing to do in these days).

On this setup i provide internet services for several domains and as needed will increase the domains hosted on the HN.

Right now i provide DNS, Mail, Database, web and ftp access to 10 domains without any problem whatsoever.

For two production boxes that i run using openvz (the other one hosts 40+ domains) i'm pretty happy on how the software performs and how secure it is.

I'm running openvz on the 40+ domains box from last years spring and i didn't had any break-in's on the HN itself. That tells me that the kernel is secure enough to not allow a compromised VE access to the HN. I had compromised VE's but mostly kids vandalizing sites because they were poorly written.

On that production box i'm running the VE's with public ip's but the incidents were only related to php applications that were not sanitized properly and after the developers fixed the problems saw by me i stopped having problems with that too.

It's your choice on how paranoid you want to be with security and if you have sensitive data your handling it's normal to be that way but if you're only a web hoster i think it's to much of a hassle to do this setup your trying to do.