

BYOD in a Dutch school community

How one school focussed on applications, not devices, to provide safe remote access

Undeniably, *Bring Your Own Device (BYOD)* has become a topic that cannot be ignored by companies, organisations and IT departments. But for Clemens Broekroelofs, Head of ICT at Greijdanus College, the challenge is not “How can we control BYOD”, but instead “How can we make BYOD safer and protect our information.” He feels that attempting to control devices is not the solution. Instead, he says, it’s important to control the applications



Clemens Broekroelofs , Head of ICT Greijdanus College, first presented this case at the BELTUG X-change on taking control of your BYOD, 24 April 2011

CHALLENGES

Home access to online program for teachers

The Greijdanus secondary school has four campuses in the northern region of the Netherlands. Its 450 staff, including teachers, presides over a student body of some 3,500. The school has long been committed to using ICT to facilitate its role, introducing VoIP in 2001, a multimedia system in 2004 – before YouTube, comments Clemens --, remote access to the network since 2008, and more. This remote access was set up primarily to allow teachers to upload student grade information onto the online program used nationally, from their homes. “Teachers’ work hours extend well beyond the school hours,” says Clemens “They do a lot of work at home, and management wanted them to have remote access from their own PCs.”

There were clear challenges: poor security from the available solutions, no control over the users’ PCs, potential infrastructure costs, demands for more remote access applications and uncertainty about the future. The school found a virtual access solution that fit the bill, and was implemented in 2008. But the environment evolved dramatically in a short time. In particular, teachers were switching from fixed PCs to laptops, while changes in regulations required the main administrative application to go into the cloud. These meant new security challenges that had to be addressed.

"You can't ignore BYOD, or pretend it doesn't exist: it's here already. But I don't want to manage laptops or smartphone; I just want to take care of our applications."

Clemens Broekroelofs, Head of ICT Greijdanus College



Greijdanus College is a secondary school in the north of the Netherlands. It has four campuses, in Meppel, Hardenberg, Zwolle and Enschede. It provides a complete educational experience for some 3,500 students between the ages of 12 and 18.

Among its 450 employees are 6 IT staff members. They oversee an ICT infrastructure including VoIP, centralised printing distribution, a multimedia system, centralised and virtualised IT, remote access for all employees, WiFi on all 4 campuses, VLE/e-Learning and a student-and-parent web portal.

SOLUTIONS

A 'hostile' WiFi and 'private' cloud

"We began offering WiFi on all our campuses by 2009," explains Clemens "We set it up so that the wireless is seen as 'hostile' by the network. To allow BYOD to access the virtual access network, our staff must use their authentication-token USB keys. This means they can switch devices as they choose, without impacting security."

The cloud issue required a more complex solution. "We have some 3,500 potential hackers on our campuses alone. We're not a bank, but we do deal with very sensitive information that must be protected. With the cloud, your online student grade tool is not very secure." His solution was to build a VPN tunnel, which provides the only access to the school's online grade tool. "This in a way made the cloud 'private'. Users must first connect to the school network, and then to the program."

While most users don't notice a difference, as they automatically go through the virtual access network, he admits that some don't like the extra step required. "They don't see why they can't just log on directly to the online student grade tool, the way teachers at other schools do. But to me it's a basic question of security."

LESSONS LEARNT

Keep it Safe and Simple—and don't bother fighting reality

Clemens is resolute that BYOD has been an important advantage for schools, which don't have the budget to provide staff with 'approved' hardware. But he has no interest in trying to control the devices: "It's their device; I can't and don't want to control it. I focus on the applications. If you only have email and smartphones to deal with, maybe it is effective to control the devices. But I have multiple apps on a variety of devices. I can't possibly manage all those devices!"

But he is also clear that, having made this choice, it is critical to manage the security of the applications. "Security and simplicity: that's my motto. Stop trying to pretend BYOD doesn't exist or that you can stop it somehow. Instead, look at how to make it work for you, safely."

He also comments that using the virtual access solution means the supplier has to worry about extending the solution to new devices like tablets and smartphones. "They continue to release versions that include new devices, so I don't have to deal with that."