CloudPro
Driving your business transformation

Mount10 CEO Q&A: inside the doomsday-proof datacentre

If Blofeld had a datacentre, this would be it.

Imagine a secure complex, sat underneath a mountain, protected against biological attacks, and complete with its own private underground lake.

It might sound like the setting for SPECTRE but, in reality, it's a hyper-secure data storage facility operated by Mount10. We sat down with CEO Thomas Liechti, who told us what it's like running a datacentre that would make a Bond villain jealous.

Thomas, tell us a little about your company, and what makes it unique.

We've been on the market for roughly 10 years. We're known for our two datacentres in the mountains. But I think customers buy us mainly because we do offer a vigorously proactive service.

That means that we're not waiting until a customer realises something isn't working any more, whether it's backup... or disaster recovery services. We call them up and make them aware that something is not right, and advice that they should probably fix it. And then we help them do that - which is all included in the service package - until it works again.

We operate two underground datacentres: Swiss Fort Knox One and Swiss Fort Knox Two. Swiss Fort Knox One is still in military possession and we rent it. We aren't allowed to tell you exactly where it is, but it's somewhere in the Bernese Alps.

Swiss Fort Knox Two, which belongs to us, is also in the Bernese Alps about 12 kilometres away from Swiss Fort Knox One. Why do we have two datacentres? We always have the data stored in two places. I'm not willing to bet the customer's data on just one rate controller. That's why we copy it, as well as geographically separating it.

What physical security do you use at your datacentres?

Swiss Fort Knox One is still looked after by military personnel, and for Swiss Fort Knox Two, we're working with a third party company. That's done on purpose, because if we control everything, we are the weakest link in the chain. So that's why we work with a large Swiss security company, which is actually provides the physical protection of Swiss Fort Knox Two.

What about cyber security? Do you partner with security firms?

We partner with a couple of external companies, but I'm not going to disclose what kind of companies they are. But we do regular ethical hacking tests for ourselves, and we work with different companies to improve our security as well, from year to year.

Why are you emphasising physical security, when many people would say that more threats come from online?

I think you should be able to withstand every single threat there is. It's - hopefully - not very likely that we face an EMP pulse or face a biological attack, even though we would also be protected there.

In commercial-oriented datacentres, if you have, say, a selfie stick and you can walk in there, you can go through the grill and switch off a server, or manipulate the server of one of the other customers. I don't think you're willing to pay for that kind of security, so we're just not doing any compromises.

What do you think are the biggest physical threats facing customer data?

I think incorrect manipulation is still the biggest physical threat, which is done by the customer itself.

Besides that, I think you can never be sure that sabotage is not taking place. I'm not thinking about military actions here, but sabotage is… well, it's present.

What are the main drivers of increased uptakes of physical security?

Interestingly enough, yesterday evening I had an interesting conversation with two Veeam customers. They were asking me more or less the same questions, but at the same time, answering them, because they both had stories.

One was actually at 9/11. He had a couple of datacentres around the country, but at that time, nothing worked any more. He said that even though he had SLAs in place, there were overwhelming priorities that day - which I understand - where the authorities went in and switched off his power, even though he had a guarantee that the power was never going to be switched off. But it just happened, due to the fact that control over the cooling, power, and communication, was not in his hand.

That's what we provide out of one hand. You can call us up, we own and operate the generators, we own and operate the communications infrastructure, we own and operate our own cooling. At Swiss Fort Knox Two, we have a lake under the mountain for cooling purposes.

Obviously, that's proof against any attack from the outside, because it's drilled from inside the mountain. And we have seven degree Celsius-cooled water to cool the datacentres, so we have a very green edge as well.

The other customer had a story from a datacentre in Houston, Texas that was flooded. So, I think you can never be sure of just what can happen. Is there 100 per cent safety? No, there is not. But I think we can provide the maximum amount of security, which you can also pay for - we're not hugely expensive.

Does being based in Switzerland provide any benefit regarding the stricter data protection regulations in Europe?

I think we provide not just the best data loss protection throughout Europe, or throughout the world, but it's also mainly the political stability which counts for safety and security of this data.

This data is encrypted anyway. As soon as it leaves the customer's premises, it's encrypted. There's no way for me, or for us, to decrypt it. So we're more concerned about providing a perfect service, and making sure that the service runs well.

The content of the data, if that customer is forced to hand it out, is beyond my control. And we have been forced by the Swiss authorities, by court law, twice in our history to provide data.

Obviously, we just provided it encrypted, and so the court then had to find a way with the customer, who had the decryption key, to actually decrypt it. We couldn't do anything.

How does Mount10 use Veeam?

Our company grew on a file-level backup service. It was a beautiful, scalable service. Having said that, it forced the customer into deciding what kind of data was important and what was not.

We've been working with a lot of customers and asking them what kind of solutions they are using and what they would like us to use. And they clearly told us Veeam.

They use Veeam, and we started to work with Veeam. We had just the right timing, I think, because in [Veeam Availability Suite] version 8, the Cloud Connect functionality was being built in.

Originally, service provider capability - on the Cloud Connect side - to be able to force encryption was not planned.

So if a customer tries to push unencrypted data into our mountain, he'll get an error message back from Veeam, saying 'well, sorry, the service provider does only accept encrypted data.' That helped us massively.

We launched on 1 June it and it's been going really well.