What if your Mission Critical Equipment is spying on your Data Center

Surprised? Shocked? Sceptical? Well probably all of these. But the possibility of your DC equipment being able to broadcast essential data without your knowledge is real and simple to implement.

While most DC operators will take elaborate care to screen visitors, employees and contractors, they almost never screen equipment that is being purchased for their DC.

The advances in recent years in mobile telephony, especially with the eSIM, makes data transmission from your DC to an outside, and most probably, an unauthorised recipient, a simple matter.

Firstly, what is an eSIM? The acronym says it all. Its an electronic sim. Very different to the sim chip that we have been used to seeing in our mobile phones. It's a tiny circuit that can turn anything into a mobile phone or more importantly a mobile data transmitting device that is almost impossible to detect. So tiny it can fit into an iWatch.

Not just physically different to a regular SIMM chip, the eSIM is functionally different too. It is programmable, never needs to be changed, can be manipulated or pre programmed with several mobile numbers and carriers. Can even be re-programmed by an outside source once they are connected to the device.

So, what has an eSIM got to do with my Data Center you ask?

Embedding an eSIM circuit into your equipment at some point is not rocket science. Power is all that is needed to get the eSIM working.

Next is connecting the eSIM to data outputs in your equipment. This can be to the Multi Meter or the Power Quality Meter in your equipment, say for example, in an UPS.

The data required to tell the outside world what your Racks and servers are doing is power consumption, power demand patterns, then add anything else to this list. The multi meter will give you most of this, and the PQM will gather enough data to fill up volumes. Even your cooling is not immune to data eaves dropping. Temperature, run hours, Humidity, Air volume and velocity are common data that is collected and sent to the BMS. This can be tapped and sent to a data logger that then transmit the data via the eSIM to an unauthorised data snooper.

Data can be sent off to a recipient or computer system and never detected. The eSIM can lie dormant and not transmit any signals until a pre-set time. Or better still, the eSIM could receive and accept a dialled in call, then start to transmit data from the data logger.

No amount of scanning or electronic detection will be able to pick up the eSIM doing its work. It could be active for a few seconds a week or month, transmit the data on demand or as programmed, then go dormant.

There could be several ways to block the mobile data transmission.

The simplest is to install a GSM jammer. Technically illegal to own or use in most countries. This will not only block the unauthorised mobile data transmission, it will also prevent people working in the DC from using their phones and tablets when within the DMZ.

The other is to have a Faraday Cage surrounding the rooms where sensitive Mission Critical equipment is installed. (Faraday Cages are often mandatory in Military or Government DCs to prevent radio wave bombardment).

The Faraday cage comes in many forms. The easiest is an aluminium or copper foil which is earthed or ground. The more complex is to have the metal foil installed between the walls – again a perfect grounding is essential or the Faraday cage may not be effective.

The other way is to select your equipment carefully. Choose who supplies you with what, their reputation in general, are they on a black list in other industries, what other industries are they active in and are they coming in very much below the market price.

A microscopic examination of each of the components, controllers, pc boards etc. during the Factory Witness test is another way. But can you tell what an eSIM circuit will look like? It can be in many forms. Even totally integrated into a common-or-garden controller card.

Imtiaz Issadeen – Tokyo.