Attack surface

With the utilities sector becoming increasingly dependent on broadband technology, Land Mobile talks to industry and cybersecurity experts about how to manage potential vulnerabilities

During its ongoing invasion of Ukraine, the Russian state has deployed numerous different tactics to try to drive its western neighbour into submission.

This has obviously included the military invasion itself, and the cruelty and loss of life associated with it. There has also been a concerted effort on the part of the Russian regime to disable Ukrainian critical national infrastructure, for instance via physical attacks on power facilities across the country.

One other, perhaps lesser known, strategy, however, has been the use of cyberattacks, which likewise have been utilised in an attempt to sow disruption. The earliest of these in relation to the present conflict were known to have occurred at the beginning of 2022, when multiple Ukraine government and banking websites were taken down by a hostile actor.

While Russian cyber activity has been primarily centred on Ukraine itself, however, the latter's western allies have also been targeted. For instance, the UK National Cyber Security Centre (NCSC) reported that Russia was "almost certainly" responsible for an attack on satellite internet company Viasat, again, towards the beginning of 2022.

To quote the NCSC's statement at the time: "Although the primary target is believed to have been the Ukrainian military, other customers were [affected], including personal and commercial internet users. Wind farms in central Europe and internet users were also [affected]."

As well as the safety and security of Ukraine, then, it is clear that threats also exist in relation to wider European stability and prosperity, particularly around the communications and energy piece. (As readers will remember, one Russian tactic in the early part of the war was to cut off its supply of gas to the continent, thereby occasioning a shortage and attendant price hike).

Regarding the latter, the situation is made doubly urgent by the fact that the energy sector is becoming increasingly reliant on broadband technology in every aspect. And as anyone who works in this field will tell you, the greater the number of connections, the larger the potential 'attack surface'.

Complex decarbonisation

Before attempting to explore the topic of 'energy' as it relates to cybersecurity, it is first necessary to give some sense of the industry's ongoing evolution when it comes to communications tech. As indicated earlier, it is no longer simply a matter of deploying two-way radio on the ground, with narrowband-based SCADA being used to monitor the network.

Offering an overview of the changes currently taking place, secretary-general at the Utilities Telecom Council, Julian Stafford, says: "The situation in Ukraine has come at exactly the same time as we're trying to decarbonise the energy sector. That means moving away from very large thermal generating stations towards more distributed generation.

"Europe and the UK have got some of the most ambitious targets in the world when it comes to de-carbonisation, for instance around electric transport. We're also fortunate enough to have lots of natural resources which make it relatively easy to build the infrastructure to harness solar, tidal, wind and so on."

While this ambition to 'decarbonise' is clearly positive, according to Stafford the move towards distributed generation will require increasingly sophisticated ways to monitor the network itself. The situation is made even more complex, meanwhile, with the anticipated drastic increase in the amount of power likely to be required to accommodate innovations such as electric cars.

He continues: "Because of the way the grid is changing, there is this increasing requirement for real-time, high-precision monitoring of data. This is also coming at the same time as we're losing some of our existing tools, for instance with the 2G and 3G switch-off, while also taking into account things like the NIS 2 [EU cybersecurity] directive."

"There is an increasing requirement for real-time, high-precision monitoring of data"

Also on the call with Stafford is utilities industry expert (and managing partner at Ledgewood Associates) Adrian Grilli. Delving deeper into the new technology itself, particularly as it relates to the security piece, Grilli does indeed believe that increased connectivity will likewise "massively increase the threat surface".

This, he says, is because "it provides far more points from which you can launch an attack, either by compromising physical devices or trying to get into the comms themselves. Our society is much more dependent on electricity than it used to be, so we're far more vulnerable.

"Most homes couldn't survive without electricity at this point. And turning off the public switch telephone network means that we won't have resilient fixed communications either."

As Grilli regretfully indicates, these are all things which are well known to potential attackers, whether independently operating cyber criminals or those working on behalf of some kind of hostile actor. "As has been demonstrated in Ukraine," he says, "the way an economy is taken down is by the destruction of its electricity infrastructure."

Systemic vulnerabilities

In December 2015, two electrical power grids situated in the western part of Ukraine were hacked. The attack – which affected over 200,000 people – was eventually attributed to a Russia-affiliated group known as Sandworm.

According to contemporary accounts, the hack took place via the use of malware given the name BlackEnergy 3. This 'remotely compromised' the IT systems of several Ukraine energy distribution companies, with the attack ultimately taking place over several stages (including taking control of SCADA systems, in order to temporarily switch off substations).

Quoting a variety of sources, a well-known online encyclopaedia relates speculation that the systems in question may have contained vulnerabilities, which rendered them as a "special case". These included both their age and what might be referred to as their provenance, with the grids having originally been built when Ukraine was still part of the Soviet Union. The systems were also apparently subsequently upgraded with Russian parts in the intervening years.

The 2015 attack is instructive for any number of reasons, not least that it illustrates the chaos which can be occasioned through the infiltration of complex, multi-layered technological ecosystems. Just as interesting, however, is what the incident teaches us about the basics of cybersecurity, particularly when it comes to the provision of energy.

Dr Greig Paul is the lead on mobile networks, and a security engineer at the University of Strathclyde.

He is also the deputy chair of the UK Telecoms Data Taskforce/UK 5G Security Group.

Asked what the biggest issue is when it comes to the sector, he is unequivocal in his response: legacy communication systems. "If you look at the estate in systems that provide power, they were predominantly built decades ago, having been designed in an era of electro-mechanical switching," he says.

"Plus, they were designed to last for decades. Fifty or 60 years would not be unheard of, during which time you'd carry out checks every few years."

He continues: "What this essentially means is that we've almost sleep-walked into a world where, in order to meet

our priorities, we're going to see a lot more demand on the network. That being the case, we'll need to understand what's going on in those networks in much greater detail."

This, he says, is "where things get interesting", with internet-connected technology now having to operate in tandem with legacy – often analogue-based – control and telemetry systems. Naturally, he says, the latter "were never designed to be secure", because at the time the systems were installed, the threat landscape was different.

"We then counter that with electric vehicle chargers, which are hooked into the internet, like IoT devices," he says. "The chip which goes inside your mobile phone is essentially the same as one which goes into any connected device linked to the electricity system. People typically replace their phone fairly regularly. The same isn't true for these connected devices."

The way Paul describes it, there are both positives and negatives when it comes to the use of legacy communications equipment in the generation and distribution of electricity. The key negative, as already touched upon, are the apparent vulnerabilities existing within that equipment in and of themselves. Plus, as he says, the older a piece of equipment is, "the less likely it is to have been patched".

"Legacy systems were designed to last decades. Fifty or 60 years would not be unheard of"

Adobe Stock/sutthichai

On the other hand, the older something is, chances are it "might not actually be connected to many things". Paul illustrates this via mention of a hypothetical "'80s-type protection relay" sitting within its own separate and dedicated circuit without an internet connection.

This last point leads neatly into Paul's observations about how the industry can help to keep itself safe from cyberattack. The first of these is that security should always be considered at a technical level at the point of procurement, not after the fact.

This, he says, shouldn't just be in relation to the product itself but also how it is architected and installed. "Where things become a challenge is when procurement processes are not led by a technical review. So, you can buy something and as long as it claims to be secure, it can be purchased.

"Everyone has to be accountable at every point in the purchase and installation chain, including suppliers."

He continues: "The other thing you need to do when you buy things is layer in security, including concepts such as 'zero trust'. The system should never be just one failure away from going wrong, something which is known as the 'Swiss cheese' model.

"With this, the attacks will still come in, but the system would be able to create a 'blast zone' so that the 'explosion' happens at the outside in the little trench we've dug. One practical way of doing this is to physically prevent any laptop that connects to the operational network from being able to talk to the internet. It's not a complicated concept."

We live in the most electricity dependent society in history. As our needs become increasingly advanced, so will the methods required to keep both society and business safe.

Find out more about the work of EUTC at www.eutc.org.