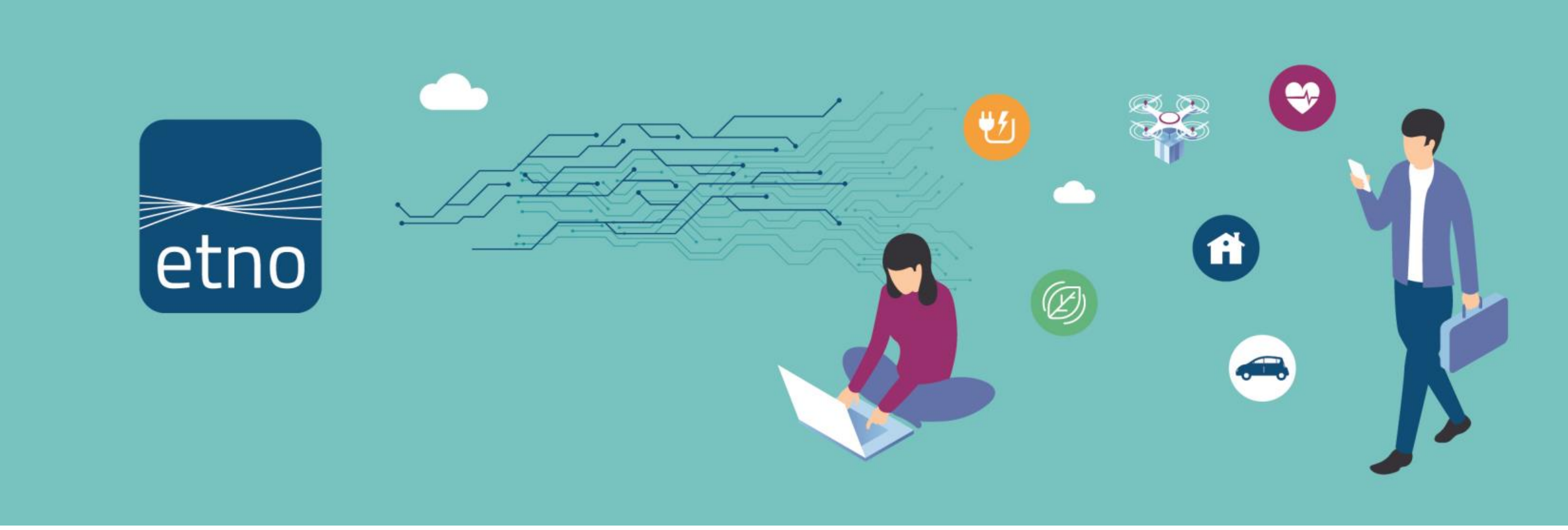

March 2021

Supply chain accountability: a priority for Europe’s cybersecurity policy

By Paolo Grassia, Director of Policy Affairs, ETNO

It is not an understatement to say that the SolarWinds hack is, in Microsoft President Brad Smith’s words, “the largest and most sophisticated attack the world has ever seen”. At least 18.000 customers of software company SolarWinds were affected by a backdoor that allowed state-sponsored hackers to compromise U.S. government agencies, leading technology firms, and other notable targets worldwide. The full extent of the hacking campaign is still being investigated, and its consequences are still unravelling.

What is clear though is that the SolarWinds cyber-attack has been first and foremost a supply chain security failure. Hackers injected malware into updates of SolarWinds’ Orion IT monitoring and management tool, which is used by over 30.000 clients from the public and private sectors around the world. The supply chain backdoor remained undetected for several months, until the breach was finally revealed by Microsoft and security firm FireEye in December 2020. However, the cyberattack is still ongoing as hackers continue exploiting vulnerabilities in the Orion technology.

Why supply chains matter, also in 5G

Over the past 20 years, supply chains have become ever more globalised and complex, entailing intricate networks of partners with strong interdependencies. Growing complexity can blur the lines between the roles and responsibilities of different parties, raise issues of information asymmetry and lack of communication, and thus increase risks and vulnerabilities along the supply chain. This evolution and its effects are particularly acute in global ICT supply chains. The reason is that they involve a sophisticated and partly intangible ecosystem of hardware, software, components, IT and data systems, and real-time remote services.

The telecommunication sector is preparing for major changes in its supply chain landscape. With the advent of 5G, operators are going to deploy a virtualised and software-defined infrastructure that will enable edge computing and network slicing. The telecom networks and services of tomorrow will be delivered by an environment of operators, vendors, and managed service providers, where more functions will move closer to the user and will be outsourced to suppliers. Already today, a third of telecom security incidents in Europe are third-party failures, such as hardware malfunctions and software bugs (see ENISA's Incidents Report). The deeper interdependence of providers and third parties in the 5G architecture will expand the attack surface of the network.

How legislation can help secure 5G

The SolarWinds attack has taught us that a vulnerability in a small piece of a global supply chain can stay under the radar for a long time, as a drop in the ocean, until it has endangered the whole chain. Risk management in the supply chain has therefore become a defining issue for the ICT industry and other sectors that are the top targets for cyber-attacks, like healthcare, energy, banking, education, and government.

On the same days as the SolarWinds hack was discovered, the European Commission unveiled a new Cybersecurity Strategy to strengthen the EU's preparedness against cyber threats, along with regulatory proposals to address cyber and physical resilience of critical entities and networks. A Directive on measures for high common level of cybersecurity across the Union – which repeals the existing Directive on the security of network and information systems (NIS Directive) – aims to step up the cyber resilience of several crucial sectors like digital infrastructure, transport, banking, healthcare, utilities, and public administration. The so-called 'NIS2' Directive introduces a risk-management approach, providing a list of basic security requirements and incident reporting obligations that must be applied by entities in those sectors across the EU.

The proposal puts emphasis on supply chain risk management, demanding that the regulated entities assess the quality and the cybersecurity practices of their suppliers and service providers, especially big data companies and managed service providers, during their continued business relationship. EU governments will play their part by adopting national policies on supply chain cybersecurity for ICT products and services. Furthermore, EU states, the Commission, and the EU cybersecurity agency ENISA can develop joint risk assessments of critical supply chains, to chart the threats of the key ICT services, systems and products used in each sector. Finally, European CSIRTs should facilitate coordinated vulnerability disclosure procedures, to improve information sharing between reporting entities and ICT vendors.

NIS Directive: going to the root of the problem

All these measures mark a step in the right direction of bringing supply chain relationships under increased scrutiny to increase business transparency and accountability. However, the proposal fails to tackle the issue at its core: those closest to the problem are closest to the solution. In the face of ever-expanding supply chains that can make cybersecurity like finding a needle in a haystack, critical entities will still shoulder the lion's share of ensuring end-to-end resilient networks and services, and of proving supplier compliance. A better allocation of responsibility for risk management along the supply chain will make the endeavour more successful.

Providers of ICT products and services that become an integral part of the critical services delivered to end-users are often best placed to manage their own vulnerabilities, and thus to address cyber threats in the first place. If the NIS2 introduced risk-management and reporting obligations directly applicable to crucial ICT suppliers through the entire product or service lifecycle, the overall resilience of critical sectors in Europe would greatly benefit.

The legislative process of NIS2 has only just begun; it is not too late to remedy its shortcomings. It may not prevent the next SolarWinds hack, but it will adapt EU's cybersecurity policy to the 21st century supply chain.