Article

Oct 2022

Cyber Security for Critical National Infrastructure

Recent high-profile attacks on critical national infrastructure (CNI), such as Colonial Pipeline in 2020 and the Irish National Health Service in 2021, have underscored the serious threats posed by, and potential consequences of, cyberattacks on CNI. These attacks can have a far-reaching, real-world impact on people's lives, disrupting critical services such as healthcare, emergency services and fuel supply.

Max Muir
Information Security Consultant
Email max.muir@waterstons.com

Operators of CNI not only have to deal with the well-documented cybercriminal threat facing organisations in the UK, but also sophisticated attacks from state-sponsored criminals and nation states.

This risk has continued to grow in recent months following the outbreak of war in Ukraine which has prompted the National Cyber Security Centre (NCSC) to issue repeated warnings of the risk posed by potential state-sponsored cyberattacks targeting CNI in the UK.

In August alone two CNI operators in the UK – the NHS and South Staffordshire Water – were hit by cyberattacks, with threat actors causing disruption to the NHS 111 service and compromising the critical SCADA systems that control water chemical levels.

Proposed changes to the NIS regulations

Due to the threat landscape, the UK government is looking to expand its regulatory powers via sweeping updates to the NIS regulations which set out the cyber security requirements for CNI.

The proposed changes would greatly expand the scope of the NIS regulations to potentially include new sectors as well as the supply chains and critical dependencies of CNI operators, drawing far more UK businesses into the scope of the regulations.

The most important potential changes to the NIS regulations are:

1. **More agile changes to the regulations in future**

NIS regulations require an act of Parliament to make any changes, making them slow to react to the fast-changing cyber threat landscape, instead these changes remove that need for some changed, potentially leading to more frequent updates.

2. **NIS regulations expanding to include new sectors**

In recognition of the serious threat posed, the government is proposing to expand the scope of the NIS regulations to cover new sectors not currently be considered CNI but that play an important role in the UK economy.

As the scope of the NIS regulations expand, organisations in newly covered sectors (for example, education, construction and manufacturing) will need to ensure they can certify against the cyber assessment framework (CAF) – a requirement of the regulations.

3. **NIS regulations expanding to include critical dependencies of CNI operators**

While CNI operators are required to ensure the security of their suppliers under the current NIS regulations, the proposed changes would expand the scope to require critical dependencies of CNI operators to also adhere to the NIS regulations.

Why are supply chains a risk?

Over the past few years, supply chain cyber security has become a major risk for UK businesses with attacks increasing by 51% over the second half of 2021. However, only 13% of UK organisations are currently assessing the risk posed by their immediate suppliers.

For CNI, supply chain attacks are often utilised by sophisticated threat actors who can bypass an organisation's cyber security controls by targeting the weakest link. In the current threat landscape, an organisation can only be considered as secure as its least secure supplier.

What is the threat?

Some of the most common ways threat actors will exploit supply chains include

- Compromising a supplier's email or website and then exploit the trusted relationship by launching a targeted phishing campaign – see the 2021 attacks on Florida's water utilities
- Inserting malware or vulnerabilities into a supplier's software or firmware update, infecting their downstream users – see the 2020 Solar Winds attack
- Inserting malicious code into open-source software which propagates downstream to its users – see the 2018 Event-stream attack

The risk of a severe supply chain attack on CNI is further compounded by a relatively small pool of suppliers for specialist functions. A supplier servicing multiple CNI operators can quickly become a critical dependency for the entire sector, and therefore an attractive target for state-sponsored attackers.

It is not enough for an organisation to assess its supply chain's cyber security as not all suppliers are equal. Organisations should also establish the level of risk each individual supplier poses and adjust the security requirements accordingly, employing a risk-based supplier assurance process. This information can also help inform business continuity and incident response plans in the event of a supply chain attack.

In CNI, some OEMs require access to usage data of their equipment to monitor the lifespan and performance of existing equipment and improve future products. While there is no issue with this type of data sharing on its own, there is a tendency to provide real-time access to this data, creating a permanent access point, and therefore vulnerability, in the network.

This access is sometimes not monitored by the CNI operator due to the trusted relationship with the OEM, creating a significant gap in their cyber defences. These agreements often occur early in procurement when cyber security is not considered, and it can be very difficult to renegotiate the contracts after the fact.

How can Waterstons help?

Whether you are a CNI operator regulated by the NIS regulations, a supplier to CNI or within a sector the NIS regulations may be expanding into, you will need to be aware of your changing obligations under the proposed updates, as well as have the capacity to identify and address the cyber threats facing your organisation and supply chain.

Waterstons cyber consultants are experienced in working with CNI in the UK and helping organisations certify against the CAF, get in touch today to see how they can support you by emailing cyber@waterstons.com

View our cyber security services.