NIS

Cyber Security and the Supply Chain

Gemserv

CYBER SECURITY AND THE SUPPLY CHAIN

For tens of thousands of people, the last weekend in May 2017 proved to be one they'd rather forget. A power failure at a British Airways data centre led to more than 650 flights being cancelled and chaos at many airports.

The incident was a timely example of the kind of disruption to essential services which the recently implemented Network and Information Systems (NIS) Regulation aims to reduce the risk of.

Although the Operators of Essential Services (OES) which fall under the wide-ranging regulations are still in the process of being identified by the sector-specific Competent Authorities (the regulators of the NIS), it is clear from the published thresholds that British Airways is one and that an incident such as last May's would need to be reported given the level of disruption caused.

The British Airways incident occurred well before the NIS came into force, but it highlights the extent to which major businesses are now dependent on supply chains and how effective risk management of third parties will increasingly be a key issue for organisations.

UNDERSTANDING THE RISKS

Minimising the impact of incidents - whether from cyber-attacks, power cuts or hardware failure - is a key objective of the NIS Regulation. Understanding and managing the security risks to networks and information systems from dependencies on external suppliers is an important part of that.

In the modern business environment, third party suppliers are involved at every level of organisations, from IT managed services, cloud or data centre infrastructure through to security staff, call agents and contract engineers.

As British Airways itself pointed out in the wake of the power failure[1], "IT services are now provided globally by a range of suppliers and this is very common practice across all industries".

Suppliers and contractors who have access to an organisation's critical service, especially privileged access, need to be identified and actively managed. Those with malicious intent will look to exploit the easiest route to achieve their goals and, in many cases, that will be suppliers with less stringent security policies and procedures in place.

A lack of transparency over security management is one indicator that suppliers are not proactively managing their risks. If suppliers are not open about their security management, then organisations should be questioning whether they should be using them. The National Cyber Security Centre (NCSC)[2] itself has recently highlighted how it selected cloud providers by avoiding those suppliers who are not open about their security practices.

[1] https://www.ft.com/content/15cab698-4372-11e7-8519-9f94ee97d996
[2] https://www.ncsc.gov.uk/blog-post/ncsc-it-how-ncsc-chose-its-cloud-services

4

IDENTIFYING WHAT IS IN SCOPE

Ultimately an OES is accountable for the security of the whole service including those elements managed by third parties. An OES is required to ensure its suppliers have suitable and relevant security measures in place to manage identified risks of disruption to the essential service and, as such, all requirements from the NIS Regulation flow down through the supply chain.

Identifying what is in scope for an essential service is a necessary first step to risk assessment. One approach for a risk assessment is to take a holistic view of the service from a system-driven[3] perspective, as well as at the system component level, where appropriate. This involves identifying suppliers, understanding what essential systems and information they will be responsible for and its sensitivity, and analysing risks which are integral to the service.

For some organisations, the steps taken to ensure General Data Protection Regulation (GDPR) compliance may have already identified suppliers and information they hold which can be included in the self-assessment for NIS.

RISK REDUCTION METHODS

Each supplier identified as part of the essential service will have risks. Many will be related to technical vulnerabilities and a large number will be around the people, policies and processes.

The method of reducing the risks will vary and may include selecting suppliers based on:

- Recognised certification like ISO 27001 for an Information Security Management System;
- Background checks on supplier staff using BS7858;
- Technical assurance from yearly penetration tests along with regular supplier audits; or
- Signed contracts applicable to the service they are providing.

If selecting a supplier based on a recognised certification like ISO 27001 or ISO 22301 (Business Continuity), it is important to ensure the scope of the certification covers the controls which form part of the essential service, and to check they are not certified just for their operations centre which may only cover part of the service. In addition, it is important to ensure that the procurement process checks that the certificate has been issued by a United Kingdom Accreditation Service (UKAS) accredited Certification Body. This gives assurance that the supplier goes through appropriate and regular onsite audits, carried out by an independent third party accredited body to conduct these audits against the applicable standard.

No matter what controls are put in place to reduce risk, communication with the supply chain is essential. If any party in the chain has an incident, rather than worrying about the implications of potential fines, the first step is to communicate it with the guidance of a pre-tested communications plan. Protecting critical national infrastructure should be paramount; a view shared by the NCSC[4], which believes there is currently an under-reporting of incidents. The sooner information about a potential incident is communicated, the quicker it can be understood and brought under control. Attacks[5] are getting more sophisticated and one of the ways to defend against that is to share what is happening.

Companies within the energy sector who need to comply with the Smart Energy Code have contractual agreements in place with the manufacturers of hardware and developers of software in the supply chain of any smart metering system. They must notify as soon as they become aware of any security vulnerability with enough detail for the energy company to notify the Security Sub-Committee of the steps being taken to ensure the cause of the material adverse effect is rectified and by when. If the energy user is also an OES, they will also need to notify their Competent Authority and the NCSC within 72 hours.

Technical vulnerabilities are an issue for organisations with critical national infrastructure, especially those with industrial control systems (ICS), and operational technology (OT). Due to their lifecycle of 10 to 15 years, some of these systems were not built with security in mind. Stuxnet[6] in 2010 was the first worm to propagate a network and infect ICS software and had a costly impact on Iran's nuclear fuel enrichment programme, and the expectation is that attacks on ICS will continue to increase. ICS equipment usually has no encryption and is highly vulnerable to denial of service attacks. The technical knowledge to maintain these systems is limited and often sub-contractors are needed to get machines back up and running, increasing the complexity of the supply chain.

[3] https://www.ncsc.gov.uk/guidance/introducing-component-driven-and-system-driven-risk-assessments
[4] https://www.ncsc.gov.uk/content/files/NCSC-2017-Annual-Review.pdf
[5] https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks
[6] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

6

IMPORTANCE OF AWARENESS

Awareness within the supply chain is something that benefits everyone and spotting that something is 'not quite right' is the first step to preventing a potential incident. Employee awareness within your own organisation should be continuously promoted, but encouraging suppliers to do the same is also important. The Centre for the Protection of National Infrastructure (CPNI) has developed a number of security awareness campaigns[7] which have been designed to provide organisations with extensive training material, but it still requires effort to implement it. This includes proactive promotion from the board and demonstrating this through leadership and commitment to an information security management system as per ISO 27001.

The supply chain is complex and categorising suppliers into different risk profiles, criticality and sensitivity to an essential service is a good place to start. It is important to establish regular dialogue and reporting of security performance, have the 'right to audit' in applicable contracts and request your suppliers to do the same with their suppliers.

Organisations should also use suppliers who have Cyber Essentials Plus[8] and ISO 27001 certification with an accredited certification body as a minimum and seek additional security standards where it is justified for a particular service. Gemserv recommends utilising what the NCSC has to offer, including joining the Cyber Security Information Sharing Partnership (CiSP).
It's also important to remember that the NCSC should be contacted whenever an organisation or one of its suppliers has a suspected incident.

The NIS Regulations are there to protect critical national infrastructure, but also to preserve life.

[7] https://www.cpni.gov.uk/security-awareness-campaigns
[8] https://www.cyberessentials.ncsc.gov.uk/

Author

Jennie Cleal
Senior Information Security Consultant

Contact Us

To find out more about the NIS or about any of our services, get in touch with us at:

E: bd@gemserv.com
T: +44 (0)20 7090 1091
W: www.gemserv.com
@gemservinfosec

London Office
8 Fenchurch Place
London
EC3M 4AJ
Company Reg. No: 4419878

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 0039

ISO 9001 001

CYBER ESSENTIALS PLUS