Radiflow

Navigating the Waters of the New EU NIS 2016/1148 Cybersecurity Directive for Essential Service Operators

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER RESEARCH TEAM

Contents

Introduction 3

Scope of the directive and of this paper 3

Provisions of the directive 5

- Security assessment and risk management 5
- Managing the operational impact of cyberattacks 5
- Information sharing 6
- The human factor 6

Implementation of the directive 6

- Security assessment 6
- Solution Concept 7
- Industrial IDS (Intrusion Protection System) 7
- Industrial IPS (Intrusion Protection System) 9
- SOC (Security Operations Center) 9

Enforcement 11

Cross-reference 12

Conclusion 13

Introduction

The responsibility of top management, both personal- and organizational-wise, for the safe and reliable operation of critical infrastructures, is essential for national security and organizational success.

The EU took an active step to ensure this in the NIS directive EU 2016/1148 (issued by the European parliament and of the council of July 6, 2016) which details the creation of a common high level of network and information system security across the EU. The directive took effect May 10, 2018.

By May 9, 2018 each member state was required to transpose this directive and issue national regulation appropriate for the specific situation, threats and risks of each country. Such bodies include for example the National Cyber Security Center (NCSC) in the UK or Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany.

The next milestone on the directive calendar is November 9, 2018, by which time member states are required to identify the relevant bodies that will be required to comply with the regulation and implement the relevant measures to protect their assets as per the NIS EU 2016/1148 directive.

Further implementation schedule is to be defined on a case-by-case basis, but clearly the first step prescribed is a security assessment process accompanied by the risk minimization mitigation plan.

Scope of the directive and of this paper

The new directive applies to two types of operators: essential services and digital services. This paper shall relate to the former only.

Furthermore, part of the directive has to do with government activities such as Computer Security Incident Response Teams (CSIRTs) which are also beyond the scope of this paper.

Regarding essential servers, Annex II of the directive defines the essential services operators subject to this directive. This includes:

- The energy sector (electricity, oil and gas)
- The transportation sector (air, water, ground and rail)
- Drinking water supply and distribution
- To some extent, the health sector

Member states have the option to alter this list and include additional areas such as building management, industrial plants, etc. They can add specificity, such as the NCSC defining drinking water operators serving 200,000 people or more; and separating rules for territories, such as making a distinction in the UK energy sector between England, Scotland and Wales with one set of rules, and Northern Ireland with another.

Section (19) of the Introduction chapter ensures that the criteria for identifying operators will apply equally to all member states on the union. As per Section (20) of the introduction and Section (2) of Article (5) the criteria are:

(a) An entity that provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) The provision of that service depends on network and information systems; and

(c) An incident will have had significant disruptive effects on the provision of that service.

Section (53) of the Introduction chapter details the fair and proportional enforcement of the rules in relation to the risks presented. It should also be noted, as per sections (9) and (10) of the same chapter, that specific regulations, which apply only to individual sectors, outweigh any general rule dictated by the directive. Therefore, in case a local to industry specific rule requires harsher measures to be takes they should obviously be followed.

Section (6) of the Introduction chapter enable operators to go beyond the minimal requirements and implement harsher measures as per top management considerations.

Provisions of the directive

Security assessment and risk management

Section (44) of the Introduction chapter and section (1) of Article (14) require the essential service operator to apply technical and organizational measures to manage and minimize risks and react to events.

Managing risk means both understanding the threats the organization faces and reacting appropriately when a risk materializes. The process should include an initial security assessment, toward mapping and modeling of all network assets, network topology, network flows and any additional information relevant. This information is subsequently used by the professionals performing the assessment to determine the vulnerabilities, exposures and threats the organization faces. Each finding is scored, weighted and prioritized by severity/importance. A mitigation plan is required for each finding, detailing the risk minimization, containment and recovery plan should the asset be attacked.

Managing the operational impact of cyberattacks

Section (2) of Article (14) specifies that in addition to the impact on network and data integrity, it is important also to understand the operational impact of a cyber event, since the two are typically uncorrelated.

While CERT (the US Computer Emergency Response Team, mandated with reducing systemic cyber-risks) is focused on preventing cyberattacks, operations professionals are concerned primarily with restoring reliable service upon attacks. In many cases these two functions are unrelated.

A useful method to bridge the divide is using a decision-support system, which uses a model of all networked physical OT assets (PLC, RTUs, etc.) in conjunction with the operational impact score for each asset. This enables assigning priorities for handling physical assets, considering the state of the attacked cyber-domain.

Information sharing

According to the directive, operators are requested to report and share information for the benefit of all operators (while protecting commercial information.) Sections (4) and (45) of the Introduction chapter and Section (3) of Article (14) further emphasize the need for promoting the culture and reporting of severe incidents.

The human factor

Section (1) of Article (7) of the directive also addresses the human factor as a decisive component of the protection system. It requires the essential service operator to regularly hold educational, training and drilling activities, as part of the broader organization-wide effort to reduce cyber-risk.

Implementation of the directive

Implementation is a complex and long processes. For a smooth start, a security assessment is the best beginning.

Security assessment

As mentioned above, the initial step in the process, before engaging in a complex cyber-security protection project is having a good plan. Performing a security assessment serves as the optimal path towards achieving this goal. By generating a prioritized mitigation plan protecting against the known exposures, vulnerabilities and risks discovered during the mapping and analysis phases, in view of threats model, one can launch the project with the highest certainty of success to reach the primary goal in an effective and efficient fashion.

The mitigation plan will include proposed action items in various fields. Industry best practices indicate a two-phase approach – detection and then protection. This methodology enables an initial conservative step that does not affect the network whatsoever and later take a more active protection course of action.

Ultimately, conducting a periodical recurring security assessment, for example every two years, will enable the operator to continuously review the situation and improve the cyber-security protection in the subsequent period. Based on achievements during the past program, changing threats model and latest technologies new adapted plans need to be devised.

Section (69) of the Introduction chapter and section (8) of article (4) define the need for a protection mechanism. Effective actual technological implementation of such a project would call for two types of solutions, which only if combined can provide effective and efficient protection: detection and prevention.

Solution Concept

Looking at parallel industry best-practices such as US ICS-CERT Defense-in-Depth, US NERC CIP ESP (Electronic Security Perimeter) access control, ISA99/IEC62443 security zones, Gartner guidelines for OT security and ISA Purdue model of control - the following model emerges. The main architecture guidelines are:

- Strict segregation should be enforced between the Enterprise level and the Manufacturing level using data diodes
- Central sites should have segregation between the Local HMI level and the manufacturing level in the Local HMI and Controller LAN levels also between individual locations as well as monitoring inside those levels
- Remote sites that typically contain Local HMI, Controller and Field I/O devices should access policy enforcement in the connection to the WAN
- Segregation should be implemented using industrial access gateways as defined below
- LAN monitoring should be implemented using an Industrial IDS as defined below
- All security alerts should be reported both to the Operations Control Center and to the SOC

Industrial IDS (Intrusion Protection System)

The IDS is a passive system that monitors network traffic in a truly non-intrusive manner. IDSs normally run on powerful servers and can provide a variety of sophisticated detection engines that analyze the traffic from different perspectives, thus increasing the chances of detecting a cyber event.

It is also important to mention that the IDS, being passive, cannot actively prevent an attack. This normally should not be of much concern, since as opposed to IT systems, the lateral movement of malware, and its activation time in the network, are generally very prolonged. Once malware is detected there is still ample time to act, since it can be assumed that the active attack is still far in the future.

It should also be stressed that the IDS used needs to be specialized for industrial systems as ICS/SCADA, and capable of performing DPI (Deep Packet Inspection) on relevant protocols such as Modbus, DNP3, IEC 101/104, etc. An IT IDS simply would not provide the required tool set.

In a typical IDS, network traffic collection is performed by connecting network Ethernet LAN switches mirroring ports (SPAN) directly to the IDS. A better preferred option is using multiple probes spread over the numerous remote sites that convey the collected traffic in a compressed and secured fashion to a central IDS for analysis with a wide network view and better cost-effective solution.

The probes option is suitable for cases such as substations, pumping stations, purification utilities and other organization with numerous sites spread all over. Due to the harsh condition in such location the probe should be ruggedized and with relevant compliance if needed for the specific industry.

Based on collected traffic a network map is built identifying the assets such as PLC, IED, RTU, HMI, engineering station, historian, etc. down to the details (vendor, part-number, hardware version, firmware version, etc.) and their network communication flows (IT and OT ones).

This provides the operator with a network wide visibility of the system. Devices are scored function of their cyber risk severity and alerts on known CVEs (Common Vulnerabilities and Exposures) are generated function of the discovered inventory of assets.

Alerts will be generated by DPI of SCADA protocols violations compared to the baseline established during the learning phase, exploitation of known vulnerabilities using a signature database for IT and OT sessions, sensible operations such as maintenance activity on industrial devices and more.

Industrial IPS (Intrusion Protection System)

The ISP secured gateway is an active inline device for real-time traffic inspection and, based on predefined rules, forwarding or discarding individual packets passing through it.

IPSs are typically devices that can perform active protection functions based on the DPI of industrial protocols. Such functions include serving as a SCADA firewall, secured remote access, industrial endpoint protection and more.

These specialized devices are proficient in the specific nature of industrial systems and obviously are very different than similar IT devices, such as firewalls.

IPS gateways, should be located between the WAN router and the LAN switches in remote sites or between the routers in central sites. Traffic should be encrypted if necessary using for example IPSec/DM-VPN AES256 encryption with X.509 certificates.

A major functionality required is DPI SCADA firewall blocking of illegal traffic forwarding legal packets and discarding the ones violating the rules. Deep understanding of protocols, specific vendors implementation and individual devices is necessary for a successful operation and protection.

For the critical technician access the gateway should restrict the maintenance session using multi-factor authentication, restricted time frame, task-based policies and recording of the session.

SOC (Security Operations Center)

All the information generated by the surveillance system is concentrated at the a SOC, most likely in a SIEM (Security Information and Event Management). SOC operators continuously monitor the normal operation of the system, and act in the event of a cyber-attack.

An SOC is normally manned 24x7 by at least two personas: a cyber expert and a substance matter expert. This translates into ten people on the payroll. The SOC can be incumbent, populated by the operator staff or can be outsourced to a managed SOC.

From the technology standpoint, the SOC includes a secured network with a set of cyber products such as IDS, SIEM, network diodes, whitening stations, firewall, etc. While these devices are OT-oriented, they are tightly aligned with the organization's IT network, since it's an integral part of the OT network and due to increasing convergence between IT and OT networks.

Reporting of alerts from the IDS to the SOC (typically the SIEM) can be achieved using IT protocols such as Syslog and SNMP, or using SCADA protocols such as DNP3 and Modbus and presented on the HMI. The second option provides important benefits: using a single monitoring system, the familiar and common HMI, for both operations and cyber surveillance, and maintaining the SCADA protocols as the unique communication means.

A managed SOC provides its services based on state-of-the-art products that provide professional and continuous cyber security monitoring and event management solutions to numerous customers.

The reality that the SOC serves multiple customers sharing the costs enables the SOC operator to employ the best products available in the market that would be out of reach for end customers in some cases. Customer traffic is analyzed by the IDS and generated events are handled by the SOC professional team.

In summary, a managed SOC is a cost effective and excellent solution for customers to gain from the superior products employed by the SOC together with the continuous professional service offered by the SOC operator. This option should be considered by essential service operator.

Enforcement

Article (15) details to the enforcement the directive. Section 2. (a) instructs essential service operators to present the regulator the security assessment document, as mentioned above.

Section 2. (b) requires proving the viability of the actual effective implementation plan. This can be achieved by conducting a second security assessment after some time had passed and showing that the overall score had been reduced thanks to the execution of the plan.

Section 3. of the same article allows the regulator to instruct the essential service operator to take additional specific steps to improve its protection. Operators failing to comply with national regulations are subject to measures set by the local law.

For example, in the UK the penalty for non-compliance is a fine. This measure is used only as a last resort, along the same line as for GDRP violations. The maximum fine the UK Competent Authority can impose can reach a total of £17M (!), however, such high fines are reserved for extreme cases.

Cross-reference

The following table summarizes the steps required to be taken for compliance with this directive:

#	Reference	Schedule	Responsible body	Action
1	Art 25-1	9-May-2018	Local government	Transpose the EU directive to a national regulation
2	Into-9, 10, 13, 19, 20, 53 Art 5-1, 2, 3	9-Nov-2018	Local government	Identify relevant bodies required to comply with the directive
3	Intro-27, 44 Art 7-1	National specific	Regulated body	Conduct a security assessment and compile a cyber security protection plan to mitigate the vulnerabilities and risks
4	Intro-61, 69	National specific	National regulatory body	Inspect and approve each body cyber security plan
5	Art 14-1, 2	National specific	Regulated body	Implement cyber security plan, detection and protection against intrusions
6	Art 15-1, 2, 3, 5 Art 17-1, 2 Art 21	National specific	National regulatory body	Guide and review the implementation plan. Impose penalties if necessary
7	Intro-4, 45 Art 7-4 Art 10-2 Art 14-3 Art 20-1	Continuous	Regulated and national regulatory bodies	Risk management and Information sharing

Conclusion

Considering the upcoming threats and the current technological and organizational situation of the essential service operator, it is now imperative to take active steps to eliminate cyber-risk, primarily to protect the organization, and obviously, to meet the requirements of the directive.

For additional information and demonstrating how to conduct the process of complying with the NIS EU 2016/1148 directive please visit:

http://radiflow.com/wp-new-european-cybersecurity-directive/

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 2461963
sales_UK@radiflow.com

http://radiflow.com/ info@radiflow.com

radiflow
Secure Your Assets