HCLSoftware

BigFix Support of NIS 2

HCL **BigFix**

The Network and Information Systems Directive (NIS 2) is a European Union regulationenacted in November 2022 that sets out cyber security requirements for providers of essential services and digital service providers. The aim of the directive is to "achieve a high common level of cybersecurity across the Union."

The directive replaces the original NIS directive and introduces new provisions to improve cybersecurity across a broader range of sectors categorized as essential or important, based upon the significance to the disruption of to the society or the economy. These include manufacturing, finance, healthcare, and transport, and other here to foremore lightly regulated industries that increasingly rely on technology to run their businesses. For more information on affected industries, please see the EU Legislation in Progress EPRS.

At its core, NIS 2 requires organizations to implement security measures to (1) prevent and mitigate cyber threats, and (2) report security incidents to the relevant authorities.

NIS2 is distinguished from GDPR in that the GDPR is oriented toward citizen data privacy and how organizations managepersonal data, while the NIS 2 directive promotes cyber risk mitigation. Enforcement of NIS 2 is scheduled to occur in October 2024.

Article 21 of the directive addresses cyber security risk-management measures includes technical, operational, and organizational measures to manage the risks posed to the security of network and information systems and to prevent or minimize the impact of incidents.Below we will explain how HCL BigFix, a key element of HCLSoftware's Enterprise Security offerings, can accelerate an organization's pursuit of NIS 2 compliance.

This document explains how HCL BigFix can support and accelerate an organization's pursuit of NIS 2 compliance.

Proposed Policy	BigFix Application
A) Policies on risk analysis and information system security;	BigFix can continuously enforce information system security and policies, preventing systems from drifting out of compliance. BigFix provides an organization with the ability to see its vulnerability landscape across the entire fleet of. Then using BigFix, the organization can prioritize and remediate vulnerabilities and non-compliance in real-time.
B) Incident handling;	The BigFix agent running on each managed system can monitor and detect any change that can lead to a security incident. Automated incident handling can be configured to respond to the detected security event.Automation may include isolating the affected endpoints from the network, launch corrective tasks, and returning non-compliant systems to the desired state.
C) Business continuity, such as backup management and disaster recovery, and crisis management;	In a disaster recovery scenario, BigFix can deploy fully provision devices using bare metal recoveries, software distribution, the ability to configure devices using established polices–speeding the recovery following a disaster.
D) Supply chain security, including security- related aspects concerning the relationships between each entity and its direct suppliers or service providers;	While BigFix does not provide specific 'supply chain security', many of its functions can also apply to an organization's direct suppliers or service providers, since BigFix is an industry independent solution.
E) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	BigFix delivers multi-platform patching and ready-to deploy patch content for a wide variety of operating systems (including Windows, UNIX, Linux, macOS) and applications. BigFix can identify all the systems that need to be patched, apply applicable patches to those systems, and then report on the patching status. Effective patch management is the most effective approach to reduce cyber security risk. Additionally, BigFix integrates Tenable and Qualys vulnerability scanning solutions compress the time between discovery and remediation, reducing the windows of vulnerability and minimizethe time required to research and correlate discovered vulnerabilities with available patches. BigFix is an essential tool for organizations to patch and remediate vulnerabilities to efficiently reduce security risks.

Proposed Policy	BigFix Application
G) Basic cyber hygiene practices and cybersecurity training;	BigFix can be leveraged to define and implement cyber security policies and best practices. These include asset discovery, patch management, continuous compliance assessment, hardware and software inventory, and user-driven software distribution.
(H) Policies and procedures regarding the use of cryptography and, where appropriate, encryption;	BigFix can enforce encryption policies at the OS level and ensure that required encryption programs and applications on user devices are running. BigFix provides enhanced security to protect the confidentiality and integrity of the data transmitted between any two BigFix components (e.g., between BigFix Server and a Relay) over internal or public networks using the TLS protocol standard.
(I) Human resources security, access control policies and asset management;	BigFix can discover all devices that have an IP address on the network through distributed NMAP scanning. BigFix provides a centralized information system inventory with detailed information on hardware devices, installed software applications and version numbers, and software license usage. BigFix provides capabilities to create and enforce security policies based on best practice security benchmarks published by CIS, DISA, and PCI DSS. These system level technical policies can augment an organization's security policies such as access control, password management, auditing and logging, and protection from malware.
(J) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	BigFix provides platform and application specific checklists security benchmarks published by CIS, DISA, and PCI DSS. These checklists help an organization enforce secure account access policies such as the use of two-factor authentication or other stronger authentication mechanisms.

In this document, we have introduced the NIS 2 directive and described how HCL BigFix can support an organization in the European Union in their efforts to become and maintain NIS 2 compliant.

HCL BigFix is a proven, effective solution to implement endpoint security measures, preventing and mitigating cyber threats. HCL BigFix has been successfully deployed to over one billion endpoints worldwide across a wide variety of industries including the government sector.

For more information, about HCL BigFix, visit BigFix.com.

For more information about software and services provided to US Federal Government agencies by our partner Four, Inc., visit https://www.hcltechsw.com/resources/us-government-contact.

Sources:
https://www.nis-2-directive.com/
https://www.lexology.com/library/detail.aspx?g=3b7a180e-dacf-4fa5-a55d-287f0a7abacd
https://www.nis-2-directive.com/Annexes_to_the_Proposal_for_a_directive_on_measures_for_a_high_common_level_of_cybersecurity_across_the_Union.pdf
https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new