Information and Network Resilience (NIS2).

AVISI

Information and Network Resilience (NIS2).

Avisi Managed Environment' Comprehensive Approach

Applicable: *Essential Entities* (Energy, Financials, Transport etc.), *Digital Service Providers* (cloud, computing, security etc.), *Public entities*, *Size* (Large and medium enterprises) AND every company in their delivery chain.

When: December 2022, *Transposition Period:* 21 months (ends September 2024.)

What is NIS2

NIS2 stands for "Next Generation Network and Information Sharing System." It is a proposed system to enhance cybersecurity and cooperation among European Union member states. NIS2 aims to improve information sharing and collaboration in responding to cyber threats and incidents. The system is designed to strengthen the EU's resilience against cyberattacks and ensure a coordinated response to cybersecurity incidents.

If the management board fails to implement adequate cybersecurity measures or comply with NIS2 requirements, they may face liability for breaches of their duty of care and potential legal consequences.

Introduction

In an era where institutions face a myriad of digital challenges, the need for a reliable, secure, and compliant digital infrastructure is paramount. Avisi Managed Environment (Kubernetes) is a basis for meeting the needs and might as well exceed them, our offering is a service that aligns perfectly with the requirements of the NIS2 directive, ensuring comprehensive digital resilience. Be aware that is not a full coverage of the NIS2 directive and always needs to be checked by your own company requirements.

This article aims to assist stakeholders in understanding the unique advantages that Avisi Managed Environment (Kubernetes) brings to your application landscape in an increasing complex infrastructure (network) landscape.

Information and Network Resilience (NIS2).

NIS2 Compliance

The impact of the NIS2 Directive (Network and Information Systems Directive 2) on network infrastructure can be significant, depending on the specific requirements and how they are implemented by the member states of the European Union. NIS2 is an update to the original NIS Directive and aims to improve the security of network and information systems across the EU. Here are some keyways NIS2 can impact network infrastructure:

1. **Stricter Security Requirements**: NIS2 may impose more stringent security standards for companies and organizations providing essential services. This could mean network infrastructures need to be upgraded or modified to meet these higher standards.
2. **Broader Scope**: The directive might apply to a wider range of sectors and digital services, meaning more organizations will need to assess and potentially upgrade their network infrastructure to comply with the new requirements.
3. **Incident Reporting**: There could be stricter requirements for reporting security incidents. Networks might need to be equipped with more advanced monitoring and reporting tools to meet these requirements.
4. **Risk Management**: The directive might require organizations to implement more comprehensive risk management processes. This could lead to a need for better network security controls and management tools.
5. **Collaboration and Information Sharing**: NIS2 could promote collaboration and information sharing among member states and businesses. This could lead to the development of shared network security protocols and standards.
6. **Compliance and Sanctions**: Organizations might need to invest more in compliance activities to adhere to the NIS2 Directive, which could lead to investments in both the physical and software aspects of their network infrastructure.
7. **Investing in Cybersecurity**: Overall, NIS2 might encourage organizations to invest more in cybersecurity, including upgrading network hardware and software, implementing advanced security technologies, and training staff in cybersecurity practices.

Information and Network Resilience (NIS2).

Proactive Security Measures

Proactive security measures refer to strategies and actions taken to prevent security incidents before they occur, rather than reacting to them after they happen. This approach focuses on anticipating potential threats and vulnerabilities and implementing measures to mitigate them. Proactive security is increasingly important in the context of information technology and cybersecurity. Here are some key components of proactive security measures:

1. **Risk Assessment**: Regularly evaluating and identifying potential risks and vulnerabilities in the system or network. This includes analyzing the likelihood and impact of different types of cyber threats.
2. **Continuous Monitoring**: Implementing tools and processes for continuously monitoring the network and systems for unusual activities or anomalies that could indicate a security threat.
3. **Security Awareness Training**: Educating employees about cybersecurity best practices, common threats like phishing or social engineering attacks, and the importance of following security protocols.
4. **Regular Software Updates and Patch Management**: Keeping all software and systems up to date with the latest patches and updates to protect against known vulnerabilities.
5. **Firewalls and Intrusion Prevention Systems (IPS)**: Using firewalls and IPS to monitor and control incoming and outgoing network traffic based on an applied set of security rules.
6. **Data Encryption**: Encrypting sensitive data both at rest and in transit to protect it from unauthorized access. Sovereignty is a very important topic considering you bring your applications (data) to a cloud environment. This is not only guaranteed by data encryption but also to easily choose and switch providers if wanted or needed.
7. **Access Control Measures**: Implementing strong access control measures, like multi-factor authentication and least privilege access, to ensure only authorized individuals can access sensitive information or systems.
8. **Disaster Recovery and Business Continuity Planning**: Preparing for the worst-case scenarios with comprehensive disaster recovery and business continuity plans that outline how to respond to and recover from disruptive events.
9. **Regular Security Audits and Compliance Checks**: Conducting periodic security audits to evaluate the effectiveness of security measures and ensure compliance with relevant laws, regulations, and industry standards.

Information and Network Resilience (NIS2).

10. **Proactive Threat Intelligence:** Gathering and analyzing information about emerging threats and trends in cybersecurity to stay ahead of potential attacks.
11. **Incident Response Planning:** Developing and regularly updating an incident response plan to ensure quick and effective action in the event of a security breach.
12. **Secure Configuration and Hardening:** Ensuring that all systems are securely configured and hardened against attacks, including disabling unnecessary services and applying security configurations.

Proactive security measures are essential for organizations to protect their assets, data, and reputation in an increasingly complex and evolving cyber threat landscape. By taking a proactive stance, organizations can significantly reduce their risk of cyber incidents and respond more effectively when incidents do occur. The basic compliance rule here is to guarantee continuity and that is exactly were our focus is on!

Information and Network Resilience (NIS2).

Reactive Security Measures

Reactive security measures are strategies and actions taken in response to a security incident after it has occurred. Unlike proactive measures that aim to prevent incidents, reactive measures are focused on dealing with the consequences of an incident and mitigating its impact. Here are key components of reactive security measures:

1. **Incident Detection and Analysis**: Quickly identifying and analyzing the security incident to understand its nature, scope, and impact. This often involves using intrusion detection systems and monitoring tools.
2. **Incident Response**: Activating an incident response plan which includes steps to contain and control the incident, eradicate the threat, and recover from the damage. This can involve isolating affected systems, applying security patches, or resetting compromised accounts.
3. **Communication and Notification**: Informing relevant stakeholders, including management, affected users, and in certain cases, the public or regulatory bodies, about the incident. This communication should be timely and include information about the nature of the breach and the steps being taken in response.
4. **Forensic Analysis**: Conducting a detailed forensic investigation to determine the cause and method of the breach. This helps in understanding how the security was compromised and in collecting evidence for legal purposes, if necessary.
5. **Damage Control and Mitigation**: Taking steps to limit the damage caused by the incident. This can include restoring systems from backups, patching vulnerabilities, or changing security policies.
6. **Legal and Regulatory Compliance**: Ensuring that the response to the incident complies with relevant laws and regulations, which may include reporting the breach to regulatory authorities within a specified timeframe.
7. **Post-Incident Review and Lessons Learned**: After resolving the incident, conducting a thorough review to understand what happened, how the response was handled, and what could be improved. This often leads to changes in security policies, procedures, and infrastructure.
8. **Updating Security Measures**: Based on the lessons learned, updating and strengthening existing security measures to prevent similar incidents in the future.

Information and Network Resilience (NIS2).

9. **Recovery and Business Continuity**: Ensuring that business operations can continue or quickly resume after an incident. This involves restoring affected services and data from backups and implementing business continuity plans.
10. **Customer Support and Public Relations**: Managing the perception of the incident among customers and the public, which can include addressing customer concerns, providing updates, and rebuilding trust.

Reactive security measures are essential for limiting the damage of security incidents and restoring normal operations. However, relying solely on reactive measures is not advisable, as it can lead to significant damage and loss before the response is initiated. A balanced approach that includes both proactive and reactive strategies is typically most effective in maintaining robust security.

Information and Network Resilience (NIS2).

NIS2 Compliance with the Avisi Management Environment

A comprehensive management platform designed to take away all your worries about meeting compliance rules and, obligations and monitoring. Our platform assists organizations in managing their IT infrastructure and security. Compliance is key and our platform can offer several benefits in the context of complying with the NIS2 Directive. Outlines how our platform supports NIS2 compliance:

1. **Risk Assessment and Management**: Our platform includes integration possibilities for tools for conducting risk assessments, which are crucial for identifying and managing the risks associated with network and information systems, as required by NIS2. Risk Assessments like RCA's and FMEA are also used with support of our platform.
2. **Incident Detection and Response**: The platform offers capabilities for monitoring network activities and detecting security incidents, aligning with NIS2's requirements for timely detection and reporting of incidents.
3. **Compliance Monitoring and Reporting**: A key aspect of NIS2 compliance is adhering to regulatory standards and reporting requirements. Our management platform includes features that help track compliance status and generate reports for regulatory bodies with support of external tools and partners.
4. **Security Policy Management**: The platform assists in developing, implementing, and managing security policies and procedures that are in line with NIS2's guidelines.
5. **Asset Management**: Effective management of IT assets is vital for security. Our management platform can help in maintaining an inventory of all assets and ensuring they are secure and compliant.
6. **Vulnerability Management**: Avisi Managed Environment integrates tools for scanning and identifying vulnerabilities in the network, allowing for proactive remediation before these vulnerabilities can be exploited.
7. **Access Control and User Management**: Managing user access to systems and data is a critical part of cybersecurity. The platform provides robust access control and identity management solutions.
8. **Training and Awareness**: Avisi Cloud provides modules for Kubernetes Cybersecurity training and awareness, which can be used to educate employees about best practices and the importance of compliance with regulations like NIS2.
9. **Audit and Review Tools**: Avisi Managed Environment offers functionalities to assist internal audits and reviews, which are important for ensuring ongoing compliance and identifying areas for improvement.
10. **Business Continuity and Disaster Recovery**: In line with NIS2's focus on resilience, the platform supports business continuity and disaster recovery planning and execution.

Information and Network Resilience (NIS2).

11. **Collaboration and Information Sharing**: The platform facilitates information sharing and collaboration both within the organization and with external entities, in compliance with NIS2's emphasis on cross-sector and cross-border collaboration.

Our platform integrates a broad range of other solutions and tools to meet (specific) demands. For example observability solutions like StackState and Dynatrace. Our platform does not create a vendor lock-in or dependency, everything will still be fully operational without our platform, of course without all the advantages.

For specific details about how the Avisi Managed Environment aligns with NIS2 requirements, it would be best to consult the platform's documentation or contact us directly. We can offer detailed insights into the platform's features and how they can be leveraged to support NIS2 compliance.

Information and Network Resilience (NIS2).

Exceptional Customer Service and Community Focus

1. **Rapid Response and Proactive Communication**: Avisi Cloud has the policy of immediate customer communication in the event of vulnerabilities ensures clients are always informed and prepared to protect their digital assets.
2. **Community-Oriented Approach**: Extending its commitment to digital security beyond its customer base, Avisi Cloud informs other companies of vulnerabilities, showcasing a dedication to elevating industry-wide security standards.

Operational Excellence and Security

1. **Scalability and Performance**: Node pools, auto-healing, and performance graphs ensure business applications are scalable, resilient, and perform optimally.
2. **Simplified Management**: The platform's ease of use, automated upgrades, and CLI management reduce operational complexity, allowing business teams to focus on their core business.
3. **Enhanced Observability**: Integrated monitoring and logging using Prometheus and Loki, and Grafana integration provide in-depth insights essential for maintaining operational resilience.

Information and Network Resilience (NIS2).

Conclusion

Avisi Managed Environment represents an ideal choice for businesses seeking to comply with NIS2 while ensuring operational excellence and security. Its combination of robust security features, proactive customer service, and a community-focused approach positions it as a leader in fostering a secure, efficient, and resilient digital ecosystem in the IT sector. You always need to check with your own organisation to what extend our solutions meets all necessary requirements.

It is a platform that mitigates and manages risks without the necessity to have all the knowledge (resources) and reducing the complexity.

Adopting Avisi Managed Environment is more than a strategic decision; it's a commitment to a higher standard of digital operations and community responsibility.