sbit
Hospitality ICT Services

NIS2

The impact on your hotel

What is NIS2?

The NIS2 Directive is an updated cybersecurity framework established by the European Union to enhance the security of network and information systems across various sectors. It builds upon the original NIS Directive from 2016, expanding its scope to include more sectors and imposing stricter compliance requirements.

NIS2 focuses on risk management, supply chain security, and incident response, aiming to create a more resilient and secure digital environment within the EU.

While hotels themselves are not explicitly listed as NIS2 obligated entities, their (business) guests could be. This means that the hotels are part of the supply chain under this regulation. And as their key partners, such as online reservation platforms and Managed Service Providers (MSPs), like Sbit Hospitality ICT Services, are.

Compliance with NIS2 by these service providers indirectly impacts hotels, making it crucial for them to align with these regulations to ensure the protection of guest data and business operations, and to meet the expectations of their guests.

Why we, Sbit Hospitality ICT Services, are taking this seriously

At Sbit Hospitality ICT Services, we have always taken our responsibility to secure our customers' hotels operations very seriously. Our commitment to maintaining the highest level of security is unwavering.

With the introduction of the NIS2 directive, we want to reassure our customers that no new requirements are being imposed. The recommendations outlined in NIS2 have already been addressed in previous standards such as the Payment Card Industry Data Security Standard (PCI DSS) and ISO27001. While these were previously recommendations, they are now being emphasized as critical measures to ensure robust security.

In recent times, we have observed an increase in phishing attacks targeting the hospitality industry, with the latest incidents involving platforms like Booking.com. This trend highlights the importance of staying vigilant and informed about potential threats. We are dedicated to keeping our customers' security updated and providing the necessary tools and knowledge to protect their businesses from such attacks.

Security is our top priority, and we will continue to work tirelessly to safeguard operations.

And importantly, Managed Service Providers (MSPs), such as Sbit, are required under NIS2 to ensure that their clients have adequate and efficient security measures in place. MSPs have a 'duty of care,' meaning they can be held (financially) liable if their clients fall victim to cyberattacks. Therefore, it is crucial for both MSPs and their clients to maintain clear and transparent communication about cybersecurity roles and responsibilities. This helps to minimize risks and ensures that accountability is properly assigned.

These organizations must comply with NIS2

NIS2 focuses on organizations and institutions with an important societal function. NIS2 applies to the following target groups:

1. Essential organizations
2. Important organizations
3. Chain partners of essential or important organizations
4. Small companies that fall under the exception (strategic targets)
5. Separately designated organizations

As previously mentioned, hotels or the hospitality sector are generally not classified under (1) Essential organizations or (2) Important organizations. But you will probably be part of one of the next target groups:

3.
Chain Partners

Not only large companies fall under the NIS2 directive. Suppliers and service providers that are part of the supply chain of an essential or important organization must also comply with the new cybersecurity requirements. This applies even to companies that are not active in a critical sector or have fewer than 50 employees.

Why? Because cyberattacks often enter through the weakest link. In the past, major incidents have started with a supplier with insufficient security.

Therefore, NIS2 requires companies to impose stricter requirements on their partners. This means that smaller companies must also demonstrably have their cybersecurity in order – not only to mitigate risks but also to continue meeting their customers' requirements.

4.
Exempted Small Companies

Some smaller companies do not fall directly under the standard NIS2 categories but must still comply with the regulations. This mainly applies to organizations that play an important role in the digital infrastructure and are therefore an attractive target for cyberattacks. Think of companies that manage top-level domain names, offer domain name registrations, or provide public communication networks and services. Additionally, government agencies within these sectors automatically fall under NIS2.

5.
Separately Designated Exceptions

If you do not fall into one of the previously mentioned categories, it is still possible that you will have to comply with NIS2. The government can designate organizations that must comply with these regulations by exception.

Why Does NIS2 Affect Us All?

NIS2 companies heavily rely on the security of their suppliers. A cyber incident at one party can have significant repercussions throughout the entire chain. Therefore, NIS2 imposes stricter requirements on suppliers to prevent disruptions. This means that many companies – even if they are not NIS2 entities themselves – will still have to comply with the stricter security rules. "Every cyber incident can disrupt the chain."

The supply chain is most vulnerable at its weakest link, and that is precisely what hackers target. Even a small mistake by a supplier can have major consequences for a company with an important role in our society.

Cybersecurity Insurance

We frequently hear that our customers are exploring cybersecurity insurance. This process often comes with numerous requirements, making it both time-consuming and costly to implement. However, we have some great news to share.

Through our partnership, our customers can benefit from discounts of up to 15% on their cybersecurity insurance. This significant saving is possible because we can demonstrate to the insurer the comprehensive security measures that our customers have in place through our Security package. By showcasing the specific security protocols and standards that you meet, we can streamline the application process, making it much faster and more efficient.

This means that not only can you save money on your insurance premiums, but you can also expedite the approval process, ensuring that you have the necessary coverage in place without unnecessary delays. Our goal is to support you in every aspect of your cybersecurity journey, and this is just one of the many ways we are committed to adding value to your business.

Fines

If an organization does not comply with the NIS2 directive, the sectoral regulator can impose fines.

The amount of these fines is determined by the severity of the violation and can be substantial:

Essential organizations: at least €10 million or 2% of the global annual turnover (whichever is higher).
Important organizations: at least €7 million or 1.4% of the global annual turnover.

Personal Liability of Directors

A significant change under NIS2 is that directors are personally liable for compliance with the legislation. This means they cannot rely on decisions made by others – the responsibility lies directly with the board. Therefore, NIS2 is not just an IT issue but a strategic priority for the entire organization.

Sbit Hospitality ICT Services
Oostbaan 1120
2841ML Moordrecht
The Netherlands
sales@sbit-hospitality.com
+31 182 747 000