HOLM SECURITY

Quick guide

IT security, GDPR and NIS

GDPR - protecting personal data

On May 25, 2018, a new data protection regulation will go into effect for all EU countries. This law will completely override and replace previous laws relating to the handling of personal data and serve as a more homogeneous piece of data protection legislation throughout the EU. It strengthens the individual's right and ability to control their personal information and privacy. The new legislation puts increased demands on the party handling any personal data. An organization that does not comply and exposes personal information (if they are hacked, etc.), can be fined up to 4% of their annual turnover, or 20 million euros.

The new law imposes mandatory incident reporting for incidents related to personal data, such as leakage of personal data when hacked.

To ensure the security of personal data, a proper security infrastructure is required to ensure the resilience of any systems that handle personal data continuously. Because most IT environments are a network of computers, servers, etc. that are all interconnected, security must be ensured throughout the entirety of an IT network in order to be effective.

> ### Example
>
> A hacker accesses a database by hacking a web application. The hacker extracts personal data, such as names and e-mail addresses. The incident, when reported, will be treated as a leak of personal data that may incur fines.

GDPR facts

- GDPR (General Data Protection Regulation)
- Goes into effect 25 May 2018
- Applies throughout the EU
- Regulates the handling of personal data
- Underlies local legislation in each EU country
- Replaces previous legislation
- Indirectly increases IT security requirements
- Incident reporting requirements are introduced with GDPR
- Fines of up to 4% or 20 million euros

NIS - legal requirements for IT security

The Network and Information Security (NIS) is a new EU directive, which is scheduled to come into effect in May 2018. The NIS Directive means that all organizations that carry out socially important activities such as water supplies, power supplies, transport, healthcare, telecom and financial services, must demonstrate that they continuously monitoring and ensuring the security of their IT environment. The driving force behind NIS is the increased cyber security threats for all types of organizations - not least of which come from external third parties.

Examples of affected activities:

- Electric utilities
- Water utilities
- Airlines
- Train companies
- Hospitals
- Telecommunications Companies
- Banks

Example

A company that provides citizens with electricity must be able to demonstrate that they work in an intentional and continuous manner to maintain the security of their IT environment. Breaches or interruptions in service that can be linked back to a lack of IT security can result in serious consequences for the company.

NIS facts

- Network and Information Security (NIS)
- Goes into effect in May 2018
- Applies to all organizations that carry out socially important activities
- Requires structured and continuous IT security work
- Underlies local legislation in each EU country
- It is the responsibility of each organization to prove that they comply with the legislation

How we can help

Our vulnerability assessment platform Holm Security VMP helps you meet new recommendations, legal requirements, and directives in IT security.

- **Increased IT security – without a heavy workload**
  We help you increase your security through automated and ongoing vulnerability analyses that search for over 52,000 weaknesses in your IT environment, as well as for leaks of personal data. The largely automated processes make maintenance an extremely small effort for your company.
- **Discover vulnerabilities before they're exploited**
  With Holm Security VMP, you can detect vulnerabilities before hackers or those with malicious intent do. Our aim is to help you always stay ahead. As an example, the vulnerability exploited by WannaCry was discovered by our platform.
- **Continuous and structured safety**
  Holm Security VMP contributes to continuous and structured security work through powerful automation.
- **Insight, overview and understanding**
  Through generated statistics and reports, you'll get deep insights into the security state of your organization. The generated reports can also be customized and tailored toward specific segments and presentations, like a summary of key security stats for management, for example.

Read more about Holm Security VMP at www.holmsecurity.com.

Holm Security VMP facts

Network Scanning

Automated and continuous vulnerability assessment of external and local systems. Cloud service and virtual instance for local scanning.

Web Application Scanning

Automated and continuous security scanning of web applications and websites. Multiple tests, including the OWASP top 10.

Fraud Risk Assessment

Vulnerability assessment of users in your IT environment to find out how resilient they are against social engineering.

Monitoring of email blacklists

Automated and continuous monitoring of email blacklists to ensure you'll be the first to discover if your mail server has been blacklisted.

Monitoring databases with hacked websites

Automated and continuous monitoring of databases with hacked websites. Discover hacked websites before they can cause damage to your organization.