KL 036.2:

Kaspersky Secure Mail Gateway

Applications covered in the course

- Kaspersky Secure Mail Gateway 2.0

Course description

The training is intended for the administrators who plan to protect corporate mail traffic against malicious objects and spam. This course describes the main scenarios of product integration into the existing infrastructure and explains how to configure protection and authenticate incoming mail using SPF, DKIM, DMARC.

Duration

1 day.

Requirements for the students

Basic knowledge of email protocols and how email server operate.

Basic understanding of networking technologies: TCP/IP, DNS, email, web. Know how to configure Windows servers and workstations. Basic knowledge of information security principles.

Outline

1. Introduction

1.1. E-mail Operation Principles
1.2. Protection Against E-mail Threats
1.3. Kaspersky Secure Mail Gateway Operation Principles

2. How To Deploy Kaspersky Secure Mail Gateway

2.1. OS installation and configuration

Lab 1. Install Kaspersky Secure Mail Gateway

2.2. Configuring an email relay
2.3. Activation

Lab 2. Install the license key
Lab 3. Configure the mail traffic
Lab 4. Check health of Kaspersky Secure Mail Gateway
Lab 5. Configure connection to Active Directory

3. Protection management

3.1. Lists
3.2. Anti-Spam
3.3. Anti-Virus and Links scanning

Lab 6. Lists
Lab 7. Header Analysis and Anti-Spam
Lab 8. Configure the Anti-Virus

3.4. Anti-Phishing, Content Filtering and Mail Sender Authentication

Lab 9. Content Filtering
Lab 10. Configure verification for incoming mail

4. Maintenance

4.1. Monitoring: dashboard, logs and reports
4.2. Notifications and warnings
4.3. Backup

Lab 11. Setting up the dashboard

5. Advanced settings

5.1. Encryption and DKIM
5.2. Accounts

Lab 12. Configure DKIM
Lab 13. Set up access for a HelpDesk employee

5.3. Scaling and maintenance
5.4. Integration with other systems