

Cursusinhoud:

Module 1: Introduction to Designing Security

A security design is a comprehensive plan that guides the implementation of security policies and procedures for an organization. A security design helps an organization to organize its assets to implement security in a consistent and effective manner.

This module describes the basic framework for designing network security and introduces key concepts used throughout the course. It also introduces a fictional organization which the labs in the course use as an ongoing case study.

Module 2: Creating a Plan for Network Security

Plans for network security include documented security policies and procedures. These policies and procedures, when implemented, help to secure networks against compromises. This module describes the importance of security policies and procedures in a security design, and explains how a security design team must include representation from various members of the organization. The module also introduces the Microsoft Solutions Framework (MSF) process model, which provides a comprehensive framework that can be used to create a security design.

Module 3: Identifying Threats to Network Security

Without security measures and controls in place, your data may be subjected to an attack. Some attacks are passive, which means that information is monitored; others are active, which means that the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of these types of attacks if you do not have a security plan in place.

In this module, you will learn how to identify possible threats to a network and understand common motivations of attackers. The module introduces the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat model as an effective way to predict where threats may

The Microsoft approach to security risk management is proactive and can assist organizations of all sizes with their response to the requirements presented by these environmental and legal challenges. A formal security risk management process enables enterprises to operate in the most cost-efficient manner by adopting a known and acceptable level of business risk. It also gives organizations a consistent, clear path to organize and prioritize limited resources in order to manage risk.

In this module, you will learn how to determine what resources in your organization require protection and how to prioritize those resources based on their value. You will then develop a risk management plan, based on the MOF risk model, to identify and analyze risks proactively and to determine an appropriate level of protection for each resource.

Module 5: Designing Physical Security for Network Resources

Physical security refers to physical measures designed to safeguard personnel, property, and information. The term applies to architectural features such as location, layout, barriers, doors, locks and bolts, and lighting, but also includes measures such as access control systems, alarm systems, and CCTV systems.

In this module, you will determine threats and analyze physical risks to resources in an organization. You will then learn how to design security for facilities, computers, mobile devices, and hardware. You will also learn about implementing disaster recovery as a way to protect physical resources. This module focuses on physical access to resources and how to protect them. Other modules will focus on access to data and how to protect it.

Module 6: Designing Security for Network Hosts

The Windows Server2003, Windows XP Professional, and Windows Vista operating systems provide many features and capabilities that you can use to configure and maintain a secure network operating environment. In fact, there are security capabilities in nearly every area of Windows. Many of these security features and

Module 8: Designing Security for Authentication

In this module, you will learn how to determine threats and analyze risks to authentication. You will learn how to design security for authenticating local users, remote users, and users who access your network across the Internet. You will also learn when to choose multifactor authentication for additional security.

Module 9: Designing Security for Data

In this module, you will learn how to determine threats and analyze risks to data in an organization. You will learn how to design an access control model for files and folders in order to protect data that is stored on network servers. You will also learn about considerations for encrypting and managing data.

Module 10: Designing Security for Data Transmission

In this module, you will learn how to determine threats and analyze risks to data transmission in an organization. You will also learn how to design security for various types of data transmission, including traffic on local area networks (LANs), wide area networks (WANs), Virtual Private Networks (VPNs), wireless networks, and the Internet.

Module 11: Designing Security for Network Perimeters

In this module, you will learn how to determine threats and analyze risks to network perimeters. You will also learn how to design security for network perimeters, including perimeter networks (also known as DMZs, demilitarized zones, and screened subnets), and for computers that connect directly to the Internet.

Module 12: Responding to Security Incidents

Network security for an organization is an exercise in prevention. A good security design that is properly implemented will prevent most of the most common attacks. However, it is very likely that an attacker will

occur in an organization.

Module 4: Analyzing Security Risks

Many organizations cannot react to new security threats before their business is affected. Managing the security of their infrastructures—and the business value that those infrastructures deliver—has become a primary concern for information technology (IT) departments.

capabilities have been added or enhanced since the introduction of the Microsoft Windows2000 Professional and Windows2000 Server operating systems.

In this module, you will learn how to determine threats and analyze risks to network hosts in an organization. You will also learn how to design security for network hosts throughout their life cycles, from initial purchase to decommissioning.

Module 7: Designing Security for Accounts and Services

Computer networks use accounts to grant users, applications, and network services access to the information on a network. Network services are server applications that are usually hosted on dedicated server computers.

In this module, you will learn how to determine threats and analyze risks to accounts and services in an organization. You will also learn how to design security for accounts and services, including determining security requirements, creating policies, and designing strategies to manage security.

eventually penetrate the defenses that you design.

When an attack happens, the key to limiting damage is early detection and a rapid and orderly response. Auditing is an important tool to help you to detect network abnormalities that may indicate attacks. An incident response procedure is a series of steps that you design in advance to guide your organization during a security incident.

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.nl

Iepenhoeve 5, 3438 MR Nieuwegein