NAMA: Wiraswanti Rismanda Putri

NO: 20

KELAS: SIB4C

Lab - Risk Management

Introduction

An organization's process of identifying and assessing risk is a continuous effort because types of threats change and they never completely disappear. The goal of risk management is to reduce these threats to an acceptable level. There are different levels of risk management. Organizations must properly manage risk to protect information and information systems. Risk management also helps to prevent legal actions, interruptions to operations, and safeguards the organizations' reputations.

Objectives

Explore the Risk management process.

Part 1: Explain Risk Action Levels

Part 2: Explain Risk Management Concepts

Part 3: Explain Risk Management Processes

Required Resources

PC or mobile device with internet access

Instructions

Part 1: Risk Action Levels

Risk management is the identification, evaluation, and prioritization of risks. Organizations manage risk in one of four ways. Each may be an appropriate choice, depending on the circumstances and type of risk in question:

- **Avoidance (Elimination)** - Risk avoidance is the complete removal or elimination of risk from a specific threat. For example, avoiding or eliminating the threat of users sharing or misusing passwords could involve implementing a fingerprint authentication system on all user workstations.
- **Mitigation (Reduction)** - Risk mitigation involves implementing controls that allow the organization to continue to perform an activity while using mechanisms to reduce the risk from a particular threat. An organization could also increase its technical controls and network oversight to reduce risk from operational threats.
- **Transfer** - Organizations can transfer risk from specific threats. The financial risk of a threat can be managed by purchasing an insurance policy, or hiring a contractor to deal with specific threats.
- **Accept** - Accepting risk involves the identification of the threats but not implementing mitigation processes only after a conscious decision has been made to do so. The conscious decision is informed by analyzing the various components of the risk before proceeding.

Step 1: Manage risk.

In this Step, you will describe examples of managing risk associated with specific threats to the organization's information or information systems.

a. An organization is regularly required to handle sensitive customer information. The release of this information poses a serious risk to the organization.

What steps could the organization implement to eliminate the risk associated with accidental emailing or transferring of this information?

Answer: **Organisasi bisa menetapkan kebijakan yang melarang karyawan mengirim email atau mentransfer data pelanggan dalam bentuk apa pun. Selain itu, organisasi dapat membatasi akses karyawan terhadap informasi tersebut. Organisasi juga memiliki kemampuan untuk**

menyaring dan memblokir semua data yang dikirim melalui email atau ditransfer melalui jaringan internal.

b. The organization has had several issues of employees sharing passwords or using weak passwords. Name two ways to mitigate this risk.

Answer: **Menerapkan kebijakan dan pedoman kata sandi organisasi dengan mewajibkan penggunaan kata sandi yang kuat di seluruh sistem organisasi.**

Give two examples of an organization transferring risk.

Answer: **Pemanfaatan asuransi atau kesepakatan tingkat layanan perlu dijadikan acuan**

Step 2: Explore risk levels.

An organization's process of identifying and assessing risk is a continuous effort because types of threats change and they never completely disappear. The goal of risk management is to reduce these threats to an acceptable level.

Perform an internet search using the following terms: negligence, due care, and due diligence to answer the following questions:
What is negligence? Give an example of the consequences of negligence.

Answer:

Kelalaian terjadi ketika tidak ada tindakan atau kontrol yang diterapkan untuk mengurangi risiko. Ancaman yang dihadapi sangat besar, dan dampak dari insiden bisa sangat signifikan, bahkan dapat berujung pada tuntutan pidana.

Define due care and due diligence and explain the difference between these two terms.

Answer:

Kehati-hatian wajar berarti mengambil tindakan untuk mengurangi risiko, meski risiko tetap ada. Uji tuntas bertujuan meminimalkan risiko dengan langkah-langkah pencegahan, meskipun sebagian risiko masih tersisa.

Part 2: Risk Management Concepts

Risk management is a technique used to identify and assess factors that may threaten information and information systems. The study of risk analysis includes several commonly used terms and concepts, including the following:

Assets – Assets are anything of value that is used in and is necessary for completion of a business task. Assets include both tangible and intangible items such as equipment, software code, data, facilities, personnel, market value and public opinion. Risk management is all about protecting valued organizational assets.

Threats – Threats are a malicious act or unexpected event that damages information systems or other related organizational assets. They can be intentional actions that result in the loss or damage to an asset. Threats can also be unintentional like an accident, natural disaster, or equipment failure.

Vulnerability – Vulnerabilities are any flaw or weakness that would allow a threat to cause harm and damage an asset. Examples could be fault code, misconfigurations, and failure to follow procedures.

Impact - Risk impact is the damage incurred by an event which causes loss of an asset or disruption of service. This damage can be measured quantitatively or qualitatively based on the impact to the organization's operations.

Risk – Risk is the probability of loss due to a threat to an organization's assets.

Countermeasures – Countermeasures are an action, device, or technique that reduces a threat or a vulnerability by eliminating or preventing it. An example would be antivirus software, firewalls, policies, and training.

Risk Assessment – Risk assessment is the process of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

What is a security risk assessment? A risk assessment identifies, quantifies, and prioritizes the risks and vulnerabilities in a system. A risk assessment identifies recognized threats and threat actors and the probability that these factors will result in an exposure or loss.

Case Study:

A business manages a customer database that tracks online purchases of the products. These purchases are made with PayPal accounts or credit cards. The database server has several vulnerabilities. The database is on a server in the server room at the company headquarters. The server cost $25,000. The database consists of all 40,000 customers and over 1.5 million transactions. The server records over 120 transaction per day generating over 25K per day in sales. The data base is backed up daily at 2AM. All orders are also tracked and logged on separate systems in case of server failure. This process can take up to 50-person hours of entry to manually process every day.
Name at least two types of vulnerabilities the cybersecurity staff should analyze:

Answer:

Kerentanan dapat mencakup kegagalan perangkat keras, serangan oleh peretas, bencana, malware, serta kesalahan dalam konfigurasi.

Describe possible threats to the server based on the vulnerabilities you identified:

Answer:

Ancaman terhadap server meliputi kerusakan perangkat keras akibat kegagalan peralatan, pelanggaran data atau serangan ransomware, bencana seperti kebakaran, tornado, badai, gempa bumi, serta kerusakan atau kegagalan sistem yang disebabkan oleh malware atau konfigurasi yang salah, yang dapat mengakibatkan kinerja yang buruk.

Describe the impact to the organization due to the following threats:

Data Breach:

Answer:

Dampaknya dapat bervariasi, mulai dari kehilangan server database secara keseluruhan hingga memengaruhi penjualan dan pendapatan organisasi. Selain itu, dampak tersebut juga dapat mencakup kerusakan terhadap reputasi bisnis.

Ransomware:

Answer:

Dampaknya dapat bervariasi dari hilangnya server database secara keseluruhan hingga memengaruhi penjualan dan pendapatan organisasi, serta mengganggu operasi sehari-hari. Selain itu, dampaknya juga bisa mencakup kerusakan pada reputasi perusahaan.

Hardware failure:

Answer:

Dampak yang ditimbulkan dapat bervariasi, mulai dari kehilangan total server database hingga memengaruhi penjualan dan pendapatan organisasi. Selain itu, dampaknya juga bisa melibatkan kerusakan pada reputasi bisnis.

List one **countermeasure** for the following threats to the organization's database server:

Data Breach:

Answer:

Tindakan untuk mengatasi pelanggaran data dapat meliputi pembaruan kebijakan atau prosedur, enkripsi data, pelatihan karyawan tentang langkah-langkah keamanan, peningkatan keamanan, dan pembatasan akses sesuai kebutuhan.

Ransomware Attack:

Answer:

Tindakan untuk mengatasi serangan ransomware dapat mencakup penggunaan antivirus dan perangkat lunak antimalware, memperbarui sistem operasi dan aplikasi, melakukan pencadangan data, menerapkan kebijakan keamanan, serta menggunakan mekanisme kontrol akses fisik.

Hardware Failure:

Answer:

Tindakan untuk mengatasi kegagalan perangkat keras dapat meliputi penerapan redundansi perangkat keras, penggunaan mekanisme kontrol akses, serta penggantian peralatan yang telah usang.

Malware:

Answer:

Tindakan penanggulangan dapat mencakup penggunaan perangkat lunak antivirus dan antimalware, pemutakhiran sistem operasi dan aplikasi, pencadangan data, penerapan kebijakan keamanan, serta mekanisme kontrol akses fisik.

Part 3: Risk Management Processes

Risk management is a formal process that reduces the impact of threats and vulnerabilities. You cannot eliminate risk completely, but you can manage risk to an acceptable level. Risk management measures the impact of a threat and the cost to implement controls or countermeasures to mitigate the threat. All organizations accept some risk. The cost of a countermeasure should not be more than the value of the asset you are protecting.

Step 1: Frame and Assess Risk

Identify the threats throughout the organization that increase risk. Threats identified include processes, products, attacks, potential failure, or disruption of services, negative perception of organization's reputation, potential legal liability, or loss of intellectual property.

After a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses. Some threats can bring the entire organization to a standstill while other threats are minor inconveniences. Risk can be prioritized by actual financial impact (quantitative analysis) or a scaled impact on the organization's operation (qualitative analysis).

In our example, the following vulnerabilities have been identified. Assign a quantitative value to each risk based on your committee answers. Provide justification for the value you determined.
Use the case study to formulate your answers.

Data breach impacting all customers:

Answer:

Dampak dari pelanggaran data dapat mengakibatkan biaya sebesar $100.000 atau lebih dan memerlukan waktu 5 hari kerja untuk memulihkan data.

Server hardware failure requiring hardware replacement:

Answer:

Dampak kegagalan perangkat keras bisa menelan biaya $5.000 atau lebih dan 2 hari kerja untuk mengganti perangkat keras yang rusak.

Ransomware affecting the entire server database:

Answer:

Dampak serangan ransomware bisa menelan biaya $20.000 atau lebih dan 5 pekerja hari untuk memulihkan data dan menghapus ransomware.

Server room flood caused by fire sprinklers being activated:

Answer:

Dampaknya bisa menelan biaya $50.000 atau lebih dan 3 hari kerja untuk mengganti perangkat keras yang rusak dan memulihkan data.

Step 2: Respond to Risk

This step involves developing an action plan to reduce overall organization risk exposure. Management ranks and prioritizes threats; a team then determines how to respond to each threat. Risk can be eliminated, mitigated, transferred, or accepted.
Rank the vulnerabilities and propose possible countermeasure for each threat.

Data breach impacting all customers:

Answer:

Dampak dari pelanggaran data sangat signifikan. Biaya yang harus dikeluarkan bisa mencapai $100.000 atau lebih, serta mempengaruhi kepercayaan pelanggan dan reputasi perusahaan. Beberapa langkah penanggulangan yang bisa diambil meliputi pelatihan karyawan, enkripsi data, serta pembaruan perangkat lunak dan perangkat keras.

Server hardware failure requiring hardware replacement:

Answer:

Dampak kegagalan perangkat keras server adalah sedang yang dapat menelan biaya $5.000 atau lebih dan gangguan layanan. Beberapa tindakan penanggulangan dapat berupa pencadangan data dan sistem.

Ransomware affecting the entire server database:

Answer:

Dampak serangan ransomware tergolong ringan, namun tetap berpotensi menimbulkan biaya lebih dari $20.000. Serangan ini bisa mengakibatkan gangguan layanan serta kehilangan data. Beberapa langkah pencegahan yang dapat diambil meliputi pelatihan keamanan dan pencadangan data.

Server room flood caused by fire sprinklers being activated:

Answer:

Dampak serangan ransomware tergolong rendah, namun tetap bisa menimbulkan biaya lebih dari $50.000, serta menyebabkan gangguan layanan dan hilangnya data. Beberapa langkah pencegahan yang bisa diambil meliputi pembelian asuransi dan melakukan pencadangan data.

Step 3: Monitor Risk

Continuously review risk reductions due to elimination, mitigation, or transfer actions. Not all risks can be eliminated, so threats that are accepted need to be closely monitored. It is important to understand that some risk is always present and acceptable. As countermeasures are implemented, the risk impact should decrease. Constant monitoring and revisiting new countermeasures are required.

What actions could decrease the impact of a ransomware threat?

Answer:

Melakukan backup data secara berkala, penggunaan antivirus dan firewall, melakukan update dan patch sistem secara teratur.