Security Assessment

These assessment tasks provide an opportunity for you to demonstrate the competencies required to identify cyber security risks and design, plan and deploy cyber security solutions.

**Successful completion of this assessment contributes towards attaining competency in the following:**

|  |  |
| --- | --- |
| ICTNWK502 | Implement secure encryption technologies |
| ICTNWK509 | Design and implement a security perimeter for ICT networks |
| ICTNWK503 | Install and maintain valid authentication processes |

**Assessment questions and tasks**

Your task, as a group of 2 or 3 people, is to redesign the network security infrastructure for Spyon Technologies so that it meets the business requirements for the organisation, and to write a detailed proposal which you will submit to Spyon Technologies for consideration.

To complete this task, you will submit a final design proposal to Spyon Technologies which will include:

* a detailed list of business requirements that must be met by the network security design
* a complete and detailed discussion of the network security design proposal. This must include complete logical diagrams of the redesigned network and a discussion of the techniques and technologies used, e.g. Clustering, zones, policies, authentication, encryption, and VPN's
* details of how the network security design will meet all the business requirements

You will also need to:

* Prepare implementation plans
* Document the network design and present the documentation to the appropriate person for approval
* Present the design in a clear and logical fashion
* Provide advice to the client on reasons for your design choice.

The most important idea to keep in mind is that the goal of any proposal is to convince potential clients to award you their contracts.

The scenario and questions below will guide you through many of the things you will need to consider for your proposal. You need to answer the questions and then write your proposal.

**Scenario**

You are employed by Spyon Technologies, a global business that manufactures weapons and military technology and equipment.  You work in the cyber security division as a network engineer. Your role is to assist with the planning and implementation of security measures and general network infrastructure.

**Company profile**

Spyon Technologies is a global security and aerospace company that employs about 120,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration, and sustainment of advanced technology systems, products, and services. The Corporation's sales from continuing operations are $46.5 billion P/A.

The company's primary business is in supplying military equipment to Governments around the world.

Company's Security Statement: Cyber Security attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry.  Adversaries are targeting anyone who possesses the sensitive information they seek including the government, prime contractors, and suppliers.  It is imperative that our suppliers understand what's at stake and recognize our shared role in protecting sensitive information and intellectual property.   A single mistake or breach could have enormous consequences for our customers, our business, the Aerospace & Defense Industry, and national security.

The Spyon Technologies Cyber Security Alliance combines the strengths of market leading companies' solutions and integrates their best practices, hardware, software and tools within the NexGen Cyber Innovation and Technology Center. The Alliance Companies include APC by Schneider Electric, ArcSight, CA, Cisco, Citrix, CyberPoint, Dell, EMC Corporation and its RSA Security Division, FireEye, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, Radware, RedHat, Splunk, Symantec, Trustwave, Verizon and VMware.

**IT Services**

Spyon Technologies uses the following server technologies:

1.Web servers for the company intranet and Web applications.  This is accessed by remote workers.

2.Mail servers - Used by internal and external staff

3.Unified Communications servers

**Security Requirements**

Much of Spyon Technologies business dealings involve top secret military projects with governments around the world.  It is imperative that the details of these projects remain confidential. The following security measures are required:

**1. The security perimeter must prevent all unauthorized access to company data.**

**2. All WAN links must be encrypted and secured.**

**3. All electronic communication within the company and with third parties must be encrypted and digitally signed.**

**4. Measures must be put in place to protect against DOS, DDOS, viruses, and all other cyber security threats.**

**5. The solution must be fault tolerant by eliminating single points of failure**

**High Level Network Diagram - Australian Operations**

<http://www.mediafire.com/view/o41o7me2uh3sp8m/Campus%20Network%20Overview_Full.png>

The FDDI and DSL WAN connections are provided by a commercial telecommunications carrier.

**Question 1**

a. Would you describe Spyon Technologies security requirements as high, medium, or low? Why?

b. What types of security measures would you use to address each of the security requirements listed?

**Question 2**

Spyon Technologies has adopted the following risk evaluation criteria using a qualitative risk assessment methodology.

In order to calculate the risk level for each risk that is to be examined, it is necessary to calculate the impact of the threat occurring and the likelihood (or probability) of the threat occurring.

Impact/Consequence Calculation

As the impact can have many different effects on the business it is necessary to consider both the direct financial impacts and the other effects on the business through issues such as damage to reputation, safety, disruption, etc.

An impact/consequence matrix is shown below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact Level** | **Financial damage** | **Reputation damage** | **Internal disruption** | **Personnel safety** |
| **Critical** | >$10 million | Widespread national press, significant damage to customer confidence | Whole organisation unable to operate for significant period | Loss of life |
| **High** | $1-$10 million | Local press coverage / damage with many customers | Disruption across organisation | Major injury to individual |
| **Medium** | $100k-$1 million | Some damage with individual customers | Business area unable to operate | Minor injury to individual |
| **Low** | <$100k | Internal only | Local short term disruption only | Potential danger |

A Likelihood/Probability table is shown below:

|  |  |  |
| --- | --- | --- |
| **Likelihood** | **The event is likely to occur:** | **Annual frequency (Probability)** |
| **Almost Certain** | At least once per year | >50% / year (>0.5) |
| **Likely** | Once every 2-4 years | 20% - 50% (0.2-0.5) |
| **Moderate** | Once every 5-10 years | 5- 19% (0.05-0.19) |
| **Low** | Less than once every 10 years | < 5% / year (<0.05) |

Risk Calculation

The level of risk is a combination of the likelihood and threat/consequence

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact  Likelihood | **Low** | **Medium** | **High** | **Critical** |
| **Almost Certain** | **High** | **High** | **Extreme** | **Extreme** |
| **Likely** | **Medium** | **High** | **High** | **Extreme** |
| **Moderate** | **Low** | **Medium** | **High** | **High** |
| **Low** | **Low** | **Low** | **Medium** | **High** |

Make a list of possible cyber security threats. Allocate each threat an impact level, likelihood, and risk level.

Example format:

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Impact Level | Likelihood | Risk Level |
| DDOS ICMP flood, UDP flood | High | Likely | High |
| Unauthorised access from external source | Critical | Almost certain | Extreme |
| Unauthorised access from internal device | Critical | Moderate | High |
| Man-in-the-middle attack | Critical | Moderate | High |

Definition of a threat:

A threat is 'a potential cause of an unwanted event which may result in harm to a system or organisation' (HB 231).

*Alternatively*, a threat is 'Anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them.  A source of, or potential for harm to occur. A threat can be a source of risk' (HB 167)

**Question 3**

Using your list of threats, create a table that lists the defences for each threat

Example format:

|  |  |
| --- | --- |
| Threat | Defence |
| DDOS ICMP flood, UDP flood | Firewall ICMP and UDP flood thresholds |
| Unauthorised access from external source | Firewall security policies, IDP settings |
| Unauthorised access from internal device | MAC limiting, IP source guard |
| Man-in-the-middle attack | PKI digital certificates |

**Question 4**

Design the firewall configuration. *Ref: How to Design a Secure DMZ*

Your design should include the following:

1.The name of each security zone you will create

2.The inter zone policy objectives including

a.Traffic allowed into the zone

b.Traffic allowed between the zones

c.Other security measures to be implemented in the policy

3.Method of securing traffic from site to site

4.Method of securing traffic to and from the public internet

**Question 5**

Write the Juniper SRX configuration required to implement all the functionality described in your answer above. You may refer to the SRX lab configurations. You will need to provide your IP addressing scheme as a separate table.

*Ref: FTP Sever/Juniper/Juniper\_Class\_Configs/JSEC/*

**Question 6**

Design failover redundancy for the firewall so that a stateful failover of processes and services will occur in the event of system or hardware failure.   Provide a diagram of your design and a description of how failover will be achieved in the event of a failure.

*Ref:JNAA-JSEC-12.a\_IG Chapters 9 and 10*

**Question 7**

Provide a typical failover redundancy configuration for a Juniper SRX firewall. *Ref: FTP Sever/Juniper/Juniper\_Class\_Configs/JSEC/*

**Question 8**

Provide a typical site to site VPN configuration for a Juniper SRX firewall. *Ref: FTP Sever/Juniper/Juniper\_Class\_Configs/JSEC/*

**Question 9**

Is the network traffic traversing the IPSEC VPN encrypted using  symmetric or asymmetric encryption? Explain the difference between these 2 methods. Compare 3 algorithms that could be used to encrypt the IPSEC VPN traffic.  List the tests you will perform to verify that your security measures and VPN are functioning as expected. *Ref:JNAA-JSEC-12.a\_IG Chapter 7*

**Question 10**

You want to encrypt email communications between all company staff and business associates.  What program could you use to do this? What are the advantages of this program? What type of encryption would be used? What encryption algorithms could be used? *Ref: Pretty Good Privacy (PGP); An Introduction to Cryptography - Phil Zimmermann, Understanding S/MIME*

**Question 11**

You want to ensure the integrity of email and other digital communication.  How can this be achieved? What algorithms could be used? *Ref: An Introduction to Cryptography - Phil Zimmermann, S/MIME for message signing and encryption*

**Question 12**

What authentication processes could you use to verify the identity of the person from who you are receiving email and other digital communication and to verify your identity to people you are sending communications to?  What algorithms could be used? *Ref: An Introduction to Cryptography - Phil Zimmermann, S/MIME for message signing and encryption*

**Question 13**

Evaluate the following providers of digital certificates and create a comparison table.  The table should compare the cost and advantages of the certificate services offered by each.

* Thawte
* Go Daddy
* Comodo
* GlobalSign
* GeoTrust
* Symantic

*Ref:*[*https://cheapsslsecurity.com.au/sslcompare/compare-ssl-certificates-prices.html*](https://cheapsslsecurity.com.au/sslcompare/compare-ssl-certificates-prices.html)

**Question 14**

Provide a brief summary of Kerberos and NTLM Authentication. Describe the benefits of Kerberos Authentication. *Ref: Module 10\_ Securing Windows(r) 8*

**Question 15**

Provide a brief summary of Biometrics for Authentication. Describe the benefits of using Biometrics for Authentication. List 3 devices you could use to provide Biometric Authentication? *Ref: Module 10\_ Securing Windows(r) 8*

**Question 16**

Explain the concept of digital certificates and how they work including:  
The relationship between user certificates and root certificates and the function of root certificates

* The role of Certificate Authorities
* The role of Registration Authorities
* The function of a digital certificate repository

Ref: <https://www.thesslstore.com/blog/root-certificates-intermediate/>

**Question 17**

What are the factors that contribute to encryption strength?

**Question 18**

You are reviewing help desk records and discover that emails to some recipients are not able to be encrypted while emails to other recipients are. What is the cause of this and how could it be resolved?

**Question 19**

Explain what a replay attack is and describe 2 methods of protection. Ref: <https://www.kaspersky.com/resource-center/definitions/replay-attack>

**Question 20**

Describe 5 security threats that can be caused by issues within the organisation. Ref: <https://www.zdnet.com/article/the-top-five-internal-security-threats/>

**Question 21**

Explain the difference between WEP, WPA and WPA2. Ref: <https://difference.guru/difference-between-wep-wpa-and-wpa2/>

**Question 22**

Explain authentication, authorization, and accounting (AAA). Your explanation should include the functions of a RADIUS server and it role in the resource accounting process. Ref: <https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting>

**Question 23**

Describe the function and operation both IPSEC and MPLS VPN’s.  Compare these 2 technologies in terms of their ability to provide QoS, guaranteed bandwidth, and changing security requirements like the need for secure voice or video. Ref: <https://community.fs.com/blog/vpn-vs-mpls-difference.html>

**Question 24**

Describe and compare CHAP and PAP authentication protocols.

**Question 25**  
Write your proposal to Spyon Technologies.

The following link may help: <https://www.linkedin.com/pulse/20140819165132-18011256-how-to-write-an-information-technology-it-business-proposal>

**Submission requirements**

1. The written tasks must be completed on a word processor and uploaded to the learning portal. You must clearly indicate which question each answer relates to.
2. Device configurations should be included as separate files which are clearly named.
3. The Visio diagram should be saved as a pdf and uploaded.
4. All files must have your name in the file name.
5. You must click the 'Submit' button.