**Introduction-**

Perfect pets in an UK based e-commerce company. They are manufacture high-quality pet products. Their growth strategy is increased day by day and they sell their 75% products via an e-commerce site. Now Perfect pets company are using LAN to control their domain which is hosted by ISP where company stored all their business data, processing and marketing system, but they are hesitate to marketing their products because ISP doesn’t provide any e-commerce facilities. Company have a security question for maintaining e-commerce via ISP. They can face any kind of online attack in future, that’s why Company MD decided to get consultant help to protect their e-commerce network system. Consultant identifies company online threats and provided better possible solution.

**Task-1**

1. Below show the five (5) most important electronically held information assets in the company-
2. Customer Personal Data.
3. Marketing Information.
4. Payment Details.
5. Financial Details.
6. Company Personal Data.
7. Production Data.

**Justification for the five point-** For the Security purpose reduced the risk assessment, I listed down this, five information assets which is valuable and prioritized for this company. Which can help to protect from the hacker, for example- a hacker can entered your network and copied your entire customer data and damaged your database information.

So that kind of information is critical for this “Perfects Pets” Company. This information assets confidentiality, integrity and availability is of utmost importance.

**Reasonable Assumptions-** This Information asset has risks associated with “Perfects Pets” Company, which is the risk of losses the assets, information will fall into the wrong hands, getting corrupted or any number of other issues. By considering these risks, we will able mitigate against risk measures and plans.

**Below shows the b, c, d question answer in a table based on Selected assets-**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets(a)** | **Threat(b)** | **CIA(b)** | **Likelihood(c)** | **Impact(c)** | **Risk (d)** |
| Customer Personal Data | Server Failure | A | Low | Medium | Low |
| Information leakage | C | Low | High | Medium |
| Phishing Data | C | High | High | Medium |
| Viruses | A | Low | Medium | Low |
| Fire | I | Low | High | Very High |
| Software Errors | C | Medium | Low | Very Low |
| Marketing Information. | Server Failure | A | Low | Medium | Medium Low |
| Loss of Support Services | C | Low | Low | Medium Low |
| Information Leakage | C | Medium | High | High |
| Ransom Ware Attack | A | Low | High | High |
| Payment Details | SQL Injection | I | Medium | High | Very High |
| Phishing | C | High | High | Very High |
| Software Errors | A | Medium | Low | Medium |
| Spyware | A | Medium | High | High |
| Financial Details | SQL Injection | I | Medium | High | Very High |
| Software Errors | A | Low | Low | Medium |
| Ransom Ware Attack | A | Low | High | High Medium |
| Malware | A | Low | Low | Medium |
| Information Leakage | C | High | High | Very High |
| Company Personal Data | Server Failure | A | Low | low | very low |
| Information leakage | C | Medium | high | Very High |
| Viruses | A | Low | Medium | High |
| Fire | I | Low | High | Very High |
| Software Errors | A | Low | low | low |
| Unauthorized use of software | C | Medium | high | High |
| Production Data | Software Errors | A | Low | low | low |
| Unauthorized use of software | C | Medium | high | High |
| Fire | I | Low | high | Very High |
| Information leakage | C | Low | high | Very High |

**Task-2**

1. **Security Threats**

After analysis the scenario for Perfect Pets company I have identified threats and highest risks and also plan the possible solutions to reduce the risk.

Below show the explanation and the plane-

1. **Fire Threats-** In the scenario we can see that Perfect Pets company using LAN included Domain Controller based on windows server 2012R2 which hosts financial systems, order processing, customer record data, email and human resources data. Now we can understand the company store all activity in the local server which is in the highest vulnerabilities, because in future if the server internal and external physical attack can be happen, for that reason they can lose all their business data. For this we have planned a proper step to safe their server data.

**Solutions -**

1. First of all, the Perfect Pets company need to set up their own server to store all the data. Because hosted server can’t provide all the security installation.
2. Setup fire detection devices and system and maintained them regularly and server room temperature must be under control.
3. Train Server staff/employees to know what measures to take when the alarm is activated.
4. Important data have a backup file needed in cloud server or another server. (lucionservices, 2019)
5. **Information leakage-** The company Store all the marketing information, financial details, company, personal data, production details which is private and Important information for the company. So if any employee betrays to the company and leaked that data into another company then the company will be faced with a big loss. To reduce that kind of internal security problems we have a plan- (sans.org, 2019)

**Solutions -**

1. To hire an employee, we must Inquiry employee background very carefully.
2. For security reason, apply lock policy for each and every employee account.
3. Fixed employee access level to set password and each other employee can’t access file and documentation.
4. Network and share devices configure securely.
5. **SQL Injection**- In the scenario company have a domain and domain hosted into the local ISP. Which is under risk because we don’t know about the server security and the network security, we can't ensure that which security standard they follow to protect the server. So today or tomorrow, the Server may face SQL Injection attacked, which may damage the company physical or logical important data like- Payment Details, company Financial Details etc. We also have a plane to reduce the SQL injection attack risk- (malwarebytes, 2019)

**Solutions –**

1. Setup won server to reduced one stage risk.
2. User validation to filter All user input data and then store them.
3. Setup Demilitarize zone which will provide additional security layer for internal and external LAN attack. (searchsecurity.techtarget., 2019)
4. **Phishing Data-** In the scenario we can see that company run e-commerce website where customer directly can buy products from their site and pay through online. They also host their domain into the other local server where they are not prepared for any kind of online attack, so we clearly say company can have faced phishing attack from online. The company and user both will be in trouble. Below shows the plan how to reduce this problem. (compuquip, 2019)

**Solutions –**

1. Provide **Two-way** authentication when buy product.
2. Transmitted website data must be encrypted.
3. Use VPN to pass Confidential data.
4. To manage system used “Secure Sockets Layer” which will secure data transmission process
5. **Spyware, Virus-** Company has no e-commerce marketing facilities to promote their products just because of they are hosted by local ISP. Company marketing staff manually access via site portal to update products information. Company can be easily effected by spyware and virus because staff can access web portal from their pc or laptop, where they are not following any kind of internet access rules and are not controlled staff internet access. Staff can browse many sites and download files from untrusted or infected or malicious websites.Which is harmful for the company for that reason we have a plane to reduce that kind of risk. (kaspersky, 2019)

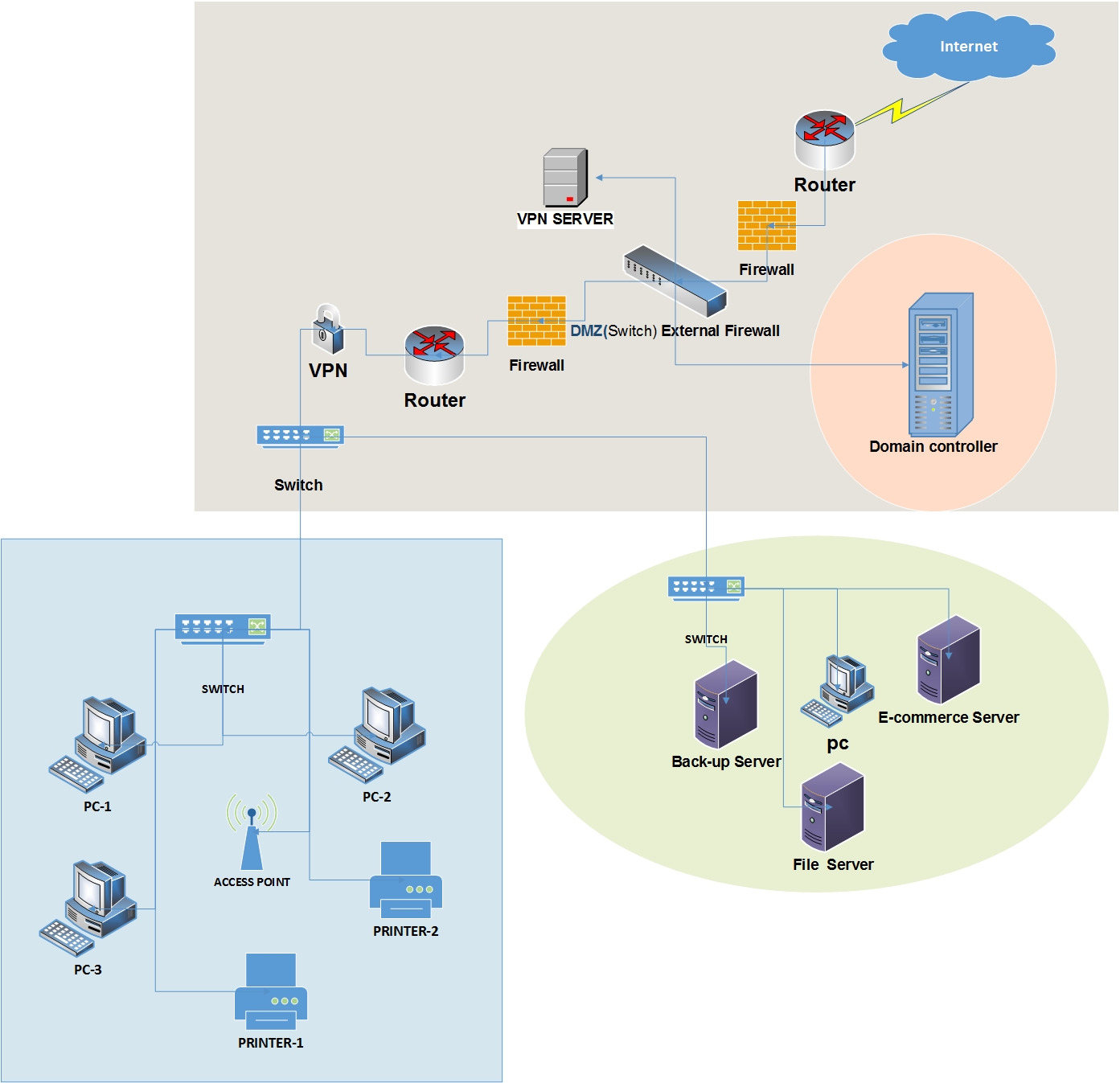
**Solutions –**

1. Blocked all the unexpected mails and links etc.
2. Control staff or employee Internet access.
3. Install all security patches and set password to access user pc or laptop.
4. All the staff PC or Laptop necessary software must be authorized software and up to date.
5. Regularly check security system to reduce vulnerabilities.
6. Obviously company needs an encryption method because the company run e-commerce business and store the customer information, also company financial and business information on the server, which is the most important data for the company and to protect from the hacker we must use encryption method to transmit data.

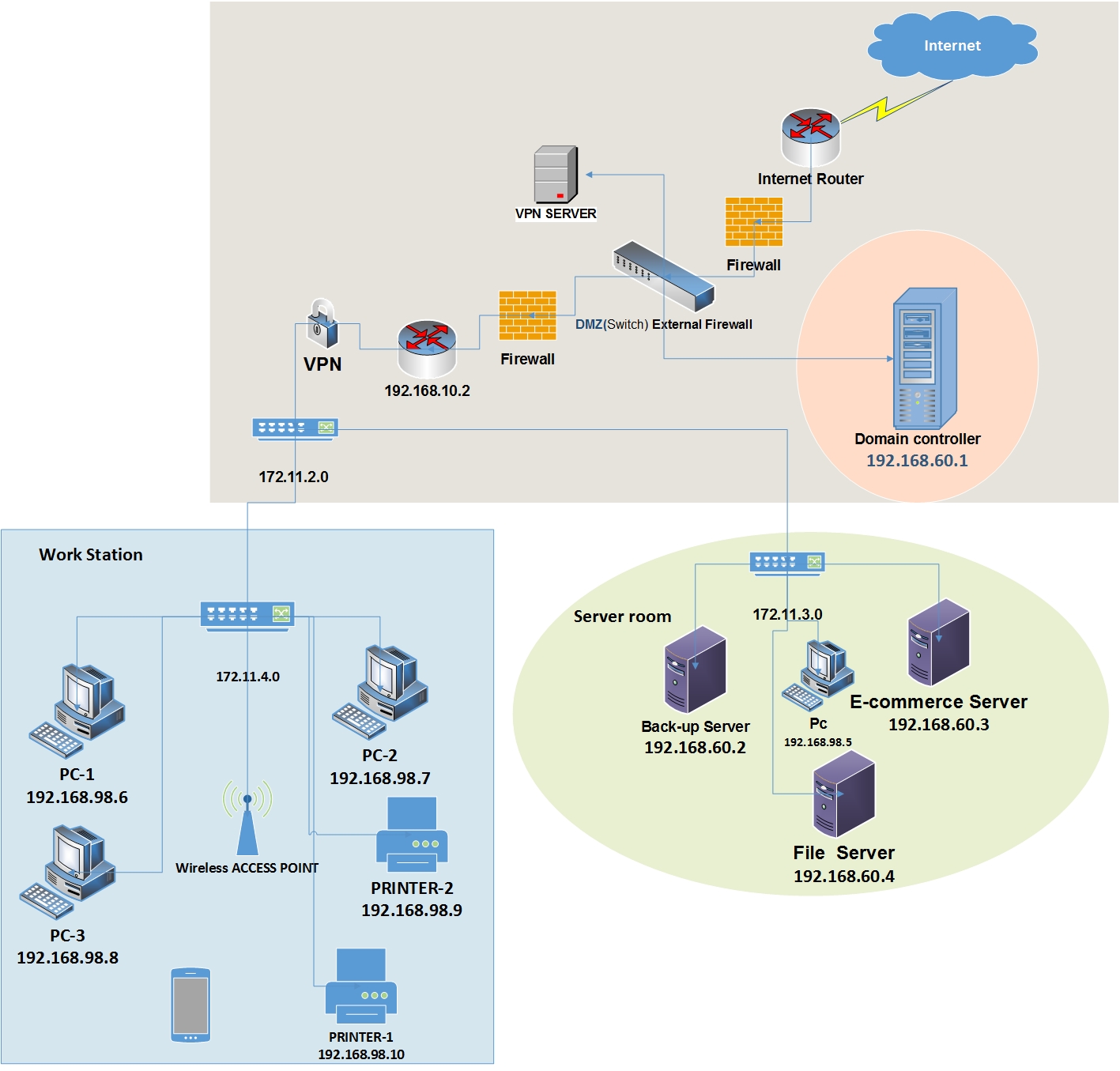
To protect perfect pet company data and authentication we can use AES, IPsec protocol, RSA algorithm and to set a more secure password we used hashing algorithm. For remote access and transmit data, we used VPN with AES algorithm where we set IP security, PPTP (point to point tunneling protocol), L2PT (Layer 2 tunneling protocol), SSTP and IKEv2.

For the data security in the storage 3DES algorithm will be used and also will be used symmetric and asymmetric encryption to store all the files and folder data.

**Task-3**

1. Below show a Network Diagram for ‘perfect pet’s’ company without IP Address-

**Figure-(1)-** Network Diagram without IP address

1. Below show a Network Diagram for ‘perfect pet’s’ company with IP Address-

**Figure-(2)-** Network Diagram with IP address

1. Perfect Pets company network diagram has been designed to reduce all the identifies risk, threats and security vulnerabilities. If we observed the network diagram which I suggest in task-3 (a), we can see that we used DMZ for online internal and external threats. To ensure secure data transmission when a customer buys a product and pay through online we used a VPN (Virtual Private Network) to transmit data.

For remote access management system using SSL (Secret Socket Layers) VPN (Virtual Private Network) system to block external access and only authorize users will be granted an access. Transmit data and Metadata will be encrypted to protect confidentiality and integrity through tunneling from external data theft and attacks at the time of data transmission over the internet.

* We are using a backup server to back-up all the important data for further safety. If incase damage any kind of data, then we get data from backup server.
* We are using file server to manage and store all the company confidential and financial and human resource information.
* We are using e-commerce server to maintain and store business, products and customer data. We also get the facility from e-commerce server to marketing company products which help to increases sell. All the server Protected by a Firewall.

So all the security required that I identify task- 1 & 2 are fulfill because we design network diagram for in house Hosting. Using in house hosting we can set up all the security needs what I want and reduce the risk. It also helps with customization, design and includes any time and provide many more facilities. Most important things we can customization User and Employee management system very easily and controls the access which helps to reduce vulnerabilities.

**Task-4**

1. After analyze the scenario we list down the threats and the risk to reduce “Perfect pet” company vulnerabilities. We design new network diagram to control and manage hole the business as well as we thought about the cyber security attacks that’s why we used SSL and DMZ to ensure the customer this e-commerce site and payment system are secured. Below show the necessary steps for company to ensure the security-
2. Company staff need Training to how the new system used in appropriate way.
3. Strictly follow the security policy for example- file-backup, removable disk using restriction.
4. Network devices both hardware and software should monitor every day.
5. Maintain access control policies for hardware and software.
6. Regularly check system software up to date are not as well as for hardware.

**Task-5**

1. I faced difficulties to analyze and design Network Diagram because if network diagram has any security vulnerabilities than the e-commerce site infected too many types of malicious attack from internet or other sources.

I identify the company security needs then implement the network security to following the data protection low, **encryption algorithm, VPN, DMZ, cryptography, authorization** and **authentication** and also take helps from internet and research about the security and data protection low.

1. If I could start again, First, I would research more deeply about the security method and data protection method and learn how to implement new network technologies for better experience and finally I will draw and develop the business system diagram.