Difficulties and risks associated with internet

ING Life Bo Sun CIS 505: CommunicationTechnologies Strayer University Darcel Ford, Ph. D. February 11, 2013 Difficulties and Risks Associated with Internet Originally, Internet was designed for absolute securityenvironment. Therefore, the protocols which are consisting of the infrastructure of Internet have no security concerns. This means Internet is easily to be vulnerable. Although major part of security issues are from inside, Internet does take external threats. When users connect the Internet, the web browsers might contain breaches that permit scripts to access the system and may cause damages potentially.

In addition, when information is transmitting through the public network, the transmission might be captured by someone else. This is known as man-in-the middle attack. (Dean, 2009) Another potential common risk associated with Internet is called reconnaissance threats. Attackers could detect the reachable networks, devices and services through the Internet connection, or even draw an entire network map. Furthermore, DoS attack is another risk users could encounter when using Internet. Hackers attempts to over-whelm the system in order to make it shut down. Oppenheimer, 2011) Analyze ING’s Solution The security mechanism existing in the current ING’s network is implemented a fire between the external brokers and the internal servers. Basically, this is not enough to protect the network, especially, the information of ING involves private personal information. The information should be protected carefully. Securing Internet connection a variety of overlapping security mechanisms will be equipped to guarantee the security of the Internet connection.

Common mechanisms include: firewalls, packet filters, physical security, audit logs, authentication and authorization. At the same time, technicians also need to implement packet filters to prevent the Internet routers from the DoS attacks. DoS attacks have great intimidation to public servers. In this condition, reliable operating system and applications are critical to solve the potential attacks. CGI and other types of scripts also could take care of the servers. Finally, firewall mechanism is efficient when facing Dos attacks.

Firewall technologies, physical security, authentication and authorization mechanisms, auditing, and possibly encryption consist of the security mechanisms utilized on remote access (Oppenheimer, 2011). Besides these normal network security mechanisms, a proper routing protocol is also important to Internet connection. The selected protocol should support route authentication. And static and default routing is an issue need to be concerned because of potential compromised routing updates. Finally, clear police and comprehensive training for the employee is significant.

After all, most security issues are leaded by human errors. Critique the Extranet Solution To support extranet connection for brokers is an excellent decision. It is simply for users to get access to the information which they needed. On the other hand, extranet is easily to be managed from the security aspect. Administrators could implement security mechanisms simply. Remote-access VPN is another way could be Implemented to connect the brokers. According to Oppenheimer, “ Reomte-access VPNs permit on-demond access to an organization’s internetwork, via secure, encrypted connections. (Oppenheimer, 2011) This function is suitable for the remote uses which don’t need always connection. Users connect the corporate’s

network through service provider’s network, this could decrease the budget of connection and the the work of network administritors. Install redundent mechanism could imprive brokers service. When primary database shut down, the backup devices could guarantee the network connection work normally. References Dean, T. (2009). network+ guide to networks. Mason: Cengage Learning. Oppenheimer, P. (2011). Top-down Network Design. Boston: Pearson Learning Solutions.