ENA FA3 20240091

Rhyno Botha

CTU TRAINING SOLUTIONS

Table of Contents

Section A:

Question 1:

1.1) It is quite unethical to use default configurations for networking services if those configurations have previously known security vulnerabilities. Default settings will make attacks very easily exposed to the network, putting users data and privacy at sever risk. Ethical considerations include the duty to protect sensitive data and minimize potential harm especially to users by addressing known vulnerabilities

1.2) There are three additional networking services, ethical considerations include:

- Security : Ensuring the new services are protected and shall never introduce vulnerabilities
- Privacy : Respecting privacy for all users by limiting data collection
- Transparency: Informing users about new services and their impact on data usage and security.

1.3) Malicious Intent : Malware distribution which has a purpose of phishing, identity theft, to try and deceive users

Privacy Violations: Violates the privacy of users by changing their intended communications and redirecting the users without getting any permission
From the users

Trust Erosion : Trust Erosion can cause harm to organizations by disrupting their access to services that doesn't intervene with internet infrastructure

1.4) Violation of Privacy: Consent is needed for monitoring infringes on users rights to privacy

Lack of transparency: Ethical practices require transparency, so users should always be told what is monitored and how their data is used.

Context Matters: Corporate Networks will always limit monitoring may be ethical if it is used for security or legal reasons

1.5) Privacy and Consent: Personal data is protected, obtain informed consent from guardians or caretakers.
Age-Appropriate Security: Security measures are suited to protect everyone under a specific age specifically from exploitation, such as parental controls and content filters

Data Minimization: Collect only limited amount of data that shall be necessary to provide the service

Transparency and Education: Always make terms of use and policies as clear as possible and easily understandable to children and adults aswell as educate these people on online behaviour that is deemed safe.

1.6) To balance functionality with risks:

- Risk assessment: Risk assessments will help to understand potential vulnerabilities and compare it to a new service
- Data Protection Measures: Implement strong data protection practices to minimize the overall impact of breaches that can potentially impact it in a negative way
- Informed Consent: Ensure users are constantly updated about risks and measures that are taken in the course of action to protect them.

1.7) No, it is not ethical at all to use third-party services without understanding their security protocols because of two factors:

- Responsibility : You are responsible for safeguarding your user's data and privacy with diligence and without it can put data at severe risk
- Trust : Users trust that you will ensure the services you integrate are secure and handle their data responsibly. Not investigating the third-party services breaches this trust.

Question 2:

2.1) No, an ISP throttling traffic without informing customers is immoral. Transparency is the ethical ideal that is being broken. Customers are entitled to know how their service is being handled, and traffic throttling that isn't disclosed to users may be interpreted as dishonest. Furthermore, if particular consumers are inadvertently exposed to worse service quality, fairness is undermined.

2.2) Among the ethical factors to take into account when routing traffic via nations with stringent monitoring regulations are:

- **Privacy**: Foreign governments may be monitoring user data, which might compromise their privacy.
- **Informed Consent**: If users' data is traveling via nations with stringent monitoring laws in place, they should be informed.
- **Security**: The security of sensitive data may be jeopardized by the possibility of data interception or disclosure to monitoring organizations.

2.3) Yes, it is legal as long as the distinction between services is made clear, it is commonly seen as ethical to give free customers with less features than premium users. Fair trade serves as the ethical guideline in this case: customers who pick a free service should be prepared to accept limitations, while those who pay for it should expect better performance. Transparency is vital, however, to ensure that customers understand the distinctions.

2.4) No, sacrificing security for QoS is immoral. Duty of care is the ethical precept that is being transgressed. Network administrators have a responsibility to ensure the integrity and confidentiality of data. Sacrificing security can lead to breaches, putting users' data at danger, and consequently, QoS should not come at the cost of security.

2.5) In general, locking clients onto proprietary technology is immoral as it goes against the idea of fair competition. Customers may be forced to pay more for upgrades or services as a result of vendor lock-in, which restricts their freedom of choice. Fairness and transparency are necessary to keep technological processes competitive and user-friendly.

2.6) No, it is immoral to oversell WAN services as it goes against the honesty principle. Deceiving clients about the quality of the service they would receive is dishonest and can erode their confidence. To uphold ethical standards, advertising must be truthful and service restrictions must be communicated clearly.

2.7)

- **Privacy**: There's a risk of unauthorized access or surveillance when transmitting sensitive information over public networks.

- **Security**: Sensitive data must be protected via secure protocols and encryption.
- **Compliance**: Confidential information handling requires adherence to legal and regulatory norms (such as GDPR or HIPAA) while conveying regulated data.

Question 3:

3.1) No, installing network infrastructure outside of a local area network (LAN) without appropriate security measures is unethical. Duty of care is the ethical precept that is being transgressed. It is the duty of organizations to prevent security lapses affecting its users, data, and networks. Adequate security is not implemented, putting sensitive data at needless risk to the system.

3.2) Yes, companies have to be transparent about the scope of their VPN surveillance and the logic behind it. Users must be aware of how their actions are being watched in order to comply with the ethical requirements of transparency and informed consent. In order for consumers to make educated decisions, it is critical that they understand how their data is handled and the precise goals of monitoring, such as compliance or security.

3.3) No, using less secure encryption techniques in order to save money is immoral. The duty of care and security principles are compromised by this. Users' data is at danger on a network that is susceptible to assaults due to weak encryption. The moral need to safeguard confidential data must never be compromised in favor of economical solutions.

3.4) No, denying workers access to internet tools without a valid reason is immoral. The ethical ideal of fairness is broken if access is denied without clear reasons. Nonetheless, limitations may be justifiable if they are based on safety issues or need to comply with laws, and staff members are made aware of this. To keep people's faith, it is imperative that these actions be implemented transparently.

3.5) The ethical considerations include:

- **Privacy**: Make sure the third-party gadgets don't gather needless data or jeopardize user privacy.
- **Security**: Make sure third-party devices' security procedures are thoroughly analyzed to make sure they don't add vulnerabilities and are in line with company requirements.
- **Accountability**: Even when employing devices from other parties, the company is still responsible for maintaining the security of its network.
- **Transparency**: Users should be made aware of the usage of third-party devices and the potential effects on or processing of their data.

3.6) Certainly, it can be morally acceptable for businesses to restrict VPN connections, particularly if doing so will protect the network or ensure that rules are followed. Nonetheless, consumers should be informed about the possible hazards connected with anonymous surfing as well as the reasons for VPN banning in order to uphold the ethical value of transparency.

3.7) No, it is immoral to impose stringent authentication requirements without taking disabled users' needs into account. The moral precepts of inclusion and equal access are broken by this. Ensuring that security measures do not disproportionately affect people with disabilities requires that they be built in a way that accommodates all users. Ensuring fairness in access necessitates offering accessible alternate authentication mechanisms.

References:

- Comer, D. E. (2018). *Internetworking with TCP/IP: Principles, protocols, and architecture* (7th ed.). Pearson.

- SANS Institute. (2020). *The importance of changing default settings on network devices*. https://www.sans.org/security-resources/

- Spinello, R. A. (2019). *Cyberethics: Morality and law in cyberspace* (7th ed.). Jones & Bartlett Learning.

- Tavani, H. T. (2011). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (4th ed.). Wiley.

- Kizza, J. M. (2017). *Ethical and social issues in the information age* (6th ed.). Springer.

Completed Declaration of Authenticity

I Rhyno Botha hereby

(FULL NAME)

declare that the contents of this assignment is entirely my ownwork except for the following documents: (List the documents and page numbers of work in this portfolio that were generated in a group)

Activity	Date

Signature: R.Botha Date: 2024/10/02