Collaborative Discussion 1 (Ethics and Morality)

Course: MSc Computer Science

Module: Software Engineering Project Management

Assignment: Collaborative Discussion 1 (Ethics and Morality) - Initial Post

Date: Saturday 12th March 2022

Student ID: 126853

Post:

The Rogue Services (Malware Disruption) case study provided by the Association of Computing Machinery highlights that despite contractual obligations to a client, an organisation should act ethically, following any Code of Ethics applicable to their sector (Such as the BCS Code of Conduct).

Rogue Services was a hosting provider that offered a ‘guaranteed uptime’ claim, which it believed should be upheld, even for their clients that were knowingly abusing this claim to host botnet controllers and browser-based exploit tools (ACM, 2018). A series of software vendors had come together to infect the network of Rogue Services and therefore take the service completely offline. Although an attack of this sort would have been considered ethically wrong, as they are acting for the greater good of society, it could be considered morally correct (Mitchell, 2018).

The table below shows the key points highlighted in the article, followed by the ACM and BCS Code of Ethics sections applicable.

Situation	ACM Code of Ethics	BCS Code of Conduct
Rogue Services knowingly allowing clients to host malware on their platform.	**Principle 1.1 –** Rogue Services were not acting in a manner that could be considered beneficial to the greater good of society.	**Principle 1 (Public Interest) –** Rogue Services were not acting in the public interest by allowing clients to host malware.

Principle 1.2 – Rogue Services allowed their clients to cause unjustified damage without mitigating the harm (Account suspensions etc.)

Principle 2.8 – Rogue Services were aware of their services being used for Malware Hosting, causing unauthorised access to computer systems.

Principle 3.1 – Rogue Services were not acting in a manner that could be considered beneficial to the greater good of society.

Principle 4 (Duty) – Rogue Services were acting in a manner that could bring themselves and other IT professionals into disrepute.

Security Vendors collectively infecting Rogue Services' network with Malware.	**Principle 1.1 –** Software Vendors were acting in the best interests of society in general. **Principle 1.2 –** Although software vendors were intending to cause harm to the Rogue Services platform, they were acting in a manner to avoid harm on a wider scale.	**Principle 1 (Public Interest) –** Software Vendors were working for the wider benefit of society and attempted to minimise the effect of their activities on third parties (Genuine clients). **Principle 4 (Duty) –** Software Vendors were acting in a manner to improve professional standards through a form of guerilla IT enforcement.
Security Vendors malware deleting the data of Rogue Services' clients.	**Principle 2.8 –** Although the Software Vendors had tried to limit the extent of their damage to Rogue Networks itself, a large number of their customers were genuine e-commerce users. Data held by these customers	**Principle 1 (Public Interest) –** Software Vendors did have due regard for the rights of third parties, however, they did not provide the mechanism for legitimate parties to object to data deletion.

	could have been mistakenly deleted as part of the attack.

References:

ACM. (2018) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 12th March 2022].

Mitchell, J. (2018) Ethics vs Morality. Available from: https://www.bcs.org/articles-opinion-and-research/ethics-vs-morality/ [Accessed 12th March 2022].

Screenshot:

Kieron Holmes

Initial Post

3 secs ago

The Rogue Services (Malware Disruption) case study provided by the Association of Computing Machinery highlights that despite contractual obligations to a client, an organisation should act ethically, following any Code of Ethics applicable to their sector (Such as the BCS Code of Conduct).

Rogue Services was a hosting provider that offered a 'guaranteed uptime' claim, which it believed should be upheld, even for their clients that were knowingly abusing this claim to host botnet controllers and browser-based exploit tools (ACM, 2018). A series of software vendors had come together to infect the network of Rogue Services and therefore take the service completely offline. Although an attack of this sort would have been considered ethically wrong, as they are acting for the greater good of society, it could be considered morally correct (Mitchell, 2018).

The table below shows the key points highlighted in the article, followed by the ACM and BCS Code of Ethics sections applicable.

Situation	ACM Code of Ethics	BCS Code of Conduct
Rogue Services knowingly allowing clients to host malware on their platform.	**Principle 1.1** – Rogue Services were not acting in a manner that could be considered beneficial to the greater good of society. **Principle 1.2** – Rogue Services allowed their clients to cause unjustified damage without mitigating the harm (Account suspensions etc.) **Principle 2.8** – Rogue Services were aware of their services being used for Malware Hosting, causing unauthorised access to computer systems. **Principle 3.1** – Rogue Services were not acting in a manner that could be considered beneficial to the greater good of society.	**Principle 1 (Public Interest)** – Rogue Services were not acting in the public interest by allowing clients to host malware. **Principle 4 (Duty)** – Rogue Services were acting in a manner that could bring themselves and other IT professionals into disrepute.
Security Vendors collectively infecting Rogue Services' network with Malware.	**Principle 1.1** – Software Vendors were acting in the best interests of society in general. **Principle 1.2** – Although software vendors were intending to cause harm to the Rogue Services platform, they were acting in a manner to avoid harm on a wider scale.	**Principle 1 (Public Interest)** – Software Vendors were working for the wider benefit of society and attempted to minimise the effect of their activities on third parties (Genuine clients). **Principle 4 (Duty)** – Software Vendors were acting in a manner to improve professional standards through a form of guerilla IT enforcement.
Security Vendors malware deleting the data of Rogue Services' clients.	**Principle 2.8** – Although the Software Vendors had tried to limit the extent of their damage to Rogue Networks itself, a large number of their customers were genuine e-commerce users. Data held by these customers *could* have been mistakenly deleted as part of the attack.	**Principle 1 (Public Interest)** – Software Vendors did have due regard for the rights of third parties, however, they did not provide the mechanism for legitimate parties to object to data deletion.

References:

ACM. (2018) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 12th March 2022].

Mitchell, J. (2018) Ethics vs Morality. Available from: https://www.bcs.org/articles-opinion-and-research/ethics-vs-morality/ [Accessed 12th March 2022].