Employee received an email from an unknown source, in which the attacker claimed that the user owes a ransom and that their data was presumably stolen. The employee rightfully thought it was spam and deleted the email.

The next day the employee got another email from the same sender that increased the ransom amount, and they included a sample of the stolen data in the email. Which caused the user to send a message to the security team.

This happened across December 22 - 28 of 2022.

The issue was found to be an e-commerce web application vulnerability, which allowed the attacker to get access to the users personal information, by modifying a URL string. The logs on the website indicated that the attacker gained access to information on thousands of pages.

The organization communicated the data breach to its customers.

It is recommended to perform a routine of vulnerability scans, and implement a way to block all requests outside of the URL's range, and ensure that every user on the website is authenticated.