Jisc CSIRT use of NetFlow data

Jisc processes NetFlow data collected on various routers within the Janet network. This NetFlow data is used in planning, network operations, research and security incident response, and is considered necessary to effectively complete some of the tasks involved in these areas.

NetFlow describes the source and destinations of network traffic and some of the IP layer attributes of the data. It can be thought of as similar to an itemised phone bill, and is considered to be communications data. Jisc is not able to link an IP address to the person using it. We may be required to disclose this data to law enforcement and other authorities in response to a notice under specific legislation.

The NetFlow data is collected at a number of points on the network; within the core, regional networks, and at external connectivity. With the permission of a connected organisation, NetFlow data may be collected from the edge of their network or Janet managed router. This coverage may not provide a complete view of all traffic on Janet. In many instances the collection of NetFlow on a router is resource intensive, and the routing of IP traffic takes priority and the data collected may only be a sample of the actual data. Jisc collects large volumes of data and storage facilities are typically limited to 90 days of NetFlow data. Due to configuration changes, network and equipment failure, the stored records of NetFlow may not be complete within that period. As stated in the Jisc Security Operations Centre Data Protection Impact Assessment [1], some data relating to cyber security incidents may be retained for up to three years.

Information is processed in accordance with the *Data Protection Act 1998* along with the *General Data Protection Regulation (GDPR) (EU) 2016/679*. Under particular circumstances it will be necessary to process this information independently and share this information with third parties. Where possible this will take the form of a statistical analysis or anonymised data, but in some cases (e.g. security incidents) this will not be possible if the information is to be of use to the third party.

If you are exporting NetFlow data to us from your network, there is a risk that a misconfiguration or error at the point where the NetFlow is exported may result in NetFlow data pertaining to traffic not destined for Janet being sent to us. If we become aware of this, we will delete the data as soon as possible.

Links
[1] https://repository.jisc.ac.uk/8433/1/jisc-security-operations-centre-dpia-may-2021.pdf