O2 network outage

Decision to conclude investigation into Telefónica UK Limited's compliance with section 105A(4) of the Communications Act 2003

Case reference: CW/01235/12/18

Issue date: 1 November 2019

Contents

Section

1. Overview 1

2. The network outage 4

3. Summary of investigation and conclusions 5

4. Lessons for providers 8

1. Overview

The network of mobile operator O2 experienced an outage in December 2018 affecting all O2 customers.

Ofcom opened an investigation to examine whether O2 had taken all appropriate steps to protect, so far as possible, the availability of its network.

O2's outage was significant, lasting for almost 23 hours and affecting all of O2's 25 million direct customers as well as other connections – for example connections to other mobile virtual network operators – across the Telefónica UK network.

At times during this period, people were unable to access their mobile data, make calls or receive messages. Mobile outages on this scale can cause significant disruption for mobile users, so it is important for Ofcom to investigate them thoroughly.

This document sets out a summary of our conclusions, including lessons that the industry can learn from the nature of the incident.

What we have concluded – in brief

- As reported at the time of the incident, the disruption to O2's network was caused by an issue with software provided by Ericsson. A fault in this critical software, linked to the expiry of a 'security certificate', caused the software to fail and disrupted O2's network.
- After reviewing a substantial body of evidence gathered in our investigation, we did not find that O2 had contravened its obligations.
- We have concluded that, in the specific circumstances of the case, O2 had taken all appropriate steps to protect the availability of its network; and it acted appropriately to restore it. We have therefore decided to close our investigation.
- However, this incident highlights that risks to, and vulnerabilities of, communications networks continue to evolve. While Ofcom has not found a breach in this particular case, it is important that providers keep pace and continue to develop and ensure availability of their services.

Summary of lessons for providers

- In light of this incident, and the specific lessons we have identified from it, we expect all providers to reflect on the steps they are taking to protect the availability of their network and services, particularly where reliance is placed on third party suppliers.
- Ofcom Guidance makes clear that outsourcing elements of a network to a third party does not excuse a network provider from its obligations.
- The circumstances of this specific incident show that, if not implemented and managed correctly, security certificates in general, and especially hardcoded security certificates, can cause software to fail. In worse case scenarios, this can render a network unavailable.
- In future, we will expect providers to be able to demonstrate that they have proactively engaged with suppliers and sought specific and appropriate assurances that they have appropriate certificate implementation and management policies in place; and in relation to critical software, adherence with these policies has been monitored throughout the software development lifecycle; any exceptions are documented and reviewed at the appropriate level; and the implementation and management has been carefully tested to manage the risk of affecting network availability.
- In response to this incident, we are now asking relevant questions of providers through our Security and Resilience Assurance Scheme. This initiative is enabling us to establish an understanding of security and operational resilience issues among providers.
- We expect to accumulate industry learnings through our engagement with providers, as well as from individual incidents as they occur. We also intend to update our guidance to reflect these learnings.

1.1 People are increasingly reliant on communications infrastructure, and operators have obligations under section 105A(4) of the Communications Act 2003 to protect the availability of their network, so far as possible.

1.2 Ofcom has issued guidance setting out its expectations of providers to meet these obligations.[1] These obligations are particularly important because of the changing nature of security and resilience risks.

1.3 In December 2018, O2 notified Ofcom of an incident affecting data services on its network. As this was a significant outage affecting the availability of O2's national network to its customers, we decided to open an investigation to assess whether O2 had complied with its section 105A(4) obligations.

1.4 Taking into consideration the substantial body of evidence gathered in our investigation, we did not find that O2 had contravened its obligations.

1.5 We concluded that, at the time of the incident and in the light of the specific circumstances described below, O2 had taken all appropriate steps, so far as possible, to protect the

[1] We have published high level guidance to providers of public electronic communications networks or services (CPs) on their security and resilience obligations under sections 105A and 105B of the Communications Act 2003 (CA2003).

availability of its network. O2 acted appropriately given challenging circumstances in response to the incident to restore network availability to its customers.

1.6 However, this incident highlights that the risks to, and vulnerabilities of, communications networks continue to evolve. While Ofcom has not found a breach in this particular case, it is important that providers keep pace and continue to develop and ensure the availability[2] of their networks and services.

1.7 Following the specific circumstances of this incident, we note that security certificates, especially if hardcoded, have the potential to cause software to fail. This can, in worst case scenarios, render a network unavailable.

1.8 Ofcom Guidance makes clear that outsourcing elements of a network to a third party does not excuse a network provider from its obligations under section 105A(4).

1.9 In light of this incident, and the specific lessons identified in Section 4, we expect all providers to reflect on the adequacy and effectiveness of the steps they are taking to protect network and service availability, particularly where reliance is placed on third party suppliers.

1.10 Additionally, as part of Ofcom's Security and Resilience Assurance Scheme, established earlier this year, we now specifically question providers on how they use and manage the expiry of security certificates within their systems, to help pinpoint any potential problems.

[2] In this document, we use "availability" to refer to the continuity of supply of services provided over the network.

2. The network outage

The Incident

2.1 On 6 December 2018, in line with its obligations under section 105B of the Communications Act, 2003, O2 notified Ofcom of a network outage affecting its 2G, 3G, and 4G Data services in the UK. On 10 December 2018, the O2 CEO wrote to Ofcom with further details about the incident. In summary:

2.2 At 4:30am on 6 December 2018, O2 suffered a major outage affecting its 2G, 3G and 4G data services. The outage affected O2's UK customers and the customers of O2's Mobile Virtual Network Operators (MVNO) partners.

2.3 As reported at the time of the incident, the disruption to O2's network was caused by an issue with 'SGSN–MME' software provided by Ericsson. [3] A fault in this critical software, linked to the expiry of a security certificate at 04:30 on 6 December, caused the software to fail and disrupt O2's provision of network service.[4]

2.4 O2 worked with Ericsson's technical support team to manage the incident and restore network availability. 2G and 3G services were restored by 9:30pm. 4G services started being restored at 11:30pm and were complete by 3:12 am on 7 December 2018. The action taken by O2 to manage the incident and restore network services is set out below.

O2's response to the Incident

2.5 In response to the incident, O2's Major Incident Management Team was engaged at 04:50am - within 20 minutes of the initial incident - to invoke incident management procedures. Progress was reported to the Telefónica UK Board Major Incident Management team meetings, chaired by the CEO.

2.6 Having engaged these procedures, O2's technical teams were tasked with investigating and resolving the incident. This involved establishing communication 'bridges' to Ericsson to understand the cause of the incident, and identify appropriate actions to restore availability of services.

2.7 To avoid potential network congestion, or overload of the network, some phone and text services were affected as data services were gradually restored.

[3] Critical software used by O2 in its communications network to manage the mobility of users' service connections. Details of the product are available on Ericsson's website.
[4] https://www.ericsson.com/en/press-releases/2018/12/update-on-software-issue-impacting-certain-customers

3. Summary of investigation and conclusions

3.1 This section sets out a summary of our reasons for concluding that O2 has not contravened the requirements of s105A(4) under investigation.

Opening the investigation

3.2 After conducting an initial assessment of the circumstances of the December 2018 incident, it was evident that network availability had been impacted. We therefore opened an investigation to examine whether O2 had contravened its obligations under s105A(4) of the Act.

3.3 Specifically, we examined whether O2 had met the requirements of network providers to take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

Evidence we reviewed

3.4 Under statutory powers[5] we required O2 to provide information to inform our assessment of the case. We also engaged with Ericsson, as the third-party supplier to O2 of the software which failed and triggered the network outage. A substantial body of information was provided to us in response.

3.5 While the incident was triggered by a failure in software provided by a third party, Ofcom guidance[6] is clear that outsourcing to third parties does not excuse network providers from their obligations. For example, at paragraph 3.52, the Guidance states that:

3.6 'We do not consider that outsourcing to third parties in this way excuses CPs from their obligations under 105A(4). Put simply, a CP cannot contract out of its statutory obligations. As such, they should have sufficient levels of contractual control over third parties in place to ensure they continue to comply with their obligations. We also expect CPs to continuously and rigorously check that actions undertaken on their behalf do not put them in breach of their obligations.'

3.7 We expect communications providers to have sufficient levels of contractual control over third parties in place to ensure they continue to comply with their obligations. We also expect CPs continuously and rigorously to check that actions undertaken on their behalf do not put them in breach of their obligations.

3.8 From the evidence gathered, we note that prior to the incident, O2 had taken a number of steps to protect against a network outage.

---

[5] Information about our statutory powers for information gathering is set out in paragraphs 3.15 to 3.18 of our published Enforcement Guidelines for regulatory investigations.

[6] See, for example, paragraphs 3.12 and 3.52 of our guidance on security requirements.

3.9 Based on the evidence reviewed and in light of the specific circumstances described below, we concluded that O2 had taken appropriate steps to establish sufficient contractual controls and put in place testing procedures, in order to assess and protect against risks to the availability of its network from the supply of Ericsson's SGSN-MME software.

3.10 At the time of the incident, O2 had in place a contractual agreement with Ericsson which included conditions for the testing and acceptance of supplied products and specifications for the supply of SGSN-MME software.

3.11 In the context of this contractual framework, O2 had established standard protocols and processes for testing of software provided by third parties. We consider these processes to have been robust.

3.12 While testing protocols were in place, we note that they did not prevent this incident from occurring. We understand the incident to have been triggered by the expiry of a hardcoded security certificate embedded within the SGSN-MME software provided by Ericsson. Neither the hardcoding of the certificate, nor the issues with the software were, at any time prior to the incident, brought to O2's attention as a potential risk to the effective functioning of the software.

3.13 The testing protocols in place for acceptance of new software were not designed to identify errors of this specific and unprecedented nature within a supplier's software development process. We note that the coding errors were not known to O2 and therefore not subjected to further scrutiny or testing.

3.14 In the circumstances of the incident under investigation, we do not consider that prior to the incident it would have been technically and/or commercially feasible for O2 to have taken additional steps to identify and implement further preventative controls against the risk of this incident occurring.

3.15 We do, however, with hindsight consider there to be lessons from this incident that O2 and other providers should take account of. We have set these out in Section 4 of this Decision.

3.16 Ofcom guidance states that it is important that Communications Providers have clear lines of accountability and sufficient technical capability to ensure that potential risks are identified and appropriately managed.[7] In our investigation, we have also taken into account the appropriateness of the accountability and expertise of O2 to provide proper management of risks.

3.17 O2 operates a corporate risk management policy and supporting processes, designed in line with international standards, to assess and manage potential risks. This approach includes the identification of risk owners responsible for the identification and assessment of risks.

3.18 We consider O2 to have had clear lines of accountability and sufficient technical capability to identify and manage potential risks to the availability of its network. O2 identified individuals who were responsible for identifying and assessing risks. We note that these

[7] Set out in paragraphs 1.4, and 3.9-3.12 of our guidance on security requirements.

lines of accountability and technical capability were especially evident in O2's response to the incident and its restoration of network availability.

3.19 As set out in Section 2 of this Decision, O2 swiftly engaged its Major Incident Management Team to manage the incident once identified. Working with Ericsson, O2 restored full service to its network within 24 hours. The unusual nature of the root cause of the incident meant it took around 12 hours before a successful fix was identified. Following this, due to the extent of the incident - affecting multiple systems and nodes supporting O2's network - we recognise that the phased restoration of service availability over time was necessary to avoid potential network congestion and/or overload and potentially further failures.

3.20 We note that, in response to this incident, O2 engaged with its affected customers and issued goodwill credits to those affected.

3.21 We also note that O2 cooperated fully with our investigation.

Conclusions

3.22 We have concluded that, in the light of the specific circumstances described above, O2 took all appropriate steps, so far as possible, to protect the availability of its network. This includes the steps O2 had taken prior to the incident, and those it took in response to the incident to restore network availability.

3.23 Our assessment also considered the "state of the art within the industry", as required by relevant EU legislation.[8]

3.24 We note O2 had an appropriate approach to risk management, an established contractual agreement with its supplier, and conducted rigorous testing of supplied software.

3.25 We are satisfied that O2 had appropriate lines of accountability and sufficient technical capability to manage potential risks to the availability of its network. In response to the incident, we consider O2 to have acted appropriately, in conjunction with Ericsson, to manage the disruption to network service and restore availability.

3.26 Given the complexity of the incident and the unprecedented circumstances, we consider that O2 took appropriate and timely measures to restore availability appropriate to the needs of its customers. We do not consider that prior to the incident it would have been technically and/or commercially feasible for O2 to have taken additional steps to identify and implement further controls to protect against the risk of this incident occurring.

3.27 We do, however, with hindsight, consider there to be lessons from this incident that O2 and other providers should take account of. We have set these out in Section 4 of this Decision, below.

[8] Article 13a(1) of Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended .

4. Lessons for providers

4.1 Section 105A(4) of the Act sets out the obligations of providers of public electronic communications networks to maintain network availability so far as possible.

4.2 These obligations are particularly important because of the changing nature of security and resilience risks and the increasing extent to which people depend on communications infrastructure.

4.3 We will continue to consider security and resilience incidents that are notified to us – which providers are obliged to do under Section 105B of the Act – and whether these give us cause to undertake further enforcement action.

4.4 We make decisions about whether to open investigations on a case-by-case basis, having regard to our statutory duties and having considered all the matters that appear to us to be relevant to whether or not we should do so. In doing so, we seek to exercise our discretion to target our action at the cases we think are most likely to produce good outcomes for citizens and consumers.

4.5 While Ofcom has not found a breach in this particular case, there may nonetheless be other instances when, having examined the information available, we conclude that a network provider has failed to comply with its obligations under the Act.

4.6 Ofcom guidance[9] is clear that outsourcing to third parties does not excuse network providers from their obligations. We expect providers to have taken all appropriate steps, so far as possible, to protect network availability. This includes, but is not limited to:

- having in place sufficient levels of contractual control over third parties;
- checking continuously and rigorously that any actions undertaken by third parties on their behalf do not put them in breach of their obligations – for instance, by establishing appropriate technical controls, change processes and testing; and
- having clear lines of accountability and sufficient technical capability to ensure that potential risks are identified, understood and properly managed.

4.7 We expect providers to have carefully considered their own approach to protecting network availability, particularly where reliance is placed on third party suppliers.

4.8 The circumstances of this specific incident show that, if not implemented and managed correctly, security certificates in general, and especially hardcoded security certificates, can cause software to fail, and that this can, in worse case scenarios, render a provider's network unavailable.

4.9 In future, we will expect providers to be able to demonstrate that they have proactively engaged with suppliers and sought specific and appropriate assurances that:

- they have appropriate certificate implementation and management policies in place; and

[9] See, for example, paragraphs 3.12 and 3.52 of our guidance on security requirements.

- that, in relation to critical software, adherence with these policies has been monitored throughout the software development lifecycle, any exceptions are documented and reviewed at the appropriate level, and the implementation and management has been carefully tested to manage the risk of impacting network availability.

4.10 Ofcom launched its Security and Resilience Assurance Scheme in February 2019. This initiative is enabling us to establish an understanding of any security and operational resilience issues among providers. In light of this incident, we now include specific questions for providers about how they use security certificates within their systems and how they manage their expiry.

4.11 We expect to accumulate industry learnings through our engagement with providers, as well as from individual incidents as they occur. We intend to update our guidance to reflect these learnings in due course.