T2RL Analysis
August 2024

Protection from a CrowdStrike

Introduction

On 19 July 2024, IT security vendor CrowdStrike released a software update to its vulnerability scanner, Falcon Sensor. The update was flawed and resulted in around 8.5 million computers running Microsoft Windows being disabled. The impact was felt across many industries including airlines and airports. Initial estimates suggested that around 50,000 flights were delayed and 5,000 cancelled altogether but these have been revised upwards in the following days. Delta Air Lines alone reports 7,000 flight cancellations so far. Estimates of financial losses due to the incident ran as high as five billion dollars across the global economy.

Impact of the CrowdStrike Incident

T2RL has little to add to the analysis of the proximate causes of the incident that have been published by more specialist outlets. A good explainer may be found on this YouTube video. Of far more interest to us is how an incident like this affects airlines using technology that may or may not be impacted by a general IT problem.

The main commercial systems of traditional airlines used to be based on mainframe computers and proprietary networks. While this brought its own share of challenges it did mean that airlines benefitted from security by obscurity. Put simply, bad actors were very unlikely to have the knowledge and skills necessary to attack airline systems or even to gain access to them. Similarly a technical issue with Windows or Unix would not directly impact airline booking or check-in systems. None of this is true in 2024.

In recent decades airlines have largely abandoned in-house computer systems in favour of software as a service (SaaS) provision from specialist vendors[1]. The mainframes used by those vendors have been wholly or partially replaced by more

[1] There are of course exceptions like United Airlines and Delta Air Lines in the USA and others including easyJet, Aer Lingus and Turkish in Europe.
Protection from a Crowdstrike

modern “open systems” platforms and provision of those open systems has been switched away from dedicated data centres to the cloud networks of Amazon, Microsoft and Google. As part of that switch the specialised networks such as SLC and AX-25 that were unique to the airline industry have been superseded by more generic networks based on internet standards. All of these changes have brought benefits but they also have the effect that airline technology provision has moved from being a somewhat obscure backwater to being firmly part of the mainstream. Not only are the central systems reliant on common components but so are the networks by which they are accessed. Sometimes this means that even if an application system escapes an outage it may be a moot point because access to it is unavailable. As a result an event like the CrowdStrike incident impacts airlines and airports as significantly as it affects sectors such as banks, retailers and governments. The big question for airline executives now is how to mitigate a set of risks that it has in common with every other part of the economy.

Paths to Mitigation

There are two broad paths to the mitigation of an event such as this. The first is about trying to ensure that its impact on the airline’s services is minimised. The second is concerned with securing compensation in the event that the first line of defence is breached. Ultimately both avenues are dependent on the contracts negotiated between the airline and its IT provider(s).

The First Line of Defence

Since 1990 professionals working on the enhancement of safety in many industries, including airlines, have referred to the Swiss Cheese model of defence[2]. In that description an organisation's defences against failure are depicted as a series of imperfect barriers, represented as slices of cheese. The holes in the slices correspond to weaknesses in individual parts of the system and are continually varying in size and position across the slices. The system produces adverse events when a hole in each slice momentarily aligns, permitting a hazard to pass through all of them, leading to a failure.

The same thinking may be applied to the provision and maintenance of technology systems. Some of the following provisions, which are covered by ITIL Version 4[3], may be deployed to protect the integrity of systems, especially when changes are being made:

- Provision of multiple operational environments such that there is no single point of failure
- Testing regimes for hardware and software changes that include performance, operation and regression
- Auditable documentation of testing undertaken
- Release Management - to ready software for release ensuring impacts are mitigated before deployment.
- Deployment Management - Enabling the production software for customer consumption at a time and in a manner agreed with the customer airline.

These measures and others should be included in the contract for services provision. In many cases there will be a reciprocal responsibility on the airline to avail of the

[2] Originally formally propounded by James T. Reason of the University of Manchester,

[3] Information Technology Infrastructure Library (ITIL) is a set of practices and a framework for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of the business

Protection from a Crowdstrike

information and facilities provided to monitor its use of the services. It is essential that airline organisations understand and fulfil their own part of the bargain.

Achieving Redress

When, despite all the provisions made for system integrity, a failure still occurs airlines should be able to obtain redress from their service vendors. It is critically important that vendors are not able to shelter behind conditions in their own contracts with suppliers. While this has always been the case it is growing in importance as provision of IT services from the cloud is now the most common model. The contract between cloud provider and SaaS vendor may include less demanding service levels than that between the vendor and the airline. It is incumbent on the SaaS vendor to use the capabilities of the cloud provider, such as multiple instances across diverse regions, to achieve better levels of reliability than the baseline. The airline's contract must provide sufficient protection with no language that limits the vendor's liability to a pass-through from the cloud platform.

Contractual service levels should apply equally to the availability of services and any extended outages. Incident recovery time provisions should incentivise providers to deploy new releases of the services or software with due regard to the need for testing and the ability to fall back changes cleanly if necessary.

Failure to deliver against quality assurance requirements should normally reflect a material breach of contract or agreement, which extends liability beyond any liability cap.

Contract Negotiation

The time to consider potential impacts of an incident like the CrowdStrike outage is when negotiating contracts. T2RL has worked on around 200 technology procurement exercises with airlines from around the world. Fundamental to our process is the principle that airlines specify their requirements and once a vendor agrees to any provision it is incorporated into a contract. Much attention is paid to functional requirements and indeed a large PSS contract will have many thousands of individual functional specifications. However, non-functional requirements (NFRs) should be considered an essential part of the process.

Effective contractual language around service management and service levels and process brings multiple benefits. On the one hand it obliges vendors to implement processes that are likely to protect the airline from adverse effects and on the other it ensures that they are able to obtain redress in the event of that protection failing.

T2RL Travel Technology Research Ltd, is an independent sourcing and research company that specializes in airline technology and distribution. Based on data since the year 2000 it has tracked industry trends for airlines as well as their IT providers, distribution partners, and customers. All parties use its research to make informed business decisions to meet current and future needs. For further information, visit our website at www.t2rl.com.