Hackney Council’s approach to moving to a cloud-first model from the PSN

This case study is part of guidance on moving to modern network solutions and away from legacy networks.

Objective

The London Borough of Hackney wanted to migrate as many of its services as possible from the Public Services Network (PSN) to the internet. Hackney wanted to use the internet to provide:

- an easier and a more convenient user experience
- a more secure and cost effective way of sharing data with other organisations
- its IT team with a way to constantly monitor compliance and network security to manage issues instead of waiting for scheduled checks like penetration tests

The migration included moving email to Google’s G Suite.

Background

Hackney used the PSN to:

- let staff connect to the Joint Asset Recovery Database (JARD) – a national database used by financial investigators, prosecutors and enforcement staff
- let staff send email using gsi.gov.uk addresses
- run the Domain Name System (DNS) to support JARD and email
- access Department of Work and Pensions (DWP) services
- provide onward connectivity to the NHS Health and Social Care Network (HSCN)

Hackney still uses the PSN to access JARD and services like Blue Badge.

How Hackney moved to the internet

The council moved away from government .gsi email domains and implemented Transport Layer Security (TLS) in response to the securing government email guidance and upcoming decommission of the GCSx email service.

Hackney's IT department has around 100 staff, supporting 3,500 users across the council, and occasionally uses third-party suppliers. The team had lots of experience so all migration activity was carried out in-house.

Hackney now forces a TLS connection to all the main public sector domains (gov.uk, police.uk, nhs.net, mod.uk, cjsm.net). If an email fails to deliver, the sender would get a non-delivery report, but the IT team has not seen this happen. Hackney staff know they should contact their internal service desk if this happens so they can get help to try again or use a different route.

The IT team is now working to further enhance their security practices through introducing a 'red team' approach. The team will proactively scan the external interfaces of services and imitate the steps a hacker might take to gain access to identify risks so that mitigating actions can be taken swiftly.

Hackney also uses the National Cyber Security Centre's (NCSC's) Mail Check and Web Check tools, which help increase security across government by providing additional assurance against services that Hackney presents externally.

Hackney is also working to provide access to on-premise services, such as their intranet, service desk portal, and finance system, using the internet, via any standard browser. This will allow users who authenticate themselves successfully to access services from anywhere. If a corporate service presented over the internet allows offline access, then users will require a trusted device.

Challenges of migrating to the internet

One of the biggest challenges of migrating to the internet is managing a centralised identity and authentication approach. Hackney would like to encourage interoperability. However, this is only possible with systems that are designed to work with open standards.

For example, Hackney would like to help staff access legacy applications from anywhere with a single sign-on with Microsoft Internet Information Services (IIS) over the web.

Hackney introduced a reverse proxy to:

Before plugging any service into its Security Assertion Markup Language (SAML) authentication solution, the team first have to add the service to their identity provider to authenticate users. In some cases, this procedure will only work if no other backend requests are made through the service using old authentication types. If the service uses old authentication types

like NTLMv2, it’s possible to end up with a situation where users can successfully authenticate to what is now a broken service.

The IT team will now require all future services to support the SAML protocol or Open Authorisation (OAuth) for end user authentication and access control. However, many of Hackney’s legacy services do not support these. The council took a couple of approaches to protecting these services while still providing them to the internet by using:

- multi-factor authentication for all internet facing services storing OFFICIAL information
- a cloud identity service to simplify the end user experience

Hackney tried to use a native web application to present legacy applications. If that is not possible they use VMware to present a Windows application, or virtual desktop infrastructure if the application still needs to integrate with other Windows services.

In all cases, the team still present everything through HTML5 so it feels more like a web service to end users.

Benefits of the migration

Since migrating away from the PSN to the cloud, Hackney Council has:

- improved reliability and provided more flexible services for end users
- started to remove PSN-related infrastructure, which is helping to reduce data centre costs and IT administration effort
- improved security through mandating industry standard security controls and NCSC guidance

Lessons learned from the migration

Hackney found it valuable to run planning workshops to help:

- agree key principles
- talk about proposed solutions
- avoid forcing preconceived ideas and plans onto teams

- highlight the benefits of the migration to the cloud
- get buy-in from across the organisation

The team found that getting backing from an impartial source like a Chief Technology Officer or a senior architecture colleague was important. This made sure the project was supported effectively and was not seen as just a security-led activity.

During the migration, Hackney found some suppliers had not yet caught up with the way government now approaches technology and security. The council had to push some vendors to use open standards and provide cloud-based solutions. For example, Hackney wanted cloud-connected printers but found this difficult to explain to some suppliers and is still in the middle of procuring these.

Outcomes of the migration

Hackney switched to a cloud-based email service by following the GOV.UK secure email guidance. This process took about 4 months after the business case and budget was approved. Most of the migration complexity centred on deciding if archive mailboxes and distribution lists were still needed.

Hackney holds a current PSN compliance certificate and will continue to use the PSN for services such as Blue Badge and connecting to DWP for policy updates and queries on revenues and benefits.

The council will continue to migrate to web and mobile technologies as part of its adoption of a zero trust architecture.

For more information on how to migrate to modern networks you can email psnservicedesk@digital.cabinet-office.gov.uk.