Considerations VA Printing’s External Connections (RCEC)

Hi Management Team and Information Security Team

I am trying to share my considerations and findings in a more timely manner to allow you to make better decisions.

The information security team requires software applications only for internal users have no traffic via Internet unless necessary. Specifically for Azure cloud applications, we are required to limit the traffic between Azure Vnet (private endpoint) and Corporate network(ExpressRoute).

While we fully appreciate the requirement /recommendation/risk identification from the Information Security Team, currently connection from Express Route to Azure Vnet is unfeasible because our infrastructure team has not set up the DNS sever in Azure to resolve the private endpoint IP address, and we do not have a timeline for that. This is based on the recent confirmation between Luwen and Larry.

The initiative of deploying Phase 1 early allows us to have got the benefits of a shift-left strategy and achieved “fail earlier”. It has also fortunately helped get our information security involved at an early point in time.

However, we do not have to take the technical debt to actually deploy Phase 1 early for the following reasons:

1. The contract with the external vendor is valid till some point next year.
2. We cannot enjoy long term parallel running due to cost restrictions.

Different from an onpremise application, the cost for an azure pay-as-you-go subscription increases over time while the application runs, as suggested by its name.

1. We may get benefits similar to parallel running by using flat files from production Life/J for a very limited timeshot, based on security approvals.
2. As more people are raising this concern, the DNS server setting may get a higher priority and be configured quicker than thought.

Of course the abovementioned reasons may change over time and may not be justified at a future point in time.

The current VA Printing application takes the following security measures to protect its Azure storage blobs:

1. The blob container is set to private and the blob url can be accessed only when a dynamically generated SAS token is appended to the url.
2. The firewall rules of the storage is configured in such a way that only people via corporate proxy servers can access the storage.

Per my knowledge, the ZAN-S application, whose confidentiality level is Restricted and is only used by our internal users such as MR , imposes IP restrictions using this approach.