Considerations on VA Printing’s External Connections (RCEC)

To Management Team and Information Security Team

Good morning

I would like to share my thoughts and findings ahead of our upcoming meeting to allow them to be factored in to support the decision-making process.

The information security team requires software applications available to internal users only,to 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 from the Information Security Team, connection from Express Route to Azure Vnet is currently unfeasible because our infrastructure team has not set up the DNS server 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 early”. 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 or design debt in order to 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.

In contrast to an on-premise application,the cost for an azure pay-as-you-go subscription increases over time while the application runs, as suggested by its name.

1. If approved and if cleared for security, we may get benefits similar to parallel running by using flat files from production Life/J for very limited timeslots,
2. As more people are raising this concern, the DNS server setting may get higher priority and be configured more quickly than thought.

I’m aware that the abovementioned suggestions may change in relevance over time and may not be justified at a future point, and look forward to decisions from management and information security after taking the whole picture into account.

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 for the storage are configured in such a way that only via corporate proxy servers can people 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.

Best regards,