Information Gathering session

Tuesday, November 9, 2021

Attendees:

Machine generated alternative text:
Oluwaseyi Mafi 
Me 
Sarah Kubiak 
Host 
Bianca Moon 
David Kaemmerer 
Mark Ostrowski 
Michael Shanam 
Nicole 
Saurabh Dilip Saxena 

Location: Webex

AGENDA:

Team roles with regards to active directory

* Julie: Mark reports to me (as part of authentication tower) under Terry.
* Julie: Engaged from an overall authentication tower.
* Julie: Here from an oversight perspective
* Mark: SME running the overall structure.

High-level, how is the AD on-prem managed?

Mark: Team is responsible for AD enterprise wise. We do not manage the affiliates - ACB, OA2, CBTY domains and international.

Who is responsible for implementing domain?

Mark: We manage new services going into production. We own the OS, the application, and the management of the system for all domains. In the event of an acquisition, they determine course of action. Extend domain, build the domain etc.

Contacts?

It is architecture depending. If it is activation and deactivation, work in partnership with Mark's team.

Setting up Domains, is the process documented?

* Can't think of last time domain was built (Julie). The technology is vendor based.
* Mark: We follow Microsoft's best practices given there are multiple domains, and the builds. We have Microsoft assessments. In 2020, 2021 there was an ongoing review, resiliency and capacity and security. There are tools we run in environments for accessing any vulnerability we might see in the environment. Internal to Mark's group.

Tools capture assessment results?

* Yes
* Captures high medium and low. Mark's team look at assessment and look to see if it pertains to the environment or not. Assign individuals to look at the different areas and then use a remediation strategy for issues identified.

Are the activities performed within the Microsoft tools? Or we are using our tools?

* From assessment, we get spreadsheets. Then also track through the account manager for the issues identified.
* Julie: We work with the global security entity to ensure we are following any legal regulations that may pop up
* Mark: We have Microsoft add disposal where we go through a lot of the items to make sure we are aligned with the security best practices. Then review with Microsoft to see controls that should be in place and the remediation tactics to adjust the environment.

From an AD environment perspective. How do you manage the different entities? How many domain controls, from a completeness perspective?

* Have USMDB from the CVS side. That must all align and be kept up to date. Work with the team to see the assets are identified appropriately. When decommissioning we send request.

Platform owners are responsible for maintaining their own asset inventory. The process of how the different asset correlates, has been within the USMDB database.

For completeness and accuracy, we will need to bring in other people, have to make the other team aware because this was not initially in the scoping conversation.

We (IA) want to understand that we are looking at everything out there. Where does the population sit. Who are the different owners?

* We own and manage all the domain controllers that fall under that infrastructure, but for the core infrastructure within CVS health.

What login and monitoring activities are performed?

* Mark: We own the login. We use Splunk to ingest all the security logs. Also use "Scum". We look at who is accessing, what accounts are trying to access etc.

NEXT STEPS:

Sarah: We will go back through our notes and look at key areas of focus. We might reach out for a few more questions in the next week or so before the kickoff meeting. We can share with you what the draft scope deck looks (key areas) before the kickoff meeting. We will make sure we are on the same page before moving forward.