Feedback on NIST Draft Special Publication (SP) 800-210: General Access Control Guidance for Cloud Systems

Greetings Michelle,

Congratulations again on the new role and thank you for seeking AUCloud's feedback and input on this document. We've reviewed the document and provide the following observations for consideration by AustCyber when developing their response.

Overall the document is well put together and takes into consideration the broad scope of access control options across IaaS, PaaS and SaaS deployments, and high-level models that could be used to develop appropriate access controls models within an organisation. In addition to this, AUCloud has made the following observations:

- **Section 1 Introduction**
  - While the introduction talks of protecting critical data and computer resources it doesn't clearly articulate the role or need for risk management to be considered as part of developing access control frameworks and models.
  - AUCloud notes that the type of cloud deployment (public, private, community, hybrid etc.) are not generally considered in the development of this guidance but the risk type and impact will vary greatly depending upon the type of cloud deployment chosen and heavily influence underlying access control frameworks.
  - Similarly, building upon risk management as the basis for any decision making, without considering the type of cloud deployment issues concerning reduced threat vectors such from validated communities or issues surrounding legal jurisdictions are given insufficient consideration or emphasis.

- **Section 2 Cloud Access Control Characteristics**
  - There is a clear difference in respect of risk between cloud provider types (IaaS, PaaS, SaaS) - for example, IaaS providers do not seek access to customer data. In fact, most IaaS providers will require a shared responsibility model with related commercial controls to ensure that they are not placed in a position to have access to the underlying customer data. This is not the case for SaaS providers, who control the circumstances under which their customers provide their data based on the workflow and services their application is seeking to deliver. Best practice guidance and related controls should reflect these differences.
  - Further clarity be provided in respect to shared responsibility models and the role these factors play in developing an access control framework. Figure 2 is relatively simplistic in the application of cloud service models and would benefit from a shared responsibility model which could then be linked to roles.
  - For the benefit of developing generic guidance there may also be value in describing the different roles people will come across in developing access control frameworks in IaaS, PaaS and SaaS deployments and how that links to shared responsibility and organisational risk. For example:
    - Cloud service provider
    - Cloud tenant
      - IT administrators
      - Software developers
      - Application users (internal/external)
  - The key objective for shared responsibility is to clarify which party has access to what data under different conditions. As with other considerations, this has different implications for IaaS, PaaS and SaaS services.

- **Section 3, 4 & 5 Access Control Guidance for IaaS, PaaS and SaaS**
  - Greater definition or guidance as to what the terms Subjects, Actions and Objects mean and how this can be applied to an access control framework.
  - While accepting that the purpose of this document is to develop generic guidance greater emphasis on the types of data requiring protection should be considered. As an example:
    - Meta data
    - Monitoring data (performance, security etc.)
    - Aggregated or derived data value
  - Wonderful to see that guidance on APIs has been considered but as the use of APIs grows the need to clearly understand their use and what they can access should be more defined (what data, under what conditions etc.)

- **Section 6 Guidance for Inter and Intra Operation**
  - No specific observations or comments other than to say that this relates back to the type of cloud deployment risk consideration we previously mentioned.

Overall, it is pleasing to see AustCyber and NIST involved in the development of access control requirements for cloud systems. As the adoption of cloud services continues to grow the need to use standards as a way of developing baseline security controls, guidance and best practices will go some way in assisting organisations to better understand their risk posture and threats that they may be exposed to.

Please don't hesitate to make contact if you would like clarification or to discuss any of the above points in more details.

Best regards,

Phil Dawson
Managing Director
12/05/20