Reims Champagne-Ardennes University

Systancia Cleanroom Session

Jade Marquette

Keywords PAM, SSO, Bastion, Systancia, third-party model, PAW

1 Summary

For several years now, the multiplication of external access to a growing number of internal IT resources has been notable. However, this access is not without risk for companies. Indeed, a study revealed that 59% of organizations have suffered a data leak caused by one of their service providers [1]. In order to counter these risks, the deployment of solutions adapted to the challenges of service provider access becomes an imperative for the global security of information systems. It is therefore with a view to monitoring access and administration actions that companies and local authorities are implementing PAM solutions. PAM solutions, or Privileged Access Management, make it possible to monitor the actions of all IT service providers when they connect (by name) to the managed network [1]. The solution described in this article is Systancia Cleanroom software, which allows the level of control to be adapted to the context of the interventions. This solution is an advanced bastion. A bastion is an element of the computer network that is located in a part that is accessible from the outside, for example the Internet. It is placed in a demilitarized zone (DMZ) of the company's intranet and is partially filtered by a firewall. A bastion is thus used to separate private activities in order to increase security, while providing a service that is accessible from the outside [8]. Systancia's advanced bastion offering does not stop there and allows many other solutions that increase the IT infrastructure‘‘s security of companies that implement their solution.

2 Introduction

Systancia is a European publisher of certified application virtualization, cybersecurity and artificial intelligence products. It has won numerous cybersecurity awards for the solutions it offers [9]. In order to study the PAM solution that this editor proposes, the Systancia Cleanroom Session, two references will be regularly cited. The first source is the eBook "The 4 main issues of service provider access". This book covers the concepts and the need to implement a PAM solution within the company. The second source is an article named "The Cleanroom Concept for Secure and Safe Administration" published on December 18th, 2018. Both of these resources were published by Systancia. The purpose of this article is to analyze the features of the PAM solution, known as the bastion solution, that the publisher Systancia offers. PAM solutions are at the heart of company projects. Indeed, it is essential for any organization to track the actions of its users, whether they are on an external or internal network. One solution is to deploy a Privilege Access Management product [2]. As will be detailed in the article, Systancia offers to cover the needs of service providers and administrators easily at an attractive price [1]. However, the sources on which this article is based are mainly produced directly

by Systancia. Their vision is therefore not necessarily neutral. I personally had the opportunity to test, handle and participate in the installation of the Cleanroom Session solution during a POC in my current company. The interest of this article is therefore to study their solution from an external point of view.

In the first part, we will present the state of the art, then we will present the Systancia Cleanroom solution. Finally, we will conclude by outlining the possible perspectives.

3 State of the art

The eBook [1] is documentation that Systancia provides to companies interested in implementing a bastion solution. The booklet begins by presenting the need for their solution within their infrastructures. This booklet does not just set out the four main issues involved in access management for companies providing services. In fact, despite the title, this booklet is a commercial model promoting the Cleanroom solution. Throughout the various pages, Systancia puts forward and highlights the various functions that its module offers. The advantages described include the possibility of recording sessions, the extremely secure connection, the ease of use of the solution and its attractive price [1]. It is easily noticeable that the purpose of this book is to encourage sales since the last page proposes information for a thirty-day POC. Nevertheless, the information is rich and complete. In fact, it sets out the challenges of PAM solutions as well as the features that make Systancia unique on the market. The article [2], available on their website, presents the Cleanroom concept in greater detail. This page explains the protocols and mechanisms found in Systancia's bastion solution. Their bastion offer is an advanced bastion that combines VPN, PAM and SSO [2], the SSO mechanism will be described more precisely in the next section. These two documents therefore represent well the issues of PAM solutions and briefly expose the mechanisms that the Cleanroom solution integrates. However, the limitations of these documents are that they are produced directly by Systancia. This means that the reader will only find the advantages of their solution; the limitations and points for improvement are not explained. The installation and details of the protocols are not described in these documents either. Today, their solution is implemented in many companies. Their solution is constantly evolving with the implementation of new modules such as the Systancia Cleanroom Desk. This last module is a sterile and disposable virtual administration desk for managing user and administrator access to information system resources [6]. Systancia is therefore an innovative company in the field of IT security. It is also taking steps to have its Cleanroom Session software certified by ANSSI. Systancia is not the only company on the market to offer a bastion. Other companies such as Wallix and Guacamole, an open source APACHE PAM solution, are competing with it. After benchmarking several products on the market and after a financial analysis, many companies nevertheless turn to Systancia for its attractive rates and services.

4 Systancia Cleanroom

4.1 Why switch to a PAM solution

The multiplication of service provider access to a growing number of IT resources is notable [1]. Many companies set up VPNs to connect external users to virtual machines. This has some notable drawbacks such as security issues, poor management and financial costs. Indeed, the manual creation of a VPN is often necessary for each new provider, as well as its removal. This implies the generation of numerous tickets. The use of personal computers, potentially infected, entails a significant risk to the company's IT security. Also,

the authentication licenses are not free, which implies a significant cost and a restrictive management. For all these reasons, the choice of installing a bastion is often considered [6]. The choice of a proprietary solution is often desired in order to have access to support and to have the security of maintained software. Systancia offers solutions that meet the needs of companies in these situations, at affordable prices.

4.2 Cleanroom Session

The Cleanroom Session solution makes it possible to provide instances of the company's infrastructure by means of a bastion. Systancia Cleanroom is a Privileged Access Management (PAM) product that allows you to define administrative access to resources by controlling the accounts used for authentication on the resource and by finely tracing all the actions performed. The level of control and traceability can be adapted to the criticality of the intervention context. [1] The administration of a resource consists of access that presents a risk. This access consists of protocol access on a server (RDP, SSH, Web, etc.) or the use of an administration application. Systancia's bastion also offers video recording of sessions and advanced search. A search bar allows you to search and retrieve videos of commands entered [1]. This web recording is done without agents or bouncing. Also, one of the strengths of the Cleanroom Session is the use of a web console to access the bastion. There is therefore no heavy administration client to install. A heavy client is however available if it is desired.

4.3 Security modules present in the Cleanroom Session

It is interesting to observe the security and authentication modules implemented in the Cleanroom solution. To secure the access to the administration console and to the user WEB portal, a self-signed SSL certificate is generated on the administration server. A self-signed certificate is a public key certificate generated by the user, in this case the administration server, in its own name. An IIS link is also created to ensure HTTPS access. IIS, Internet Information Services, is a WEB server for the various Windows NT operating systems. Windows NT, Windows New Technology, refers to versions after Windows 98.

Regarding the mechanisms set up for authentication, the installation of various agents is required. An agent is a piece of software that acts autonomously according to what its author has requested. One of these agents ensures the operation of the SSO mechanism in the enrolled applications. Overall, SSO mechanisms attempt to address authentication issues. SSO, or Single Sign On, makes it possible to implement a true authentication policy at the network and application levels. The single sign-on system makes it possible to facilitate the evolution of authentication methods, to homogenize connections, notably with synchronization techniques between domains, and to manage access rights and authorizations to an application. The architecture implemented by SSO software generally uses the mechanism of an n-tier architecture. Systancia offers four different SSO modes:

- A fixed SSO, which is the selection of an alias in the safe
- A requested SSO, where the user is presented with an authentication box to enter their identifiers
- Disable SSO
- An activated SSO, where the login/password pair with which the user logged in to the user portal is taken over

Another agent that manages authentication is the "Password Vault" agent. This agent is imperative in order to inject the "Login/Password" automatically into

the enrolled applications. It is installed on the reference machine and works with two registry keys. These keys allow to use user groups for shared containers. A registry key is a piece of information in the registry of one's computer. A registry is the place where files that are essential to the proper functioning of the system are stored and organized. In other words, a registry organizes the settings of certain programs and processes where each piece of information is called a registry key [5]. Added to all these security solutions, an MFA, multi-factor authentication, has been activated with the possibility of using an OTP Mail.

4.4 A step towards the third-party model

One of the expectations of this solution is to be able to propose to companies to set up the administration acts in a three-tier model. This model makes it possible to compartmentalize resources according to their criticality. Each third party must have at least one administration account and a PAW workstation to administer the resources referenced in that third party. The PAW workstation, a privileged access workstation, complies with recommendation R9 of the ANSSI document PA-022, which explains that the main security measure consists of dedicating a physical workstation to administration actions, which must be separate from the workstation that allows access to conventional resources accessible on the organization's IS [3]. The network exchanges between the PAW workstation and the various infrastructure elements must be done using the Kerberos authentication protocol with shielding. The Kerberos protocol is an authentication protocol based on a secret key mechanism (symmetric cryptography) and the use of tickets.

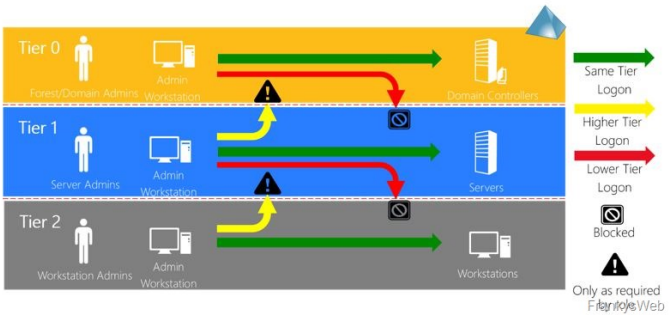

Fig.1. Representation of the Microsoft three-tier architecture [7].

The three-tier architecture regularly implemented is as follows:

- Tier 0: VMs, servers only accessible by administrators. High risk machines such as domain controllers or hypervisors. Authentication can be done by an AzureAD account (password + loggin) coupled with a physical means.
- 1st tier: less risky administration servers. This third party can be partitioned according to the different subsidiaries that the company owns for example.
- 2nd tier: It would hold, among others, the users' machines. The lowest risk [3].

For example, providers could connect to the bastion with a login/password authentication coupled with a code to be validated on their phone to satisfy the MFA, which is strongly recommended. This model adds significant security to the companies implementing it.

5 Conclusion and outlook

Despite certain operating problems that were noted with the solution during POCs with some of their clients, Systancia was able to provide corrective patches to resolve these problems. In an environment where the multiplication of service provider access to a growing number of IT resources is notable, the need to set up a compartmentalized and secure architecture is no longer an option. Systancia's Cleanroom Session product enables service providers and administrators to meet their

needs at an attractive price. This solution makes it possible to create a single entry point to the IS. A protected access point with the implementation of secure authentication systems. Despite the problems encountered, the company's reactivity and the feedback from various customers show the reliability of their solution. The perspectives of this solution are, as mentioned in the previous part, the implementation of an n-tier architecture and more specifically of the tier-model. Installing the Cleanroom Session solution with the Cleanroom Desk would also add a layer of security.

References

[1] Systancia, *The 4 main issues of service provider access*, [eBook]

[2] Systancia, *https://www.systancia.com/le-concept-de-cleanroom-pour-une-administration-securisee-et-securisante/*, December 2018, [web site]

[3] Systancia, *Deployer du PAM en respectant les principes du silotage AD "AD tiering"* , [eBook]

[4] Systancia, *Peer review for Systancia Clearoom* , PAM-1.pdf, July 2020, [Peer review]

[5] Microsoft, *https://learn.microsoft.com/fr-fr/windows/win32/secauthn/authentication-registry-keys* , [Web site]

[6] Systancia, *https://www.systancia.com/systancia-cleanroom-desk*, [web site]

[7] Thibaut from Akril.net, *https://akril.net/comprendre-le-tiering-model-de-microsoft-en-francais/*, November 2022, [web site]

[8] Wikipedia, *wikipedia.org/wiki/Bastion*$_{(informatique)}$, [*website*]

[9] Wikipedia, *wikipedia.org/wiki/Systancia*, [web site]