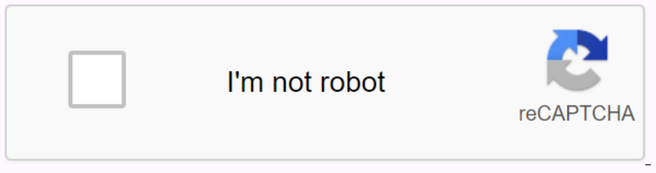

Continue

Information security architecture pdf

The private security industry provides paid protection. Protection may include investigating theft, corporate bodyguard, internal security, and IT security against hackers, and industrial espionage. While historians credit the British Sir Robert Peel with founding the first modern police force in the early 1800s, private security was around much earlier. Crime was high in 1700 England, and both the government and private offered rewards for catching fraudsters. Professional thieves have made a career out of recovering stolen goods for a fee or catching thieves for reward. Many thieves were criminals themselves, extorting payment from thieves in exchange for not arresting them. Jonathan Wild, for example, ran the London underworld in 1720. He secretly arranged many burglaries and also arrested thieves who refused to work with him. The classic figure of the private eye emerged in 1833 when former French criminal Eugene Vidocq founded an investigative agency in Paris. Other investigators followed, investigating cases that police were unable or unseeded. Police agencies have also provided armed security. Pinkerton in the United States, for example, tracked outlaws such as Jesse James and the Sundance Kid. The agency has also broken down strikes and spied on union organizers for entrepreneurs. His eye logo inspired the term private eye. Private investigators from the 1800s worked mainly for the rich. The growth of the middle class in the 20th century made it possible for ordinary people to afford to hire PIO. While police occupied railway safety and other jobs traditionally handled by investigators, tires branched out into areas such as investigating alleged cases of infidelity, missing persons and insurance fraud. The profession became large enough that state governments began licensing private investigators in the early 20th century. The history of private security includes companies selling technology rather than investigative services. A benchmark in security technology came in 1853, when Boston's Augustus Pope patented the first electromagnetic alarm system. Pope's invention created an electrical circuit around doors and windows that set off alarm bells if they were opened. Edwin Holmes acquired the rights to Pope's invention in 1857 and launched the first electrical alarm business. Cybersecurity did not exist before the first mainframes were built in the 20th century, and initially, security meant only protecting the physical computer or magnetic tapes that stored the information. With the development of the Internet, saboteurs, hackers and spies do not more needed physical access to computers to wreak havoc. In the 1990s, computer users faced the first phishing and denial-of-service attacks, but IT security developed as an industry. As hacking has become a big criminal enterprise, the security industry has grown with it. I write about Tech, Cyber and and Not in the exact order. In my latest article on The Rise Of zero Trust Architecture, I wrote about the broad and rapid adoption of this relatively new concept in the world of cybersecurity. However, there are still several other security architectures currently in use: traditional network perimeter security Traditional network perimeter security consists of many different parts, all together to provide a security solution for the network. Traditionally, network security will begin with user authentication, typically using a username and password. This method is also referred to as one-factor authentication, with two-factor authentication having to be verified, such as a mobile phone, USB drive, or even some sort of token. On the most advanced end of the spectrum, there is also three-factor authentication, which will involve the user's biology, such as a retina or fingerprint scan. Once the user is verified, a firewall will make sure that the sign-in protocol is followed by restrictions on what the user can access within the network. This is a very effective method to prevent people from accessing the network when unauthorized. In addition, communications between two hosts on the network can be encrypted to provide an additional layer of security to the network. (Photo by Thomas Jensen on Unsplash) Some companies may also distribute honeypots. A honeypot is essentially a network resource that acts as bait within the network itself. These can be used either as a surveillance tool or as a form of early warning system because honeypots are not used for any legitimate commercial purpose. This means that if you access a honeypot, normally something is wrong. Honeypot attacks can be analyzed by security teams to keep up to date with new attacks. These results can then be applied to further increase the level of security in the real network by highlighting previously unknown vulnerabilities. Similar to honeypots, honey nets are bait nets that are set with intentional security flaws. These are designed to attract attackers so that their methods can be analyzed to increase real network security. Currently, more and more companies are making use of network segmentation and adding it to their systems to strengthen their security. Despite the positive aspects of traditional perimeter security, this procedure is not entirely reliable to prevent Trojans and computer worms from spreading across the network. Traditionally, to combat this either anti-virus software or an intrusion prevention system will be They can detect and prevent the spread of these attacks. In addition, although this system is excellent for preventing external threats, it is not effective in preventing internal threats. With the number of people working remotely from their device there is also a greater risk that contaminated devices may connect to a company's network, potentially putting the network at risk. This has led to the growing popularity of zero-protection architectures. Virtual Private Network (VPN) REMOTE VPN Remote Access works to create a private network over an initially public network. This allows the VPN user to send data and receive data in the same way that if they were actually connected to the primary private network itself. This means that any application running through a VPN will be able to use the functions, security, and private network management features that the VPN is connected to. VPN technology was initially developed to allow remote users and different office branches to have access to applications and other items that would be hosted in the network of the headquarters' primary branch office. To gain access to the VPN, users must authenticate using a password or security certificates. When a company uses VPN technology, it can help ensure that remote workers and other offices can establish a secure connection to the headquarters network without the risk of an attacker infiltrating the network through the remote user. Network segmentation In the context of the computer network, the practice of network segmentation is that of dividing a network of computers into a group of subnets. Each of these subnets is then called a network segment. (Photo by Alina Grubnyak on Unsplash) One of the security advantages of segmenting networks is that all transmissions from segments will be kept within the internal network itself. As a result, the network structure will only be visible inside. Another advantage of network segmentation is that if a segment of the network is compromised, you can reduce the surface space for moving an attacker. In addition, some types of cyberattacks only work on local networks, which means that if you segment the different areas of the systems, making these decisions from their use. For example, if you were to create separate networks for your database, web servers, and devices, this would help keep your network a little more secure. This would be done by tactically deploying resources to various networks and assigning specific individuals to each network segment. The correct use of network segmentation to improve security levels would split network segmentation into those different subnetwork and give each subnetwork a certain level of permission needed for access. So, you need to take steps to make sure that you have been put in a protocol to limit the elements that can move between each subnet. Role-based access controls Role Role Control (RBAC) restrict access to certain systems, based on a user's permission level. The vast majority of companies with more than 500 employees use role-based access controls, and more frequently, small to medium-sized enterprises are starting to use this technology. To more effectively use role-based access control, a company will split its user profiles by certain categories. In general, they will be based on the role of work, the level of seniority and the resources that each individual will need based on the first two factors. For example, if an organization had to use role-based access control and a junior member of the finance team had to access their network, the employee would have access to the lower-level financial data that they will need to view within their work role. However, their access would be limited to this. They would not be able, for example, to view files or data related to the legal team or files that should only be viewed by senior financial team members, such as the finance director. When a company uses role-based access control, it can be an incredibly effective way to make sure that all sensitive data is only viewed by individuals who are allowed to view it. It can also help prevent deliberate internal leaks of information. (Photo by Jonathon Young on Unsplash) Software-defined perimeter (SDP)What is a software-defined perimeter? One of the ways you can create a zero-trust architecture within your organization is to create or use an SDP. We'll see what an SDP is so you can do just that. As cloud storage has become more common in the present day, there has been an increased risk of cyberattacks on these cloud systems due to the fact that cloud servers cannot be protected from traditional perimeter security measures. This led to the creation of Software Defined Perimeter in 2013. Software Defined Perimeter is a research working group. Their main goal is to create a security system that can help prevent attacks on cloud systems. Any results of their research will be made free to use for the public and will not be subject to any usage fee or other restrictions. From the very beginning of the working group, they decided to try to focus on building a security solution that is cost-effective, but still incredibly flexible and effective. During their work, the team identified three essential design requirements. First, they decided that their security should have confirmed the user's ID, which device they are using, and the permissions they have to access certain directories. Next, they decided that verification using encryption (which is also used as the fundamental technology behind what we all know today as a blockchain) would be the best option to ensure that their security protocol would be applied. Finally, it was decided that the tools needed to achieve the first two requirements are tools that have a proven track record and are in the public domain. SDP came to the decision that their security architecture should be based on a control channel. This control channel would make use of standard components that the team thought would be best suited for the task. These components were SAML, PKI and mutual TLS. Finally, the working group published a paper based on this idea to assess whether or not there was a demand for such a system. This is where they called it Software Defined Perimeter.There was a lot of interest in the work that SDP was doing and this led to the release of the version one of their systems in April 2014.Il their first ever design was made up of a startup host, which would give the Controller information about which device is being used and who from. This information would be transmitted along with a reciprocal TLS connection. After you do this, the controller will join an issuing CA to confirm the identity of the device and will also join an ID provider so that it can verify the user's identification. After this information is confirmed, the controller will provide one or more reciprocal TLS connections, these connections will be linked to the previously mentioned boot host and all necessary acceptance hosts. This system works with significant effects, being able to prevent any strain of network attacks, including Man-in-the-Middle, DDoS, and Advanced Persistent Threat.The Architecture of SDP Version OneI original SDP products for commercial use has been implemented using an overlay network for business applications, examples of which are remote access to high-value data, or to protect the cloud system from attacks. The startup host for the SDP took the form of the client and the acceptance host became the gateway. (Photo by Anastasia Dulgier on Unsplash) SDP clientThe SDP client itself is responsible for a wide range of functions. Two of these include verifying your device and the user ID you use, as well as routing applications to the whitelist for protected applications that have been authorized. The SDP client has a real-time configuration to ensure that the reciprocal TLS VPN connection is linked only to the items that the individual user is allowed to use. This means that the SDP Client performs the function of placing restrictions on access to certain data points based on the user's level of authority. This is done after the user's ID and device have both been verified. SDP GatewayThe SDP gateway serves as the point where the Mutual TLS connection to the SDP client ends. In a topological sense, the Gateway will be to be as close to the protected application as it is practical. the sdp gateway will receive the ip address and its certificate once the identity of the device requesting access and their permission level is confirmed been brought to light. SDP ControllerThe SDP controller acts as a trusted intermediary between back-end security features, such as the identity provider and certification authority, to the SDP client itself. Once the SDP client has reached verification and the authority level for the user has been reviewed, the SDP controller will then begin configuring the SDP client and SDP gateway so that they can establish a real-time connection through a reciprocal TLS. Security properties of SDP architectureWhen you properly implement all three of these features, the SDP architecture can provide excellent and unique properties for the security system. These features are listed below. (1) Hide information There is no DNS information, nor are there any visible ports within the secure application infrastructure. Because of this, SDP-protected resources are called dark resources because they cannot be discovered, even if you scan for them. (2) Pre-authenticationThe identity of the device attempting access will always be verified before they are granted a connection. The device identity will be confirmed using a MFA token that will be embedded in each other's TCP or TLS architecture. (3) Pre-authorization users in an SDP system only have access to the servers they need to access because of their role. The system used to confirm the identity will communicate user permissions to the SDP controller. This is done using an SAML assertion. (4) Application-level accessThis when a user is granted access to the application, it will only be at the application level and not at the network level. The SDP also whitelists some applications on the device that the host is using, which helps maintain app-to-app-level system communications. (5) Extensibility.The SDP architecture is created on the back of various parts based on different standards. These include TSL, SAML and mutual safety certificates. Due to standards-based part management, SDP architecture can be easily connected and integrated with other types of security systems, including data encryption systems and remote claims systems. Through the combined use of pre-authentication with pre-permissions, companies can create invisible networks to unidentified hosts, while providing the necessary permissions to known users, based on their organizational role. One of the main parts of SDP is that pre-authentication and pre-authorization must occur before a TCP connection is granted between the user and the secure application. In addition to this, authorized users only granted permissions for certain applications to ensure that compromised devices cannot move sideways across the network. (Featured image of Rubén Bagés on Unsplash) Sign up Hacker Noon Create your own free account to unlock your Experience. Experience.