Dr. James B. Fraley

Implementing Zero Trust — Lessons Learned

Implementing Zero Trust can be a difficult process. This presentation will discuss and present a zero trust checklist. This presentation approaches Zero Trust (ZT) in an easy way so as to not overwhelm stakeholders and others with implementing policies, architectures and deploying tools across your entire network. Focus is on protecting the most valuable digital assets. These topics include: Sensitive Data - This includes the data of customers and employees, as well as proprietary information you do not want to fall into the hands of a thief. Critical Applications - These are the applications that play a central role in your most crucial business processes. Physical Assets - Physical assets can range from point-of-sale (PoS) terminals to Internet-of-Things (IoT) devices to medical equipment. Enterprise Services - These include the elements of your infrastructure used to support the day-to-day work of employees and executives, as well as those that facilitate customer sales and interactions. Implement Controls Around Network Traffic - The way traffic flows through your network will often pivot on the dependencies each system uses. For example, many systems need to accessa database holding customer, product, or service information. Requests, therefore, do not simply “go into the system.” Rather, they have to be routed through a database containing sensitive and delicate information and architecture. Understanding these kinds of details will help you decide which network controls to implement and where to position them. Architect a Zero Trust network - A zero trust network is designed around your specific protect surface—there is never a one-size-fits-all solution. In most situations, your architecture may begin with a next-generation firewall (NGFW), which can act as a tool for segmenting an area of your network. Also at some point, you will want to implement multi-factor authentication (MFA) to ensure users are thoroughly vetted before being granted access. Create a Zero Trust Policy - After you have architected the network, you will want to design your zero trust policies. This is most effectively done using what is known as the Kipling Method. This involves asking who, what, when, where, why, and how for every user, device, and network that wants to gain access. Monitor Your Network - Monitoring activity on your network can alert you to potential issues sooner and provide valuable insights for optimizing network performance—without compromising security. Reports - Reports produced on a regular or ongoing basis can be used to flag abnormal behavior. You can also analyze them to assess how your zero trust system impacts employee or system performance and ways you may be able to improve it. Analytics - Analytics takes data generated by your system and provides insights regarding how well it functions. Insights are valuable when you need to monitor network traffic, the performance of components of the network, and patterns of user behavior. Logs - The logs produced by your system provide you with a permanent, time-stamped record of activity. These can be analyzed manually or using analytical tools, such as machine-learning algorithms that can recognize patterns and anomalies.

Biography

Dr. Fraley, Assistant Professor, Chair for Information Assurance in the College of Technology, Wilmington University. Dr. Fraley has over 30 years of experience working as an educator and security practitioner. He has taught at Wilmington University for over 6years. He has held such positions are Senior Threat Intelligence Strategist and Global Security solutions supporting the Fortune 100 companies. His commercial experience has been with McAfee, Northrop Grumman, L3 Communications, Dupont and Integic. He has managed and supported some of the largest and most complex cyber security projects for both the private and public sectors including DOD, Intelligence Community (IC), Federal Aviation Administration (FAA) and the City of New York. Dr. Fraley's research focused on advanced detection techniques using machine learning for Polymorphic/Metamorphic malware. He is also a retired US Army Signal officer with over 22 years of service.