Zero Trust Cybersecurity: Procedures and Considerations in Context

Subjects: Computer Science, Cybernetics

Contributor: Brady D. Lund , Tae-Hee Lee , Ziang Wang , Ting Wang , Nishith Reddy Mannuru

In response to the increasing complexity and sophistication of cyber threats, particularly those enhanced by advancements in artificial intelligence, traditional security methods are proving insufficient. This paper provides an overview of the zero-trust cybersecurity framework, which operates on the principle of “never trust, always verify” to mitigate vulnerabilities within organizations. Specifically, this paper examines the applicability of zero-trust principles in environments where large volumes of information are exchanged, such as schools and libraries, highlighting the importance of continuous authentication (proving who users are within the network), least privilege access (providing only access to what users specifically need), and breach assumption (assuming a breach has or will occur and thus operating to limit the spread through the use of multiple checkpoints throughout the network). The analysis highlights avenues for future research that may help preserve the security of vulnerable organizations.

zero trust | security frameworks | data security | security in context

In a time where rapidly evolving threats—bolstered by advancements in technologies like artificial intelligence—pose substantial danger to organizational well-being, it is critical to adopt advanced security solutions to protect assets. Conventional methods of security are no longer sufficient, in isolation, to ensure organizational cybersecurity. Multifaceted approaches, which consider each element of an organization as a potential vulnerability, are requisite. Enter zero-trust cybersecurity, a security paradigm that embraces a zero-trust philosophy: in order to limit vulnerabilities, there is no default trust that any person or object within a network is what it claims or should have access to unnecessary segments of the network [1]. This philosophy means that all users must continuously provide evidence that they are who they claim (e.g., through multi-factor authentication), and access is limited to only that information that is position-critical.

Traditional cybersecurity relies on a perimeter-based approach, where the network operates as though an enclosure with a perimeter fence. Once a user successfully enters the perimeter, they are “in” and no longer need to worry about further verifying who they are or why they need to access any part of the network. This model is problematic, as it means that if an attacker makes it through the network’s perimeter, they can access and disrupt nearly all network functions, increasing the likelihood for major interruptions that could take the entire network offline and cause permanent damage. The zero-trust approach ensures that users must pass through a constant series of checkpoints to access any part of the network, which limits the spread of any threat that emerges. Consider, for example, a breach that compromises a list of organizational clients. This breach is costly, but less so than a breach that also places human resources and financial records at risk. Isolating a threat and minimizing its impact can mitigate the costly nature of cyberattacks.

Organizations where large amounts of information are regularly exchanged and private records are secured—such as schools and libraries—are especially at risk from cyber threats. Recently, the Toronto Public Library fell victim to a cyberattack that hijacked its systems and data for months, crippling the organization's ability to function properly and threatening patron privacy [2]. In these organizations, zero-trust cybersecurity practices may offer a way to remain resilient in the face of increasing threats. The purpose of this paper is to discuss how zero-trust cybersecurity principles may be integrated into learning and information organizations to preserve the sanctity of these organizations' information and records.

References

1. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture; NIST Special Publication, 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
2. Bridge, S.; Zoledziowski, A. 1 Million Books and 4 Months Later, Toronto's Library Recovers from a Cyberattack. Canadian Broadcasting Corporation. 2024. Available online: https://www.cbc.ca/news/canada/toronto/toronto-library-ransomware-recovery-1.7126412 (accessed on 12 June 2024).