C768/D339 Task 2 Template

The Benefits of Zero Trust Architecture at eBay

Section A: Executive Summary

To provide a safe and secure environment for eBay members we identified a need for further securing the infrastructure. Research suggests that a new method of authentication is needed. Zero Trust Authentication will add the layers of protection needed to continue to protect our member data in an ever-evolving threat landscape. This summary provides a brief description of Zero Trust Architecture.

What is Zero Trust Architecture?

In 1994 the Jericho Forums began detailing the concepts of Zero Trust Architecture. Zero Trust Architecture is a security framework that requires authentication, authorization, and continuous real-time validation before being granted or keeping access to applications or data on the infrastructure. Zero Trust Architecture postures the organization to be secure beyond the network edge.

Benefits of Zero Trust Architecture

When properly implemented Zero Trust Architecture:

* Reduce the load on border gateway firewalls
* Reduce the blast radius of compromised user accounts
* Reduce the reliance on network segmentation
* Reduce overhead for SOC 2 and PCI compliance
* Further reduce the risk created by the mobile workforce

Given the current hybrid workforce created by Covid, eBay is supporting a significant increase in mobile employees. Zero Trust Architecture provides a more inherently secure infrastructure. This would significantly reduce the number of credentialed attacks commonly seen with online vendors. More than 80% of all attacks involve credentials use or misuse in the network (Raina, 2021).

Zero Trust Architecture also removes the physical and logical boundaries of network edge as it operates independently between local, cloud, or hybrid network configurations. Gone is the concept of protecting the network edge, and allowing users who have authenticated to that edge.

In conclusion the research advocates for the configuration and implementation of Zero Trust Architecture.

A1. Executive Summary Tone

The diction is kept semi-formal as this is written for an executive audience. The diction is also pedestrian due to the topics chosen. The executive audience will not need the technical details taken to implement and maintain a Zero Trust Architecture, instead, a high-level overview has been provided.

A2. Executive Summary Jargon

The executive summary is addressing senior leadership for a technical department. The department is working to drive the overall safety and security of eBay, while they are still technical people the use of buzz words and industry jargon are still used, such as “real-time”, and “blast radius”. These terms are commonly used while discussing network security.

A3. Executive Summary Message Timing

Delivery of the message on Wednesday mornings between 10:00 AM and 11:00 AM PST would allow for executives to further discuss Zero Trust Architecture while going to lunch with their peers. The information contained in the message is not sensitive as documentation and industry standards have been published on various public-facing sites, such as NIST, and Crowdstrike. The classification of this message is internal, this again is industry standard as it is not commonplace to divulge details of the network infrastructure as outside sources can leverage these details in a formulated, targeted attack.

Section B: Press Release

Write an internal press release that gives your entire organization a glimpse of your topic that contains the following items:

Headline: eBay To Lead Industry with Zero Trust Architecture

Lead-in: The Information Security Team at eBay is proud to present the addition of Zero Trust Architecture. Join us to discuss the benefits to learn more.

Location: 541 eBay Way, Draper, Utah

Body: As a pioneer in the Information Technology industry, the eBay Information Security team is proud to present the addition of Zero Trust Architecture at eBay. We will be discussing the below benefits and more:

* Security beyond the network edge
* Ensure security between on-prem and cloud data centers
* Increase in trust and stability of the numerous internal and external applications used by both members and employees

The addition of Zero Trust Architecture provides a more secure working environment that will allow eBay employees to bring their full selves to work every day, no matter where they may be from. Thanks to the additional security provided, employees will have the ability to be even more mobile.

Contact Information:

Matthew Lorenzen, eBay Incident Response

mlore23@wgu.edu

1.712.259.2099

B1. Press Release Tone

This press release uses informal diction to drive excitement. The tone of the press release is informal, the press release is written to drive curiosity and engagement.

B2. Press Release Jargon

The jargon used keeps the press release light on technical details while driving the interest of those that may be more technical. I avoided using more technical terms to assist in driving by non-technical employees and departments.

B3. Press Release Message Timing

This should be released at 10:00 AM PT on a Wednesday, with the press release scheduled for Thursday at the same time. These times are chosen to drive the continued conversation while individuals and teams break for lunch and afternoon meetings. The sensitivity is internal, however, company-wide. This is due to the overall impact of the implementation of Zero Trust Architecture, while not meant to be “public knowledge”, it has a low risk in the event of public exposure. The classification aligns with the sensitivity, intended to be internal to all employees, however, little risk is associated if publicly exposed.

Section C: Frequently Asked Question (FAQ)

Question: What is Zero Trust Architecture?

Answer: Zero Trust Architecture is a security framework requiring all users, regardless of physical location internal or external to the organization's network to be authenticated, authorized, and continuously validated before being granted or keeping access to applications and data.

Question: How does Zero Trust Architecture keep accounts safe?

Answer: Zero Trust Architecture works to remove the “network edge” or “trust but verify” concepts, instead relying on the concept that “no implicit trust” will be allowed, meaning users are validated at every step of a workflow, from selling an item on the eBay site to configuring and deploying new applications on the internal network to support internal employees supporting members.

Question: How does Zero Trust Architecture allow for a more mobile workforce?

Answer: Zero Trust Architecture provides authentication and validation beyond the network edge, allowing for a more open infrastructure as accounts are authenticated, accessed, and validated at every step across the network. This would significantly reduce the number of credentialed attacks commonly seen with online vendors. More than 80% of all attacks involve credentials use or misuse in the network (Raina, 2021).

C1. FAQ Tone and Diction

The diction is informal, meant to be high-level and non-technical enough to ensure that both technical and non-technical employees can quickly digest the information.

C2. FAQ Jargon

Limited use of jargon is used to ensure the information is easily digestible by the entire audience. Some technical usage is unavoidable; however, the jargon is kept to a minimum to ensure understanding and maintain audience engagement.

C3. FAQ Message Timing

This should be released at 10:00 AM PT on a Wednesday, with the press release scheduled for Thursday at the same time. These times are chosen to drive the continued conversation while individuals and teams break for lunch and afternoon meetings. The sensitivity is internal, however, company-wide. This is due to the overall impact of the implementation of Zero Trust Architecture, while not meant to be “public knowledge”, it has a low risk in the event of public exposure. The classification aligns with the sensitivity, intended to be internal to all employees, however, little risk is associated if publicly exposed.

Section D: Sources

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., 2020. Zero Trust Architecture. [online] NIST. Available at: <https://www.nist.gov/publications/zero-trust-architecture>.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., 2020. NIST Special Publication 800-207 - Zero Trust Architecture. [online] https://nvlpubs.nist.gov/. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

Raina, K., 2021. What is Zero Trust Security? Principles of the Zero Trust Model. [online] crowdstrike.com. Available at: <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>.

Dean, E., Fonyi, S., Morrell, C., Lanham, M., & Teague, E. (2021). Toward a Zero Trust Architecture Implementation in a University Environment. The Cyber Defense Review, 6(4), 37–48. https://www.jstor.org/stable/48631305

Davis, J., Simos, M. and Skoniecki, J., 2020. Back to the future: What the Jericho Forum taught us about modern security - Microsoft Security Blog. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/security/blog/2020/10/28/back-to-the-future-what-the-jericho-forum-taught-us-about-modern-security/>.