Identity-driven security

Identity management, device security are essential to achieving zero trust

As cloud and mobile computing continue to dissolve the network perimeter, organizations need a zero trust security strategy based on strong identity and access management.

Identity management can help organizations prevent the nearly 80 percent of data breaches that are caused by compromised credentials.

By tackling these known security challenges first, organizations can better protect their assets and create a strong foundation for a zero trust architecture.

Zero trust means that organizations give the right people the right level of access to the right resources in the right context, said Kelsey Nelson, senior product marketing manager, at Okta.

This also means organizations must continuously assess their environment and understand their risk without making it difficult for users.

"A lot of what were seeing from zero trust is not only increasing security, but also doing it in a way that is beneficial and easy for end users," Nelson said. "I don't think that can be understated."

Okta approaches identity-driven security by providing an independent and neutral platform for workforce identity; a scalable and secure customer identity platform; and an identity-centric approach to zero trust security.

However, identity doesn't just apply to an agency's workforce, Nelson said. "You need to manage access and security for that extended ecosystem—contractors, partners, even your customers… are going to require access into those different services and we need to do this with that zero trust approach to security."

Security has to be looked at holistically, she added. Interoperability and collaboration need strong security that is applied across all these constituents.

Okta maps its different technologies to the draft NIST 800-207 guidance on zero trust architecture. The company enforces access to the application, provides direct and delegated administration to policies for zero trust access, and serves as a policy engine.

The policy engine helps organizations apply adaptive policies and analyze risk signals from across the ecosystem to determine for instance, when is there a need to restrict access, or take other actions.

The company supports different deployment models including a device agent/gateway model to enable access not just to applications, but also to servers.

There are a lot of pieces that go into zero trust, so organizations have to consider not just identity, device, access, and the network, but also how they interplay, and take a holistic approach to zero trust, Nelson said.

"It's not just applications we need to think about access to, but it's the holistic data and down into infrastructure as well," she said.

By starting with the idea of the user and device, and adding context such as location, network and application data, and using analytics, organizations can gain insight into their risk posture.

For instance, if a user's device posture has changed, or a user is coming in from an unmanaged device, an organization can change the user's access capabilities so they are only allowed to access a limited part of an application or resource.

"By being able to ingest that insight into something like an identity system, you can start to set policies that are appropriate," Nelson said.

About 93 percent of agencies are engaged in zero trust projects, which indicates that this is work is already underway.

However, to go from zero to zero trust doesn't happen overnight. From an identity standpoint, it takes time to go from a fragmented identity with active directory on-premises and no cloud integration, to an adaptive workforce with risk-based access policies and continuous and adaptive authentication and authorization, she said.

For early and rapid success, organizations should focus on improving identity management and device security. These are foundational pieces to achieving zero trust.

Agencies don't have to completely rethink their security stack in order to achieve zero trust, she said. This is evident in some of the work that agencies are already doing. "A lot of it is about how do we leverage the tools we have, how can we start to extend the components coverage across our ecosystem."

"It's not just applications we need to think about access to, it's the holistic data and down into infrastructure as well."

– KELSEY NELSON, SENIOR PRODUCT MARKETING MANAGER, OKTA

Article Source: FCW Zero Trust Virtual Workshop | May 19, 2020