Leveraging the iboss Zero Trust Edge and NIST 800-207 Zero Trust Architecture to Protect Against the Okta Breach

Overview

In March 2022, Okta disclosed a breach that may have put organizations at risk who rely on Okta as their Identity Provider for authenticating users to sensitive enterprise-owned resources. The outline and timeline of the breach was described by Okta's Chief Security Officer via a blog post on the **Okta site**.

This white paper provides an overview of the breach and how organizations that may be impacted can protect themselves while providing visibility and future protection from breaches of this kind. The focus is on leveraging the core NIST 800-207 Zero Trust Architecture principles which are delivered by the iboss Zero Trust platform.

Understanding the "Root Cause" of the Okta Breach and the role the NIST 800-207 Zero Trust Architecture Plays in Protecting Organizations

Before the analysis is performed, it is important to understand the "Root Cause Analysis" of this breach which is simple. An attacker obtained unauthorized access to an enterprise-owned system. The enterprise-owned system was Okta's administrative platform used to support customers. This is important because it sits at the core of what Zero Trust, according the NIST 800-207 Zero Trust Architecture Publication, aims to solve - which is preventing unauthorized access to data and services. This is a critically important point.

Let's first start with the Cybersecurity and Infrastructure Security (CISA) report "**2021 Trends Show increased Globalized Threat of Ransomware**".

This provides technical details of the root cause of the top initial infection vector for breaches in 2021 related to ransomware:

> **"Gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities. Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021."**

CISA Technical Details on Ransomware

Ultimately, the "Root Cause Analysis" of these breaches was an attacker gaining unauthorized access to resources. The result was a ransomware infection that resulted in data loss or data destruction which is the same risk organizations face in light of the Okta breach.

Now, refer to the **NIST 800-207 Zero Trust Architecture**.

It provides an operative definition of Zero Trust that contains the following:

> **Zero Trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.**

NIST 800-207 Zero Trust Architecture, Zero Trust Basics, Page 4

The NIST 800-207 continues with:

> **This definition focuses on the crux of the issue, which is the goal to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible.**

NIST 800-207 Zero Trust Architecture, Zero Trust Basics, Page 4

Zero Trust, according to the NIST 800-207 and the iboss implementation of that architecture with the iboss Zero Trust Edge, is centered around resource access. This is made clear in the following statement within the NIST 800-207:

> **That is, authorized and approved subjects … can access the data to the exclusion of all other subjects (i.e., attackers). To take this one step further, the word "resource" can be substituted for "data" so that ZT and ZTA are about resource access … and not just data access.**

To summarize, the top three initial infection vectors for ransomware in 2021 were all unauthorized resource access vectors. The root cause of the Okta breach was unauthorized resource access. The potential risk to an organization that leverages Okta for identity is potential unauthorized resource access. All result in the same outcome to an organization which is data loss, data destruction or denial of access to systems and services in exchange for ransom. The iboss Zero Trust Edge, based on the NIST 800-207 Zero Trust Architecture, is centered around protecting an organization from the root cause of the breach and the implications of that breach by protecting enterprise-owned resources from unauthorized access. A properly implemented Zero Trust model will make all enterprise-owned resources private and authorize, inspect, and log each request to a resource. Each request is authorized, not just the request that occurs during login, to ensure organizations are protected from breaches and data loss.

Outline of Okta Breach

The Okta Chief Security Officer, David Bradbury, provided details and a timeline of the events. The core issue that resulted in this breach is that an attacker gained access to a support engineer's system, via Remote Desktop, and used that virtual session to interact with the Okta support admin portal. Although David indicates over 125,000 audit logs were analyzed to determine if any changes were made to tenant accounts that could put an organization at risk by allowing unauthorized users to access their resources, Okta is not clear on what changes were made by the attacker.

Risk Analysis

Okta did not provide information on the changes made by the attacker to the authentication settings which may result in unauthorized attackers gaining access to protected resources. This creates a blind spot for organizations that have not implemented Zero Trust, according to the NIST 800-207, that are attempting to determine if their applications and data are at risk. This is a result of a very important principle that is often missed by organizations and is clearly stated within the definition of the NIST 800-207 Zero Trust Architecture which states "per-request access decisions" must be used when protecting resources via Zero Trust principles.

The NIST 800-207 states the following for Zero Trust basic principles:

> **"To lessen uncertainties (as they cannot be eliminated), the focus is on authentication, authorization, and shrinking implicit trust zones…"**

Authentication and Authorization are two key principles that must be understood. Authentication is the process of determining who a user is. For example, using an analogy of an Airport Security Checkpoint, authentication involves checking a traveler's ID and passport to determine if the person is indeed the person they claim to be. Authorization is granting the user the privilege to access the protected resource (application, data or service). In the airport analogy, this allows the traveler to cross the checkpoint so that they can board the plane (the plane is the protected resource). Zero Trust principles apply in much the same way but instead of the protected resource being a plane, the protected resource is an application, data or service owned by the organization.

Okta, and similar Identity Providers (IDPs), provide strong authentication so that a user that wishes to interact with a protected resource is identified with high confidence. In addition, an Identity Provider provides authorization when the user is allowed to log into the system. However, this is where a very particular nuance matters most. According to the NIST 800-207 Zero Trust Architecture definition, authorization must occur on each and every request between the user and the protected resource. This is what allows every transaction to be inspected, protected and logged for visibility. Unfortunately, the Identity Provider is only able to authorize at the point of login which misses the vast majority of requests between the user and the protected application, data and service. The Identity Provider is blind to these requests which results in the organization being exposed to data loss and breach as well as lack of visibility.

This is where the root cause of the issue resides. An organization with a properly implemented Zero Trust service, such as the iboss Zero Trust Edge which uses the principles of the NIST 800-207 Zero Trust Architecture, would not be stuck wondering whether or not their resources were accessed by unauthorized attackers. The organization would not be in a position that leaves them uncertain of whether or not sensitive data was hijacked due to an authorized user, via the Okta hack, gaining access to a system and extracting data with no visibility. The organization would not be in a position that leaves them vulnerable to future data hijacking or compromise. This is because each and every request to all protected resources would have to be authorized, logged and approved regardless of whether they were authenticated and authorized at the point of login by Okta or the Identity Provider.

There is another risk area as well. Although Okta expired the user sessions of accounts that may have been impacted, the logged in sessions between the user and the application were already created and could have an extended period of time that those sessions are valid without needing to re-authenticate against Okta or the Identity Provider. This means that if a long lasting session to an application exists, Okta will not be consulted for a long period of time allowing unauthenticated attackers to remain undetected as well as putting them in a position to exfiltrate data or create other breaches. With a Zero Trust edge, it is possible to expire ALL sessions that exist between a user and an application immediately, even if those sessions are still valid and do not require another authentication request to Okta. This is because the iboss Zero Trust Edge provides the ability to perform modern authentication on every application, data and service (including those services that do not support modern authentication) which results in the ability to terminate the session between the user and the iboss Zero Trust service edge (before the request is sent to the application). With this functionality, an organization can guarantee all sessions created by Okta logins are terminated immediately to all protected resources resulting in users needing to re-authenticate to ensure proper identity.

Conclusion

A properly implemented Zero Trust strategy ensures authorization occurs on every request to a protected resource. It does this by placing all sensitive applications, data and services behind a Zero Trust Service Edge which makes them private and only accessible through the service edge by authorized users. There is no direct access to resources and every request is authorized, beyond the single point of authentication. It provides continuous protection and visibility to ensure breaches and data loss are prevented. It protects from situations like the Okta breach and puts organizations into a stronger position by reducing cyber-risk and providing the necessary visibility to ensure a high level of confidence in protecting critical sensitive resources. For organizations that have not implemented Zero Trust in this way, it can immediately remediate the risk by placing those resources behind a service edge that will protect and provide visibility for resource access moving forward.

About iboss®

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022. To learn more, visit www.iboss.com

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston, MA 02110