+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Incident Review

Okta breach widens to affect 100% of customer base. Read about it here and how your organisation to stay vigilant and protected.

Okta breach widens to affect 100% of customer base. Okta has released further updates about the September cyber attack, now revealing that 100% of customers were impacted by a data breach.

What happened?

In October, Okta disclosed that its customer support systems had been compromised, and support data from customers stolen. Some of this support data contained session tokens which allowed the threat actors to carryout subsequent attacks on some of Okta's customers including BeyondTrust, 1Password, and Cloudflare.

In the initial reports Okta stated that date relating to only 1% of customers was stolen in the breach. However, in an update posted on November 29th, Okta disclosed that threat actors successfully carried out a second data breach during the attack.

While the previously disclosed data breach related to stolen customer session tokens, Okta also found that an unauthorised user was able to obtain a report which contained data of every customer within Okta's customer support system.

This data potentially included customer account created date, last login, full name, username, email, company name, user type, address, date of last password change or reset, role (name), role (description), phone, mobile, time zone, contact information, user name, role description, and SAML federation ID.

While none of the stolen data could directly lead to a compromise of Okta's customers, it could be used to launch spear phishing attacks against Okta's clients.

The Challenge of Post Incident Investigation

This is now the third month of updates on the Okta data breach, as more details continue to emerge regarding the cyber attack.

The ongoing updates following the initial incident highlight the significant challenges associated with post incident investigations that aim to establish what data the threat actors have compromised.

A successful investigation requires not only committing resources to the investigation post breach, but also careful planning prior to the breach to ensure appropriate logging and monitoring is in place to support investigations.

Organisations using Okta Should

• Be aware of an increased risk of spear phishing attacks targeting any users who had access within the Okta customer support portal.

All Organisations Should

• Implement a data classification policy which outlines how data should be classified and the security control that needs to be applied to each classification. The policy should require all files to be classified in accordance with the policy so anyone accessing the file is aware of the security controls that should be applied and who should have access to it.

• Implement a Data Loss Prevention (DLP) strategy, which includes the implementation of security tooling, to control and restrict data movement in and out of the organisations network and SaaS platforms. This can help organisations detect and prevent malicious or accidental transfer of data out of the network.

• Ensure they have implemented a logging and monitoring strategy that supports the forensic investigation requirements so that the impact of an incident and any potential data breaches can be identified quickly after an incident.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430