Cynch Security Case Study

Cyber security in practice: multi-factor authentication

Cyber threats are an ever-present risk for organisations big and small. In this blog, we look at a 2022 cyberattack on global Customer Relationship Management (CRM) provider, Twilio.

The attack exposed thousands of individual user records and highlighted the limitations of multi-factor authentication. Read to the end for suggestions on how to strengthen your multi-factor authentication security processes.

What happened

Twilio is a global software developer that provides CRM tools to thousands of companies around the world.

In August 2022, Twilio became aware of unauthorised access to information related to Twilio customer accounts. Cyber criminals gained access via an advanced social engineering attack whereby current and former employees received text messages posing as Twilio's IT department. This is known as phishing.

The text messages suggested that employee passwords had expired or calendars changed and requested the employee log in via a malicious URL. Twilio's cyber defences involved the use of multi-factor authentication via SMS message. In this instance, the multi-fact authentication platform had also been breached by the cyber criminals.

Two employees failed to recognise this was a scam. They logged into the site controlled by the attacker. The attacker was then able to access Twilio's systems, providing access to hundreds of Twilio business customer accounts and details from thousands of individual user records.

Twilio's response

When the incident was confirmed, Twilio revoked access to the compromised employee accounts, engaged an external forensics firm to support the internal investigation and delivered additional security training for all employees.

Twilio also began individually notifying affected customers with the details of the attack and outlining what data had been accessed.

A subsequent attack

In the weeks following the initial attack, Signal, a client of Twilio experienced a related incident.

Signal is an encrypted messaging platform that uses Twilio services for phone number verification.

Using information gathered from Twilio's systems, the attacker compromised the accounts of 1,900 Signal users and attempted to re-register their mobile numbers to other devices.

Signal subsequently notified the impacted customers and de-registered Signal from the associated devices.

Cloudflare incident – multi-factor authentication using physical keys

In August 2022, technology company Cloudflare also experienced a cyberattack. The Cloudflare attack was separate to the Twilio incident but was similar in approach.

Three Cloudflare employees failed to recognise the phishing scam. However, Cloudflare's systems were not breached thanks to its sophisticated multi-factor authentication approach.

Specifically, Cloudflare does not rely on SMS based authentication codes. Instead, it uses physical security keys. A physical key (a specialised USB device) uses a version of multi-factor authentication called Universal 2nd factor (U2F), which lets users log in by inserting the USB device and pushing a button on it. Once the device is linked to a certain site, users do not have to enter their passwords.

Key takeaways

The attack on Twilio demonstrates that while SMS codes add an extra layer of security, they can be by-passed. They may not be sufficient for sensitive IT systems as SMS (and email) authentication are less secure than other forms of multi-factor authentication.

As demonstrated by Cloudflare, organisations should consider adopting strong forms of multi-factor authentication such physical security keys or authenticator apps for sensitive systems and accounts. Organisations should also provide regular security awareness training to ensure staff know what to look for and what to do if they receive a suspicious text, phone call or email.

In addition, organisations should regularly review the level of access individual team members have for key systems and limit access to essential staff only. For example, if an employee with limited access to sensitive company data has their access details compromised, the risk is reduced compared to a breach of where they have access to the full suite of company data.

Three steps to strengthen the security of your critical accounts:

1. Identify all systems and accounts that have access to your sensitive systems and data.
2. Ensure multi-factor authentication is enabled for all sensitive accounts identified at step 1.
3. Implement stronger multi-factor authentication options (i.e. physical or app-based authentication) wherever possible.

More information

The Australian Cyber Security Centre recently published a guide: Protect Yourself with Multi-Factor Authentication.

For regular updates and insights on topics including cyber security, consider joining the .au membership program. .au members have access to a range of benefits including a partnership offer with Cynch Security, to help small businesses strengthen their cyber defences.