SecureITWorld

MFA Against The Brute Force Attacks

The Threat of Brutal Force Attacks

30% of Attacks Bypass MFA

SMS-based MFA being the most common and least secure type of MFA.

32.5% of businesses were targeted by a brute-force attack within a month.

What is a Brute Force Attack?

A brute-force attack is a method of gaining unauthorized access to a protected account through a

A seemingly endless stream of login attempts.

It works by hacking into login credentials, encrypting keys, and hiding URLs.

How to Prevent Brute Force Attacks?

01 Enhance public IP address with Geo location, ASN (Autonomous System Numbers) value for all the remote application logins.

02 A dashboard/graph can be used to identify login attempts from a different geographic area.

03 Identify the unknown ASN sources from the login, to analyze use of VPN by the user.

04 Train ML to link users to Geo and ASNs, and anomalies can be generated if users log in from different geographic areas.

Preventive Measures to Defend Against Brute Force Attacks

1. Configuring MFA to OTP-based authorization
2. Configure the application to be stopped if the user has abandoned the push notification three times within a very short time.
3. Configure the remote application to reject user's authentication from a different geographical area.
4. Train employees effectively on a regular basis. Inform them to not share OTPs. Not authorizing MFA to push notifications unless authorized by a user.
5. Inform the IT team on receipt of push notifications or unauthorized access.

To know more about the trending cybersecurity trends, updates, and preventive measures, visit: www.secureitworld.com now.