Multi-Factor Authentication – Benefits, Risks, And How You Can Get The Most From It To Ensure Your Organization's Data Is Secure

NEWS RELEASE BY **BIO-KEY INTERNATIONAL, INC.**

Wall, New Jersey | February 10, 2023 08:45 AM Eastern Standard Time

By Gita Karunakaran, Benzinga

Cyberattacks are on the rise everywhere today, with organizations and individual account passwords routinely targeted by hackers – especially where accounts are vulnerable due to a lack of additional layers of protection beyond the traditional password itself to help keep them secure.

According to **Microsoft's Digital Defense Report 2022**, the volume of password-based attacks has risen to an estimated 921 attacks every second – representing a 74% increase in just one year.

This is why companies in the cybersecurity space like **BIO-key International Inc. (**NASDAQ: BKYI)

that provide Identity and Access Management (IAM) solutions to enterprises look to Multi-factor Authentication (MFA) as a mandatory minimum standard when designing solutions to prevent unauthorized access to company systems.

The increasing widespread awareness of cybersecurity risks has propelled many companies to embark on their IAM journey by implementing a strategy that includes a variety of authentication methods that meet necessary requirements in security, usability, and flexibility.

What Is Multi-factor Authentication?

Multi-factor Authentication (MFA) is a core component of a strong IAM strategy. It's an authentication method that requires the user to provide two or more verification factors to gain access to an online system or account, which helps decrease the likelihood of a successful cyber attack.

The main benefit of MFA is that it would enhance an organization's security by requiring users to identify themselves using more than just a username and password. Passwords continue to be the weakest link in the chain and remain vulnerable to brute force attacks or theft by third parties. Having an MFA solution is therefore able to reduce the probability of hackers gaining access to company systems and accounts.

MFA may be based on a combination of two of three different types of authentication factors, including:

- Things you know, such as a password or PIN;

- Things you have in your possession, such as a token or smartphone;
- Things you are, such as biometrics like fingerprints, palm, face, or voice recognition.

The options chosen by each organization may depend on their risk appetites and budgets – but what is certain is that the cybersecurity and MFA market is poised for appreciable growth.

The global MFA market was valued at US $10.3 billion in 2020. The market is estimated to expand at an impressive **CAGR of 16.08% from 2021 to 2031** and is expected to exceed $51.37 billion by the end of 2031.

Some of the key players in the Multi-factor Authentication market include **Broadcom Inc.** (NASDAQ: AVGO), **Duo Security Inc.** (private), **Cisco Systems Inc.** (NASDAQ: CSCO), **ForgeRock Inc.** (NYSE: FORG) and **Entrust Inc.** (TYO: 7191)

MFA Is Great, But What About MFA Fatigue?

As MFA continues to gain prominence across the business landscape, it is seemingly becoming increasingly vulnerable to exploitation by cybercriminals. While there is no doubting the merits of MFA over mere password protection, MFA needs to be managed properly in order to avoid a phenomenon known as"MFA fatigue".

Even though having an MFA in place is a step in the right direction to stronger security, the process can become tiring and tedious on account of the multiple additional PINs, codes, and push notifications, instead of only a username and password that users needed to recall previously. This could result in MFA fatigue among users.

Cybercriminals who manage to hack into passwords are able to generate repeated push notifications in what is known as a brute force attack. While some users will be diligent all the time, MFA fatigue can result in some users inadvertently approving a push notification and granting full access to the hacker.

BIO-key May Have A Highly Secure And Nearly Fail-Safe Solution

According to BIO-key, although most organizations have begun to implement a variety of MFA methods as part of their IAM strategy, the best outcomes can only be achieved by deploying a cohesive solution across the entire organization. Deploying disparate solutions would make the proposition unnecessarily expensive and difficult for IT teams to manage.

BIO-key boasts flexible Identity and Access Management solutions that are integrated with their unique biometric authentication option – Identity-Bound Biometrics – making it easy for organizations to secure access using fingerprint, palm, and facial scanning.

BIO-key's single, unified IAM platform, PortalGuard, provides security solutions for a wide range of use cases and business initiatives, with Multi-factor Authentication, Single Sign-on, and Self-service

Password Reset abilities.

MFA with PortalGuard could be the most efficient and secure solution, says BIO-key – allowing organizations to consolidate and aggregate existing methods under a single, unified IAM platform, with the ability to add more powerful authentication methods like Identity-Bound Biometrics to further strengthen their cybersecurity as necessary.

To learn more about BIO-key's MFA solutions, visit the company **webpage**.

*This article originally appeared on Benzinga **here**.*

BIO-key is revolutionizing authentication and cybersecurity with biometric-centric, multi-factor identity and access management (IAM) software managing millions of users. Its cloud-based PortalGuard IAM solution provides cost-effective, easy to deploy, convenient and secure access to devices, information, applications, and high-value transactions. BIO-key's patented software and hardware solutions, with industry-leading Identity-Bound Biometric (IBB) capabilities, enable large-scale Identity-as-a-Service (IDaaS) solutions, as well as customized on premises solutions.

This post contains sponsored advertising content. This content is for informational purposes only and is not intended to be investing advice.

Contact Details

Catalyst IR- William Jones, David Collins

+1 212-924-9800

BKYI@catalyst-ir.com

Company Website

https://www.bio-key.com/

Tags

BIO-KEY INTERNATIONAL TECHNOLOGY CYBERSECURITY