nevis®

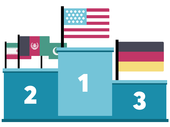
You can protect yourself against these attacks with MFA

Multi-factor authentication as a security mechanism and a key factor in the IT security strategy is an authentication process that combines and validates two or more factors (credentials).

The goals of MFA

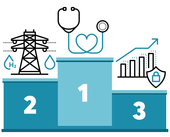
- → Integrating an **additional security level** in the authentication process
- → Fulfilling **compliance requirements**
- → **Identifying** authorised users and granting access to required resources
- → **Preventing identity theft** through the exploitation of weak passwords
- → Early **circumvention of attack methods** employed by cybercriminals
- → **Protecting sensitive data** against data misuse
- → **Optimising the user experience** with an intuitive and secure login

Costs of data hacks



The consequences of data hacks are enormous: a data breach will cost a company an average of **EUR 4.79 million**. This puts Germany in third place behind the USA with EUR 8.21 million and the Middle East with EUR 5.99 million.

Costs by industry



Sorted by industry, the healthcare sector clearly dominates the ranking with the highest costs on average: In 2020 alone, data leaks resulted in costs of **EUR 7.15 million worldwide**, followed by the energy sector and the financial sector in second and third place, respectively.

An extra layer of security does no harm

x2 **Two-factor authentication = 2FA**
→ two validation processes

x? **Multi-factor authentication = MFA**
→ more than two validation processes

The greater the interaction between authentication factors, the stronger the protection against data misuse.

The four factors of authentication

Knowing

A factor known only to the user.

Possibilities:
Password, PIN, answer to a security question, transaction number, one-time password (OTP)

Having

Use of a mobile additional device that queries relevant information during the authentication process.

Previously: TAN generator, hardware token

Today: Smartphone + authentication app for generating a one-time password

Being

Biometric factors that are used to identify the user.

Possibilities:
Fingerprint, iris, facial profile or pitch of the voice

Location

The user's IP address is queried. This can be added using the location based on GPS data or the duration of use.

What Exactly Does MFA Prevent? The Top 5 Methods of Attack

*'Armed with **personalisation and credibility**, I'll get what I came for'*

Phishing

A hacker pretends to be a trustworthy source and sends their victim a fake email. The email instructs the victim to perform an action, for example, using a link to log into a bank account. The link is malicious, which means that a victim who clicks on it will be directed to a manipulated website, not to the expected website. This fake website is configured so that the hacker can record the victim's login details and then gain access to the account.

*'I am reading **every word** you type.'*

Keyloggers

A keylogger is a monitoring program that is usually installed on the victim's device by a virus. Since it records every keystroke the user makes, it also captures login details, passwords and answers to security questions or banking data. This data is then used for malicious purposes.

*'I'll try **every combination** until I succeed.'*

Brute-force attacks

In a brute-force attack, hackers use a program that generates every conceivable combination of password and user name. They use these variants to try to gain access to an account. Such an attack can have serious consequences, ranging from the hijacking of company systems to the spreading of malware and spam advertising all the way to hacking into user accounts.

*'I know you use your **login details on multiple platforms**.'*

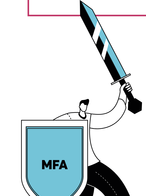
Credential Stuffing

Credential stuffing is a special form of brute-force attack and is currently used very frequently by hackers on the internet. These attacks use passwords that were either published as a result of data breaches or harvested illegally. Cybercriminals enter these passwords in as many websites as possible in the hope that the same login combinations of password and user name are used simultaneously across multiple services.

*'I'm **eavesdropping** – you just can't see me.'*

Man-in-the-middle attacks

A man-in-the-middle attack (for short: MITM) is when a hacker uses a software program to observe how a victim interacts with another application for example, on a public WLAN network. The hacker's program runs in the background and can capture login details, cause damage to data or even sabotage communications. Although MITM attacks against public hotspots are less frequent due to the adoption of SSL and modern browsers such as Google Chrome, they are still used to mount highly sophisticated attacks.



With all five methods of attack, the password is a critical vulnerability that can be eliminated using MFA. Even if cybercriminals manage to crack the first authentication factor of 'knowledge', the game is up when they encounter the second level of MFA.

As a result, MFA offers reliable protection for sensitive company data because it repels a broad range of attack methods. It also promotes the zero-trust strategy in the modern cyberthreat environment.

nevis®

Learn more about multi-factor authentication at Nevis, Switzerland's market leader for customer identity and access management:
nevis.net