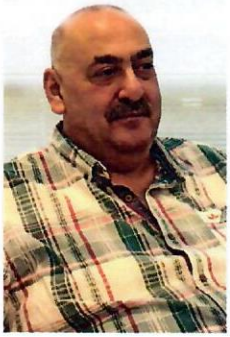
Dr Mounes Kayyali
IDENTITY THEFT: PASSWORD SECURITY RISKS



>> Dr Mounes Kayyali, CEO, The Kernel, an information and network security services, talks about security risks associated with only using passwords in user authentication.

Many organisations still focus only on passwords in user identification. Especially when users choose their own passwords, it inevitably leads to security risks - and this, of course, is an open invitation for cyber criminals.

In a recent report on IT security in Germany, the Federal Office for Security in Information Technology (BSI) warned against the increasing threats from identity theft.

The problem lies not in the changing threat landscape, but in the lax attitude toward authentication. Many organisations still focus only on passwords in user identification.

> "It seems paradoxical that almost every week cyber attacks make headlines in the news, but companies still implement outdated security mechanisms."
>
> **DR MOUNES KAYYALI, CEO, THE KERNEL**

EASY GAME FOR THE ATTACKERS

New malware makes the situation worse, but it is only a part of the criminal infrastructure in this area.

The data collectors gain access to data via phishing, drive-by exploits, breaks in servers, keyloggers and spyware. Specific malware can not only record access data but also hack poorly protected accounts with repeated login attempts.

TRY AND ERROR PRINCIPLE

Unless there are industry-specific standards, there are two basic principles that can be applied to improve identity protection:

Basic protection: This is about the basic protection of all business processes in order to avoid the greatest risks as soon as possible. In identity management, these would be mechanisms to protect any account against unauthorised access, even if it is considered uncritical.

Core protection: Processes and accounts are assessed according to their importance. Particularly critical accounts get special, stronger security clearance, in order to put a special firewall around critical assets in case of an attack.

MECHANISMS FOR BETTER IDENTITY PROTECTION

These theoretical approaches can be put into practice by relatively simple means. An example of basic protection is the consistent use of password managers for all accounts. The number of accesses increases the number of passwords required. Secure passwords are long and they are difficult to remember. In almost every organisation, employees use passwords multiple times to make them easier to remember.

As a rule, users do not distinguish between private and corporate accounts. Attackers are aware of such double use and exploit the security risk. Intercepted access data are systematically synchronised with other accounts in order to gain access.

Password manager allows centralised backup and account administration in one solution with only one password. This eases the burden on users and thus companies can increase the basic level of protection. This improves overall security and blocks numerous attack vectors.

Nevertheless, secure passwords can also be stolen or cracked. Therefore, accesses with higher security clearance should be protected according to the principle of core protection with appropriate precautions. Admin accounts or management board accesses, for instance, should be protected with appropriate encryption.

Due to the current boom in the IT security industry, new interesting concepts are entering the market almost every day. However, only a few approaches reach the almost classic two-factor authentication. The protection of something you know (password) and something you have (hardware) has proven effective with particularly critical corporate assets. New tools often seem interesting, but they are also often unsuitable in practical terms, especially if they do not meet local standards.

Encryption of critical information ensures protection even in a case of a successful attack. Even if criminals have access to the network, retrieved will be only encrypted data and that's useless. Of course, it is always difficult for security departments to comply with the theoretical approaches of authorities. Organisations must be able to clearly identify users. Without an appropriate solution, there is a risk of identity theft. At the same time, the users should not be overloaded, otherwise, there is a risk of workarounds such as multiple passwords use.

It seems paradoxical that almost every week cyber attacks make headlines in the news, but companies still implement outdated security mechanisms. There are easy-to-implement approaches that significantly increase the protection level - without costly restructuration of IT security architectures.

The risk potential of stolen identity is enormous. Attackers can completely infiltrate a network and can remove almost all existing security mechanisms. Basic protection of simple user accounts and core protection for particularly important accounts ensure protection against a large number of threats and are relatively easy to implement. ■

The views expressed in this article are Dr Mounes Kayyali's own opinions and not necessarily those of Channel Middle East magazine.