NJORD Estonia: Deficiencies in cyber hygiene will prove to be expensive

Tips for secure authentication

Secure authentication in a digital society is all-important. To ensure security, organisations should enact measures that allow users to use the systems in the safest possible way. It's long past the time when relying only on a username and password for authentication was adequate. Cyber-attacks are not the "hacking" we know from the movies. It is much easier for the attackers to gain access to a system by using weak, stolen or otherwise compromised authorisation measures. Identity has become a new field of security in combating cyber-attacks.

By harming the business activities of companies, attackers try to extort them to giving large sums of money. Even if the organisation decides not to submit to blackmail and abandons the compromised system, it still involves both the reputation and the material damage.

To ensure security and alleviate risks, it is advisable to consider more effective measures. One option is two-factor authentication, which as the name implies, requires two different authentication mechanisms. The most common is asking the user for something they know (such as a password) and for something they have (such as a smart device or smart card). When authenticating by using a smart card, the person is asked for a password or PIN-code. By inserting the card to a smart card reader, it is established that the card is in the possession of the user. Using a smart device for two-factor authentication, the user is identified by asking them for a password and reacting to a notification that is sent to the device.

Of course, all passwords should be as strong as possible. However, considering how many different services we all use which require some sort of password, it is perhaps unsurprising that most of us take the easy way out and re-use one simple password with different service providers. A strong password is inevitably more difficult to remember.

Additionally, there are services that cannot be accessed without relying on passwords. The most well-known examples are perhaps certain wallet services, which cannot be accessed if the user loses the password or someone changes it.

PKMaaS – Private Key Management as a Service

A question arises as to what will happen if passwords are lost. Let's imagine a situation where the estate of a deceased person is kept in a virtual wallet, the password of which the successors do not have. In that case, the assets would be lost in cyberspace forever.

Managing the most important passwords and private keys in some way should be considered so that they are not lost, even if something happens to us. Unfortunately, it is difficult to find a secure and reliable service that alleviates the risk of losing sensitive passwords. One possible solution could be a password management service, which, however, might not be suitable for everyone in terms of data security. There is also the question of what will happen if the password, which allows access to the management service itself, is lost.

Perhaps in the future, there would be space for a centralised solution for managing sensitive data. An option could be something akin to a deposited will, i.e. depositing the most sensitive data to a secure place. However, passwords may need to be changed from time to time, due to data leaks or general cyber hygiene. A notarial service could consequently prove to be overly burdensome and expensive.

Using the Estonian ID-card infrastructure could be considered to create a new service for managing, but also sharing, sensitive passwords and private keys in a way which, considering the nature of digital measures, is sufficiently quick, easy and dynamic, without conceding in security.

HENRIK LINK
SENIOR ASSOCIATE

(+372) 66 76 440
HENRIK.LINK@NJORDLAW.EE

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE