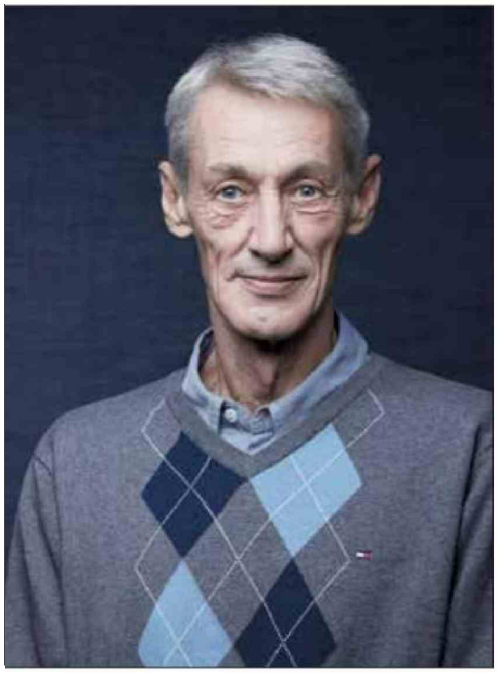
ŽARKO KECIĆ ACTING DIRECTOR OF THE SERBIAN NATIONAL INTERNET DOMAIN REGISTRY



Modern Business And Domains

RNIDS
Registar nacionalnog internet domena Srbije

Owning a domain name gives you a free choice of where and on what terms your company's web site is hosted, and lets you exchange e-mail using an address that identifies your organisation

Why it is important for a company to own its own domain name and for it to be a national one, how RNIDS provides users with permanent domain availability, and the importance of information about threats on the Internet; the Acting Director of the Serbian National Internet Domain Registry, Žarko Kecić, speaks with e-Serbia.

• Modern business takes place to a great extent online, and a company's survival has become almost impossible without an Internet presence. How is this related to domains and what is the role of RNIDS?

- Development and expansion of the Internet has helped to make business faster and more efficient. Online business allows companies continuous presence and communication with partners and customers, regardless of working hours and physical location.

All Internet users use the Domain Name System (DNS) to connect to the appropriate Internet service. Because of its specificity and its global role, the DNS system must always be accessible, reliable, fast and flexible, because it makes domain names accessible and visible on the Internet. So, an internet domain name is the basis of a company's online presence, enabling it to create web sites and exchange e-mails with anyone at any time.

RNIDS manages a registry of national Internet domains (.rs and .срб) and an infrastructure that allows them to be permanently accessible. Key RNIDS services must be operational 24/7/365, since the Internet also works without interruption

RNIDS manages a registry of national Internet domains (.rs and .срб) and an infrastructure that allows them to be permanently accessible. Key RNIDS services must be operational 24/7/365, since the Internet also works without interruption. If the critical IT systems supporting the registry fail, all Serbian domains would be unreachable, web sites on .rs and .срб domains would not be visible, online shops would stop working, and domain users would not be able to exchange e-mails.

• Why is it important for a company to be present on the Internet in the right way, that is to have its own internet domain name and for that to be a national one?

- Online presence is possible in many ways - companies can be present on social networks, online portals and business listings and, of course on their own website on their own domain name.

The use of social networks and portals has its advantages, but they are controlled by someone else and there

is no guarantee that the terms of use will not change. It is a fact that many social networks, portals and listings have ceased to exist, some even without notice, which practically means the online disappearance of companies whose internet presence and business are based on them.

Companies that have their own domain name have full control of their online presence. Having a domain name enables a free choice of where and on what conditions the web site will be hosted, allows exchange of e-mail messages with an address that identifies the organisation, and it provide global access to other Internet services offered by the company to its users.

The use of national internet domain names allows companies to show their business presence on the territory for which these domains are intended. In addition, national domains often provide a higher level of security than generic ones (.com, .net, .xyz ...), through somewhat more stringent registration terms and requirements that user data is accurate and up-to-date, which makes them less attractive for misuse. Also, national domains have an advantage in local Google searches, where the results that are geographically closest to the location are displayed first.

• How does RNIDS ensure that their Internet domains are permanently available?

- RNIDS takes its responsibility very seriously and seeks to organise and develop its technical and human capacities according to modern trends. The task of ensuring that RNIDS key services and systems are always available is not easy, especially with the number of staff and the limited resources available.

We base our business on best practice and the experience of the world's leading top-level domain registries, using current technical solutions that enable a high availability of services. RNIDS's key services work in multiple locations and enable continuous service provision even in case of equipment malfunction or interruptions in communications.

DNS systems that are responsible for the .rs and .срб domains have worked non-stop since the establishment of RNIDS. DNS-OARC measurements show that RNIDS belongs to a group of only seven top-level domain registries whose DNS services have been available 100% of the time since these measurements began.

RNIDS has implemented three types of domain protection - all three types significantly reduce the risk of 'theft' of domains, and it is up to the user to choose which one provides the required level of protection

• RNIDS is the only national internet domain registry in the world that has three levels of domain name protection. What is this actually about?

- There are more and more cases of 'theft' of domains, which apart from lost reputation and profit can lead to the theft of sensitive business data, so along with accessibility we pay special attention to the security of domains under our authority.

In the interests of its users, RNIDS has implemented three types of domain name protection. All three types of protection significantly reduce the risk of the 'theft' of domains, and it is up to the user to choose which one provides the necessary level of protection.

The basic level of protection is 'Secure Mode', which is simply activated through a registrar where the domain name is registered. In this case, for each change of domain-related data, confirmation will be requested before the change is allowed. A slightly higher level of protection is provided by 'Client-Side Lock', which should be sufficient in most cases. The highest level is provided by 'Registry Lock' service. This service provides the highest level of protection but requires additional administrative and technical activities of the registry and is therefore charged separately.

• Why is domain security among the most important issues today?

- The DNS service is one of the key internet services, which leads to frequent attempts to abuse it. One of the most common ways of abuse is redirecting users to Internet services controlled by the attacker, with the aim of collecting sensitive personal or bank account data or user credit card details.

RNIDS ensures domain security to the best of its ability, but it is very important that users take the necessary steps to protect their online presence. We therefore try to inform them about the importance of the Internet domain names for doing online business, about risks and types of abuse, and steps they should take to reduce the risk. Properly configured DNS servers provide a reliable service for their direct users, but they also protect other Internet users from various types of abuse, and also minimize the risks that they may be used to launch attacks to other systems. ■