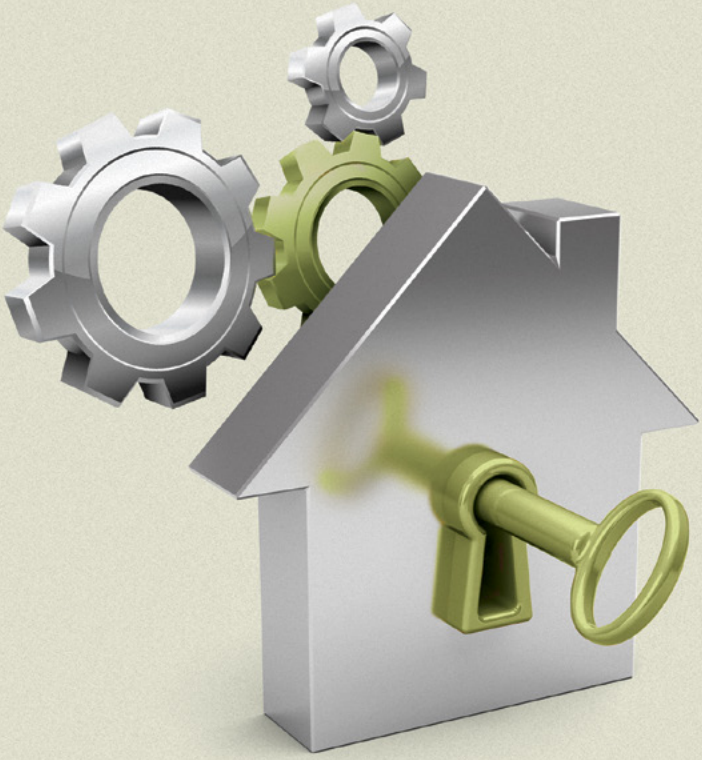


THE ABC OF SECURITY FOR WEBSITE OWNERS

si·cert
VARNI NA INTERNETU
register.si

THE ABC OF SECURITY
FOR WEBSITE OWNERS

For additional information visit:
SI-CERT - *www.cert.si*
Varni na internetu - *www.varninainternetu.si*

Slovenian Computer
Emergency Response Team
2013

CONTENTS

YOUR ONLINE PRESENCE

The Internet is part of our everyday life. The boundary between the real and the virtual world is becoming increasingly blurred. Most companies have a web presence, and many also offer online shopping. Various groups in our society use the web to communicate and collaborate with their members, and as individuals we can quickly present our impressions and opinions in a blog. Yet with all the advantages of the Internet, we cannot afford to forget about traps and dangers.

So what should we watch out for, and how can we avoid difficulties online? Your website is usually set up for you by an outside partner, but you remain responsible for its operation, so you have to keep control over it and ensure that it is maintained.

The guidebook offers some useful information, whether you already have a web presence or are just planning to set-up one. It was produced in collaboration with the awareness-raising programme **Varni na internetu /Safe on the Internet** from the national response centre for network incidents **SI-CERT** and the national registry for the Slovenian top-level domain .si, **Register.si**.

VARNI NA INTERNETU si·cert register.si

Your website is set up by others, but you have to maintain control and bear responsibility.

SELECTING YOUR HOSTING PROVIDER AND WEBSITE CREATOR

Reliable partner

Choose a reliable and responsive provider. Your decision should not be influenced just by the price of the package, you should think about what really matters. Perhaps the fact that the provider is just around the corner? Are you interested only in the capacity of the server and connections, or in additional services that are offered?

Phases of setting up a website:

(1) PLANNING A WEBSITE

What do you want to present? Just your contact details, or a full website with a catalogue and perhaps even an online store? This will determine your decision about the web content management system. The smaller your requirements, the simpler the system that you can select. The more complex it is, the more maintenance it will require. The most common **Content Management Systems (CMS)** include: Wordpress, Joomla and Drupal. Simple web sites can actually be set up with HTML pages only.

My friend's son

Small companies and societies often choose an acquaintance to design and set up their websites. This sort of "friend's son" does actually know about computers, but next year he might be off on a student exchange abroad, right when your website crashes. The occasional website designer might perhaps know only one platform, and cannot and does not know how to adapt to your needs.

The fact is, the days of "garage" Internet wizards have passed, and you need to set up your website with adequate professional support.

(2) SETTING UP THE WEBSITE

Your website will be "set up" on the Internet through a **hosting provider**. In making your selection, apart from price your criteria should include:

1. the satisfaction of other clients with this provider,
2. availability of provider – how and when you can contact them in case of difficulty,
3. whether they provide regular security backup of data and its recovery in the event of difficulty,
4. whether you have the option of packages with additional website protection, and what this protection involves (for instance identifying unauthorised access and defence against DDoS attacks).

By leasing a web server, you have rented business premises on the Internet. The method of operation and the security of documents on the server are your job. You regularly clean your office, you tidy up the documents in it, change dead light bulbs and lock it. Similar maintenance tasks await you on the web. It is not essential for you to do all this yourself, and it is highly likely that you will contract an outside provider to do most of the tasks. And that provider must have appropriate knowledge and experience. Many difficulties in online operations result from those involved not being aware of what exactly they need to take care of.

Select the most appropriate package from your hosting provider depending on the requirements of your website.

Home or abroad?

The Internet has erased borders, so why not get hosting abroad? First think about what you are getting for the price. Avoid free hosting, since they do not offer support when you have problems (even if it is Google). How will you deal with some complication between yourself and a provider in Germany or the USA? With a local provider it is usually smooth and quick. Servers outside the EU can also be problematic from the legal standpoint if you store personal data on them.

(3) MAINTAINING A WEBSITE

The most common cause of difficulty on a website is poor or non-existent maintenance. I**f you do not provide this, it is only a matter of time before one complication or another arises.** Eliminating the consequences of website abuse will take a certain amount of time and money, while lack of access to your site or online store can cause loss of customers, commercial damage and will certainly not contribute to your image. The web is a dynamic environment and your website will have to keep pace with its evolution.

If your company has IT personnel, they should of course be familiarised with the content management system and should assume responsibility for maintenance. Otherwise you will need to come to an agreement with your website creator, hosting provider or another partner. In any event, regular maintenance of your website should be the job of a reliable and professional provider.

200 hacked each month

Between December 2012 and May 2013, SI-CERT dealt with **1300 cases of Slovenian corporate websites** that had been "defaced": a third party had broken into their server and altered the home page with their own message. In some cases the hackers had also exploited the server for their own criminal purposes. All these cases are the result of badly maintained content management systems.

Maintenance works:

- ☑ checking the operation of the website (daily)
- ☑ monitoring news about new developments for the web platform and operating system (weekly)
- ☑ upgrading the web platform (monthly and immediately for critical errors)
- ☑ updating contact data for the domain (as necessary or at least once a year)

Anyone home?

It will not necessarily be you who first notices abuse of your website. You may well receive notice of a security incident from the SI-CERT response centre, and at that time we have to find your e-mail address quickly. Your website could be completely erased, so contact data on your website cannot be seen. In such case it is important for us to get to you quickly. Usually we rely on the registry of Slovenian domain holders. **Do you still know what contact you gave when you registered your domain?**

DOMAIN

The **domain** is the address of your web presence, and we could say that it is an important inventory of your company or society. Proper management of the domain also contributes to your security on the web.

First a few basic terms:

Registry is the organization that administers the top-level domain. It ensures the database of registered domains, the functioning of top-level domain servers, it develops and maintains the domain registration system and provides other services tied to the top-level domain. One registry exists for each top-level domain.

The **registrar** has access to the domain registration system and performs registration, extension and other services associated with the domain on behalf of clients. Registrars can offer their customers domains with various suffixes, and each registry can have several registrars..

The **holder** is the party that registered the domain and has acquired, for a specified period, the right to avail himself of it and use it as a web and/or e-mail address.

You can also register a domain under some other top-level domain. You can find the instructions for registration online. The recommendations and instructions below apply to Slovenian domains, but they are also generally applicable for domains with other suffixes.

What you need to look out for in domain registration:

1. **You are the domain holder.** Since only the holder can administer the domain, be sure that the data on the holder are correct. Do not let your website creator be listed as the domain holder. If the creator is listed, it should only be as a technical contact. It can happen all too quickly that after a few years you find out that your **web identity, which is the basis for instance of the company's entire operations**, is in the hands of someone you terminated commercial contact with a long time ago. In addition to the **title and address of the holder**, it is essential that when you register you **give a working e-mail address**, if possible one that cannot be accessed by all employees. All official communication between the registry and domain holder is conducted via this e-mail address. **Whoever has access to that address can confirm the deletion of the domain, a change of registry or even the transfer of the domain to someone else.**
2. **The technical contact knows how things work.** The technical contact for the domain should be someone who knows how to set up your website and arrange entries into DNS servers, and will be able to respond to communications about technical difficulties and about any potential abuse of your website.
3. **Selection of registrar.** There are a large number of registrars for the .si domain. In selecting the right one, think about what you want: personal contact, advice, help or perhaps a simple, automated registration; a range of additional services or a phone call if you have forgotten to extend the domain. You will perform all tasks relating to domains (e.g. renewal, change of data, entry of domain servers) **exclusively via the registrar**, so check how these procedures are conducted at the selected registrar and how responsive the registrar is.

When you have a domain, you must not forget about it entirely

You register the domain for a period of one to five years, depending on the agreement with the registrar. After that period expires, it needs to be **renewed**, which the registrar will do on your behalf. Failing this, your website and all e-mail addresses under the expired domain will **stop working**. The domain will "wait" for you for 30 days, after which time someone else can register it. If you have forgotten until when your domain is registered or even who your registrar is, you can verify all this online at the "WHOIS" page of the registry: **register.si/whois**. Also note the data on the domain holder that WHOIS gives you. If they are not correct, immediately notify your registrar. **Inaccurate data can mean deletion of your domain!**

What do you do if you find out that someone else has registered "your" .si domain? If you can show

1. that the domain is the same or very similar to your trademark or company title,
2. that the holder has no legally recognised interest regarding the registered domain and
3. that the domain has been registered or is being used in bad faith,

you can instigate a domain dispute at the registry by means of the procedure for **alternative domain dispute resolution** (ARDS).

As holders you must also be aware that you are responsible for the selected domain not violating any laws or rights of other persons.

Why use a domain under the national suffix .si?

The advantage of the .si domain in terms of security is quite clearly that the registrar operates in the Slovenian language and in the same time zone, which eases communication and facilitates rapid responses where there are complications and difficulties, and all those involved are subject to Slovenian law.

LEGISLATION

You are responsible for the content on your website. If someone hacking into your website sets up tools that harm other web users, you may also be liable if you have not taken appropriate action upon being notified of this activity.

The web is also subject to Slovenian legislation. You can review the relevant laws and articles at **www.cert.si/zakonodaja**, while we highlight certain areas that you must be aware of as a website owner.

RESPONSIBILITY

The Electronic Commerce Market Act (ZEPT, Article 11) provides that the hosting provider is not responsible for information that you, as the customer, place on servers, until they are aware that it might involve unlawful activity. As soon as they are aware of this, they must remove or prevent access to such information. **Where there are possible complaints about content placed on your website, the provider therefore has a clear legal duty to prevent access to it if there is a complaint.** Moreover, in their general terms and conditions, the provider may set out additional rules that need to be taken into account when using their services.

ADVERTISING AND SPAM

Sending out advertising without the prior consent of the addressee is counter to Slovenian law. The area of unsolicited e-mail (spam) is regulated by four different laws: the Consumer Protection Act, the Electronic Commerce Market Act, the Electronic Communications Act and the Personal Data Protection Act.

The excuse that you obtained addresses on publicly accessible websites is insufficient. It does not constitute consent to spam!

INTELLECTUAL PROPERTY

You must ensure, together with the website creator, that you have the relevant authorisation to use content. **If you found a picture "on Google", that in no way means that you can use it.** It may be someone else's property, and if it has been made public, this does not necessarily mean that its copyright owner has allowed free use of it! Certain content can indeed be used freely, and some under specific conditions (e.g. Creative Commons), otherwise you need to obtain permission from the rights holder. .

USER TRACKING AND COOKIES

Web cookies are small text files that a web server, upon being visited, offers the visitor's browser, and they are usually stored on their computer or mobile device. On subsequent visits the stored cookie is sent once again from the browser to the server. Cookies are used to store settings, manage individual users' sessions, differentiate between users and track them on the website (and possibly across several websites). **If you use cookies on a website, in accordance with the Electronic Communications Act (ZEKom-1) you must notify users** of the type of cookies you are using and obtain their consent.

You can find out more about cookies in the **Information Commissioner's guidelines**.

PERSONAL DATA PROCESSING

If your server stores or processes personal data, in accordance with the Personal Data Protection Act you **must register personal databases with the Information Commissioner**. If you lease a server abroad, check whether the export of personal data to that country is permitted (data export to EU Member States is permitted, but in the USA only to companies that have signed the relevant agreement). You can enquire at the Information Commissioner about this, and also check whether you need to sign a contract on personal data processing with the hosting provider.

POSSIBLE ABUSE

Consequences of hacking:

1. disrupted operation or failure of website,
2. loss, change or theft of data,
3. endangering visitors to your website,
4. blocking your e-mail,
5. blocking your website.

HOW DO YOU GET HACKED?

Most commonly hackers find security loopholes in an unmaintained content management system or server. They can also gain access by stealing your password or guessing it if the password is simple. We list some of the most common forms of hacking below.

DEFACEMENT

The appearance of the website is altered. Defacement is like putting "graffiti" on your website, whereby the perpetrator seeks to express his opinion, be it personal or political, or just wants to leave his signature. Instead of a presentation of your company, the visitor to your website will see the message: "Hacked by Hmei7" or some pronouncements about freedom for Palestine.

PHISHING - STEALING PASSWORDS

The **attacker exploits your website to set up a fictitious copy** of e.g. a bank website, and via your website attempts to steal passwords and then also the money of that bank's customers. Attackers also use phishing techniques to steal other data: e-mail passwords, credit card numbers, user accounts and so forth. The attacker generally lures victims to the phishing website via adapted e-mails in which he notifies them that, for various reasons, they must once again enter their data, and the link leads to the tampered phishing website on your server.

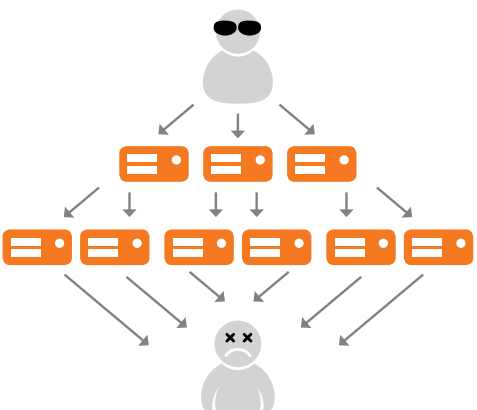
MALICIOUS CODE ATTACK

Attackers exploit your website to spread malicious code: viruses, Trojan horses and worms. The attacker injects software code on your website that attempts to exploit weaknesses in the visitor's browser or in browser plug-ins. In this case you are actually **a participant in the infection of your website visitors' computers**. These infections may result in data theft from the infected system or financial damage. **For this reason you must act as soon as you find out that your web server is being used to spread malicious code.**

DISABLING WEBSITES

Your website has become inaccessible because of a DDoS (Distributed Denial-of-Service) attack. You could be subject to an extortionist from a distant country, an angry customer or former employee, or even the competition. If you had warning of the attack, keep a copy of all communication and keep as much data as possible on the offending traffic.

You can also find yourself on the other side, where an attacker hacks into your server and then uses it to attack other websites. In December 2012, several dozen Slovenian web servers with unmaintained Joomla content management systems were abused by attackers from abroad. After hacking into the servers, they loaded their own software onto them and then used them to attack banks in the USA.



RECOMMENDED MEASURES

You can reduce risk by taking some simple steps: ensure you regularly update your web server and the installed content management system, be careful in selecting passwords and limit logins to your server to your usual Internet locations.

1. **STRONG PASSWORD.** In selecting a password you need to be careful not to make it too simple or common. It should be made up of various characters (capital and lower case letters, numbers and symbols) and should be at least eight characters long. The biggest security risk is default user names, such as admin, administrator, and passwords such as 123456, test123 etc.
2. **RELIABLE SYSTEM.** You should only log in to work on a website from trusted systems. Many abuses are a result of logging in from infected, publicly accessible systems, such as from a internet cafe or library.
3. **REGULAR UPDATING.** Adequate monitoring and updating of the server and content management system will ensure protection against the majority of attacks. The person maintaining the website must regularly monitor security notices from the content management system developer, and diligently install fixes for it and for all files used. If you do not carry out security updates yourself, you must entrust this task to a contracted maintenance provider.

More advanced websites that store personal data or perform financial transactions (online stores) should probably be checked with an independent security audit and a penetration test. A security check will provide better results if you select an independent company that regularly provides this service.

What should you do if your website is attacked or hacked?

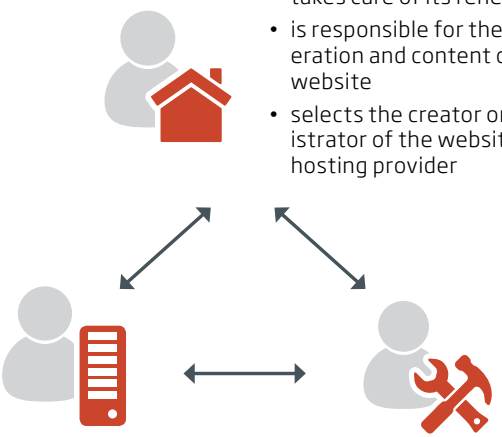
If you notice that there is something wrong with your website, and you suspect unauthorised access or hacking of your website, take the following steps:

1. Get in touch with your server administrator or hosting provider where you have leased a web server; make sure you protect the evidence of a hack: in particular, the perpetrator's files and changes to the system and log files. Be very careful not to change the specified files and to store them in their entirety together with appropriate time stamps (creation time, changes and access to file).
2. Report the hack to SI-CERT via the e-mail address: **cert@cert.si**. In your message, describe the signs of hacking and the circumstances that you know of. SI-CERT will offer you further assistance in investigating the hack, in providing extra protection for the server and will carry out the necessary communication with others involved (these may be Internet providers, CERT centres abroad and where necessary, law enforcement authorities).

(!) The majority of abuses originate from already known vulnerabilities in content management systems. **For this reason regular maintenance is the most important thing**. Updating ensures that you close security loopholes. This work should be done by someone who is technically familiar with maintenance of servers and content management systems.

Attackers do not plan their selection of victims. They find the majority of them through web search engines or random testing. It is only when they get to your website that they decide in what way they can use it most profitably: to spread malicious code, attack others, or perhaps you have certain data on your site that they can cash in directly.

ALLOCATION OF ROLES



WEBSITE OWNER

- is the domain holder and takes care of its renewal
- is responsible for the operation and content of the website
- selects the creator or administrator of the website and hosting provider

DEVELOPER AND MAINTAINER OF WEBSITE

- is the technical contact at the domain
- designs and creates the website
- maintaines entries in the DNS server
- removes errors
- monitors advisories and regularly installs updates for the content management system

HOSTING PROVIDER

- ensures operation of the server
- ensures Internet connectivity for the server
- by agreement may also take responsibility for the DNS
- takes over server maintenance, if this service is offered in an appropriate package

LIST OF CONTACTS

Who can you turn to in difficulty?

1. Website failure

First, approach the developer that set up your website and maintains it for you. If necessary, they will contact the host and find out why the difficulty arose.

2. Website inaccessible

Contact the website maintainer, who will find out why the server is inaccessible. If there is a distributed attack on your server, contact the hosting provider and the SI-CERT response centre for network incidents: **cert@cert.si**.

3. Interruptions in domain accessibility

Contact your registrar.

4. Hacking or abuse of website

Contact the SI-CERT response centre for network incidents: **cert@cert.si**.

TOP 5 RISKS

1. Defacement of website

Your website shows a message where the intruder boasts of hacking you. You have allowed this to happen because of poor maintenance of the web server.

2. Website exploited by criminals

After hacking into your web server, criminals install a virus that will infect the computers of your visitors. They can install software for web attacks on other servers or install on your server fictitious websites for a foreign bank (phishing) and steal money through them.

3. Theft of personal data or password

By hacking, the perpetrator can gain access to databases, and often also to the personal data of your customers. By phishing they can steal the passwords of other users.

4. Deleted data

The hacker deletes data on your website. This might be done by a competitor, terminated worker, a blackmailer whom you did not wish to "pay off", or someone that hacked in through your server and is now removing traces they left behind.

5. Loss of domain

You forgot about your domain, so now it has expired and no longer functions. If the contact details are not up to date, you will have some difficulty reactivating it. In the worst possible case, you may even lose the domain and someone else will take it over.

TOP 5 TIPS

1. Find someone to do maintenance

When you set up the website, someone must provide regular care for it. If you yourself lack sufficient expertise, you must entrust the task of maintenance to a professional provider and also pay the proper price for this.

2. Price is not everything

In selecting the host, do not look just for the lowest price, but also at what the host offers, what kind of experience others have with that host and whether difficulties will be rapidly resolved. If the host is abroad or you have chosen free hosting, solving problems could take a long time.

3. Website protection

Limit access to your website to known locations, regularly install software updates on the server and choose sufficiently strong passwords. Enquire whether the host offers additional protection packages.

4. Backup copies

Regularly make backup copies of content on your server. Ensure records of access and errors in log files. Both will be important in the event of your server being hacked and in a loss or change of data on the server.

5.Maintain control

The operation of the server is your own responsibility, and if you are notified of any abuse or hacking, you must respond appropriately. You must be listed as the domain holder in order to confirm any changes to it.

THE ABC OF SECURITY FOR WEBSITE OWNERS

si·cert

VARNI NA INTERNETU

register.si

REPUBLIC OF SLOVENIA
MINISTRY OF EDUCATION, SCIENCE AND SPORT