White Paper

Web security is within your reach. 10 ways to keep hackers in check and ensure safe web resources.

By Marsel Nizam
Head of Web Security Development, Bitrix, Inc.

April 2010

CHAPTERS

INTRODUCTION

46,541 – this is the number of zombie computers added to the ranks of the botnets[1] on a daily basis. The number of sites and pages infected with malware on the web is capable of doubling in a span of 6 months, and was around 640,000 websites and 5.8 million web pages toward the end of 2009[2]. Of those infected entities, 77% of them are legal websites which for one reason or another have been infected, that is to say, that they are unwilling or even unknowing victims producing more victims. About 210,000 websites or about 2 million web pages become victims of hacker attacks per month. In the last year, this indicator grew 671%[3]. $234,244 is the average cost to organizations which have suffered security breaches.[4] Despite the clear danger, 41% of companies consider themselves underprepared against potential hacker attacks[5].

The numbers give one pause, do they not?

There is a widely held view that there are lies, damn lies, and statistics. Perhaps it would be preferable to believe that such numbers are simply the product of a worldwide conspiracy on the part of software security companies to sell defenseless customers more products. However, launching an unprotected website and waiting for the first attack will quickly dispel this thought: on average, you will have to wait 1.3 seconds.

Botnet – a network of zombie computers united by a centralized control system. A botnet carries out commands given by the control center which can be, for example, the sending of spam, a DDoS attack, or tracking the actions of a user.

Zombie computer – a member of a botnet, controlled by a backdoor program. The backdoor programs are controlled by a distant malicious person, and can be used without the knowledge of the owner of the zombie computer to perform predatory or illegal actions.

A computer plague has spread over the world. The remains of civilization are assaulted from all sides by hackers, their weapons blackening skies and monitors alike. Every day brings a new set of victims. Network attacks blow new holes in protection technology. Security technology developers can't handle the pace of development and themselves become victims of the computer underworld.

This type of apocalyptic scenario is easy to envision when one analyzes modern trends in the field of web security. But is it really like that? Has the online community

[1] Symantec Global Internet Security Threat Report, April 2010, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

[2] Ilinor Mills, "Web-based malware infections rise rapidly, stats show", October 2009, http://news.cnet.com/8301-27080_3-10383512-245.html?tag=content;col1

[3] Dasient, White paper "Drive-by-Downloads,Web Malware Threats, and Protecting YourWebsite and Your Users", https://wam.dasient.com/wam/info?prod=18

[4] CSI, Computer Crime and Security Survey 2009, http://gocsi.com/survey

[5] McAfee, "In the Crossfire. Critical Infrastructure in the Age of Cyber War", 2010, http://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf

become the hostage of ultra-powerful evil elements? Is there a way to protect your website from cyber-attacks and guarantee uninterrupted business?

This document contains the viewpoint of Bitrix, Inc. concerning the state of affairs in web security, the factors influencing it, and its consequences for the development of the Internet as business tool. As one of the leaders in the field of integrated security for web projects including websites, intranets, and extranets, the company sets out its opinions about the principles of protection and rules of modern web hygiene. These very principles and rules have been and are proving themselves among the 30,000+ Bitrix clients throughout the world.

We hope that this practical guide will promote understanding of today's threats and encourage choices in favor of a truly protected web platform.

APOCALYPSE NOW?

"How can one guarantee uninterrupted business?" a mindful reader may ask, in all fairness. "In the absolute sense, one can't," we answer, also in all sincerity.

It's a shame, but our modern world of euphemisms, approximations and interpolations does not allow much that is absolute, especially a guarantee. It's probably that anyone making claims to the contrary will be in search of new employment in the extremely near future. It should be understood that the word "guarantee" indicates moving ever-closer to an ideal, constantly reducing the frequency and degree of deviation from, in essence, perfection.

When considering security, it is specifically the frequency of system failures which is of interest. To be exact, the issue is how to achieve the greatest *minimization of risk* in connection with uninterrupted business.

The Internet underworld of not long ago was somewhat like the Wild West with a somewhat more socially-introverted Billy the Kid sitting in a basement getting himself into both trouble and the newspapers.

Tempora mutantur et nos mutamur in illis. Our days are no longer those of teenagers with Herostratus-type yearnings.

> "The global economy depends on the internet. If we had some serious trouble with the internet infrastructure, if the internet were to be switched off, you'd forget about the financial crisis and global warming."[6]
>
> Eugene Kaspersky
> Kaspersky Lab CEO

Against us now is an organized criminal network, a fine-tuned machine armed with technology which would make Hollywood special effects look like the cartoons of 50 years ago by comparison. Imagine a Trojan horse program with mutating code and obfuscation technology to hide its presence on an infected computer building an army of 3 million zombie computers to carry out a whole spectrum of illegal actions from sending spam to stealing bank account passwords, launching massive DDoS attacks, and cyber-terrorism.[7] Or this: breaking into a respected bank's database, stealing the data of a 1.5 million clients, cloning a number of bank cards, sending those cards to 280 cities throughout the world, and within 12 hours withdrawing 9 million dollars[8].

This isn't fantasy. This is reality. Moreover, the respected reader may himself be the unknowing the owner of a zombie computer or victim of identity theft.

---

[6] PCR, "Eastern promise", April 2010, http://www.pcr-online.biz/features/369/Eastern-promise

[7] Dmitry Tarakanov, ZeuS on the Hunt, April 2010, http://www.securelist.com/en/analysis/204792107/ZeuS_on_the_Hunt

[8] World Market Media, "9 Million Stolen By Russian Hackers", November 2009, http://www.worldmarketmedia.com/801/section.aspx/498/post/9-million-stolen-by-russian-hackers

FACE THE FUTURE BEFORE BOTH OF YOU ARE HISTORY

Slowly crawling to the cemetery under a white sheet is not an option for civilized, enlightened society. Any event or trend must have a comprehensible cause and, understanding that cause, resistance against it can be planned.

Let's concentrate on enterprise web-resources. First of all, there is security for the company website, intranet and extranet. These are the main attack points for malicious programs. They are also the areas in which Bitrix can share its 12-year experience in the development of protection of web project management systems and give a wealth of valuable and practical advice to a wide audience.

"A powerful security system", "unique protection technology", "maximum access protection of your resources". These mottos can be found everywhere and themselves block a customer's ability to get a full picture of what going on in the system, paralyzing the decision-making process. The customer expresses that web resource security is a priority. The developer answers directly and confidently: "we have everything covered, you don't have anything to worry about, sign here." But what exactly does 'everything' really cover, and more importantly, what should it?

> "It's a myth that hackers are 15-year olds in darkened rooms, and similarly that all cybercriminals are overseas. As with drugs, you have major traffickers but also street dealers. Wherever there is criminality there are criminal hierarchies, and there will also be local pockets of criminality."
>
> Bob Burls
> Detective Constable, Metropolitan Police
> Computer Crime Unit (UK)

It is a rare specialist who, when choosing a website management system or intranet/extranet portal, is able to declare precisely what security requirements are needed. As a result, the label "unique technology" is hung onto whatever access permission management that the product happens to have, for example, SSL-protected communications. The question "what do we do with a harmful program that has entered our environment?" comes later. Actually, that's one of the better questions. Much worse is a false sense of security which leads to a major break-in and the tougher questions which are asked post factum.

Unfortunately, one must admit, that an overwhelming majority of modern web content management systems are in all practicality missing built-in means of protection from external attack. Developers simply recommend working with a security expert to set up the given environment with ample security; a process that usually involves buying additional software.

IN THE LION'S DEN

To begin, let's try to get an understanding of the motivation and make a profile of the typical attack. It is ancient wisdom that you must know your enemy as well as possible. That is the key to victory.

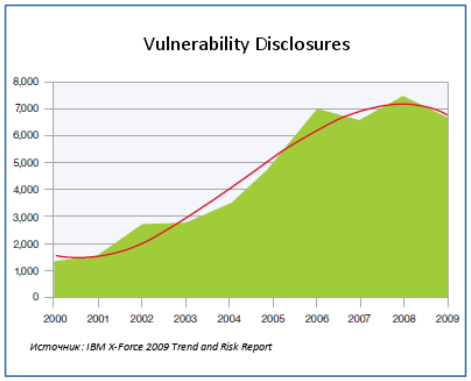
Web attacks are generally based on a relatively simple strategy: create a critical mass of infected web resources and users with as many participants as possible. To carry out this strategy, a tactic called 'cross-pollenation' is used: web resources infect users, and users infect new web resources.

The following principles are generally used to guide the process to its ultimate goal, whatever that may be:

- Scale
  An attack needs to form from as many different places and systems as possible to achieve the desired result.
- Automation
  Attacks are made by robot programs, which are capable of scanning and invading the greatest number of systems.
- Stealth
  Avoid taking any actions which may lead the owner of an infected system to believe that the system is compromised.

We will explore five basic means by which a web resource can become the object or the source of an attack:

- **Use of vulnerable web applications**
  The attacking party launches a bot on the network, which automatically scans for accessible web resources and determines vulnerabilities in them by means of a specially constructed query. The result is that the bits of infecting code are included and 'dissolved' into the code of the web resource, which can in turn infect computers of visiting users. The most well-known types of these attacks are SQL Injection[9] and Cross-Site Scripting[10] (XSS). It is important to note that the deletion of malicious code fragments is by no means a guarantee against future infection.



[9] SQL Injection Wikipedia definition: http://en.wikipedia.org/wiki/Sql_injection

[10] SQL Injection Wikipedia definition: http://en.wikipedia.org/wiki/Sql_injection

An example of an XSS attack

A malicious user sends an email message to the victim containing some specially constructed link that is masked as a link to a trusted site:

http://trusted.website.com/search.php?q=trololo<script>GetAccessData();</script>

Once launched, the link executes a malicious script which discreetly sends the victim's personal data, such as the login and password to the trusted site, to the attacker. This scenario works when the victim is already logged into a site at the moment that the false link is clicked.

- **Administrator password theft**
  This is the most common method for break-in to a web resource. Invasion occurs by means of stealing the administrator password and accessing the control panel of the web resource. To accomplish this, a "Trojan horse" is normally used, which is installed on the personal computer of the administrator. The program scans the victim's disk in search of useful data and captures keyboard input, then secretly passes this information out to the attacker. As a result, the web resource is exposed to an attacker who turns it into a platform for spreading malicious code.

- **Rotating malicious advertisements**
  Internet predators often use the lack of security regarding web advertisements to introduce malicious banners into the advertisement rotation. These, in turn, attack visiting users (as a rule through system vulnerabilities) and embed their 'Trojan' programs. As a result, even a 'clean' web resource can become the implement for an attack and the spread of security threats.

- **External applications**
  Sometimes it happens that the functionality of a management system does not satisfy the specified requirements. In this can the administrator of a web resource may use a plug-in module or widgets from third-party developers. As in the previous case, this is another way in which an attacker can operate through a 'clean' web resource. Concretely, this can be done by creating a malicious plug-in or widget, or by exploiting a weakness in a legitimate plug-in.

> When it comes to plug-ins, however, the sweet song sours, and plug-ins for some applications fare worse than others. Eighty percent or more of the vulnerabilities affecting plug-ins for Apache and Joomla!, for example, had no patch.
>
> IBM X-Force 2009 Trend and Risk Report

- **UGC**
  The Web 2.0 revolution brought users the chance to bring their 15 minutes of allotted fame to fruition through UGC (User-Generated Content). Web resources are now open platforms inviting, even encouraging, users to put up news, maintain journals, and participate in discussions or simply to socialize with other people online. The reaction of the computer underworld was immediate and predictable: attackers actively use the tools of Web 2.0 to spread malicious code, links, files, and media content. They found rich soil for

the technique of phishing[11], based on Cross-Site Request Forgery[12] (CSRF) attacks.

> **Example of a CSRF attack**
>
> The attacker posts a specially constructed link in a forum masked as a tag for placing an image:
>
> *<img src="http://bankaccount.example/withdraw?account=john&amount=10000&to=joe">*
>
> When the forum is opened, the victim's web browser goes to the user's bank account and completes an unauthorized operation, instead of loading the image. For this fraudulent operation to be successful, the browser must save the parameters to authenticate of the bank account.

Important: the above descriptions of methods for compromising web resources is really only the tip of the iceberg in each case. New types of web attacks are invented on a regular basis, along with new combinations of known attack methods. Zero-day vulnerabilities – security flaws in applications which the developer himself does not yet know about and for which patches do not exist.

WORKING ON FUTURE MISTAKES

Web resource management systems are the frontlines – taking the brunt of the attacks of the computer underworld. Websites, intranets and extranet portals are the first objects exposed to attack and the sweetest morsels for spreading malicious code.

Unfortunately, an analysis of the situation shows that this front is not in good shape and that the 'dark forces' are attacking from higher ground.

Authoritative research[13] has revealed that web applications are the largest source of security threats, making up 49 percent of all vulnerabilities. The report states that the top ten list of most vulnerable applications include well-known web content management systems: Drupal (2,7 percent of all vulnerability disclosures in 2009), Joomla! (2,6 percent), TYPO3 (1,5 percent), and Wordpress (0,4 percent) with only 33 percent of the breaches patched. The most disturbing thing is that the share of unpatched third-party plug-ins is 86%.

Indeed, it's difficult to overestimate the importance of making the correct choice concerning security of web resources. What should receive the most attention? What kind of technologies are mandatory to secure protection in the face of an Internet criminal. The answer to these questions can be found in the following table, which contains an overview of the security technologies applied in the top ten most 'popular' forms of web threats.

---

[11] Phishing Wikipedia definition: http://en.wikipedia.org/wiki/Phishing

[12] CSRF Wikipedia definition: http://en.wikipedia.org/wiki/Cross-site_request_forgery

[13] IBM X-Force 2009 Trend and Risk Report: http://www-935.ibm.com/services/us/iss/xforce/trendreports/

Problem	Solution
Attack through application vulnerability	Regular update of user and system software. Implementation of a firewall and IPS.
XSS-attack	Filtering of special HTML symbols. Insert double quotes around tag parameters with dynamic values. Methodically add protocol (http) where it is needed for parameter tag values, for both HREF and SRC.
CSRF-attack	All queries of critical importance actions are signed with a parameter connected to the cookies of the current user.
SQL injection	Make clear designation of data types for numeric data. For text data, process the data using filtering of SQL symbols. Carefully control the length of the data string.
Password theft	Use a password no less than 12 characters including letters, numbers and special symbols. Change the administrative password no less than once per month. Save the password in a reliable place, not locatable by potential attackers (for example, in an encrypted container). Use one-time passwords[14].
Phishing	Apply protection technology against re-addressing queries, carry out awareness programs among users.
DDoS-attacks	User activity control, banned lists, limits on the number of connections from a single IP address. Proper configuration of web servers and firewalls, creation of back-up and bandwidth capacity, as well as securing adequate hardware capacity. Unfortunately, guaranteed protection against this type of attack is not possible. Protection measures serve only to complicate the work of attackers, eliminating 'amateur' attempts.
Spambots	Use Turing[15] (CAPTCHA) tests to identify bots and prevent contamination or use of public elements of web resources by spammers and malicious code.
Recognizing Infection	Timely identification of site intrusions can be achieved using a code integrity checker and web antivirus, which warns of suspicious activities on a web resource.
Traffic Interception	Encryption of traffic, authentication by IP address, and regular changing of session identity.

[14] OTP Wikipedia definition: http://en.wikipedia.org/wiki/One_time_password

[15] Turing test Wikipedia definition: http://en.wikipedia.org/wiki/Turing_test

WITHOUT FALSE HUMILITY

Bitrix is deservedly considered to be a pioneer in development of security technologies for web resource management. In contrast to the competition, the company concentrates a great amount of attention on the development of integrated protection from network attacks, as well as on implementing the principles of development of secure web applications and intense inspection and certification of third-party modules.

As a result, the client receives a website, intranet or extranet portal which is ready for use without the need to acquire and install additional software or hardware. Is the phrase "integrated protection" scary? It shouldn't be: the system is controlled using different pre-set security levels. All you need to do is choose the level of security and the system will automatically adjust the various parameters involved.

The PRO+PRO™ security framework is an integral part of the platform and is included in the two flagship products: Bitrix® Site Manager and Bitrix® Intranet Portal. It contains the following technologies:

- Web application firewall
  The firewall filters incoming website requests from malicious code, hacker attacks and suspicious activity like buffer overflow. Protects against XSS, CSRF, SQL injection and File Include attacks.
- Web antivirus
  In case the website has been compromised or a hacker has succeeded planting malicious code, the web antivirus is invaluable. It scans generated HTML pages before the website transfers them to the visitor and cuts out suspicious code fragments, notifying the website owner about the threat. The web antivirus uses double scanning technology, leveraging a signature database and behavior analyzer.
- One-time passwords
  A hardware token generates a number of digits that the user has to add to the password each time he or she logs in. Thus, the password changes with each session and even if a malicious person acquires it, there is no possibility to use it in the future.
- File integrity
  This feature allows discovery of changes that have been made to the system files. The administrator can verify the integrity of the system kernel, system files or public files at any time. This way it is easy to locate unauthorized changes and undertake necessary measures to prevent website intrusion.
- Backup
  Backup protects the website from a range of risks from server hardware failure to malware infection. When a website gets infected, it is nearly impossible to

clean out all the malicious code fragments. They are usually spread over all the site content and manual eradication would require too much time. With proper backing up in place, you can simply restore the original non-infected version.

- Anti-phishing
  Phishing is the fraudulent attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy website. Phishing protection allows prevention of redirection to potentially dangerous websites and safeguarding of your visitors.
- Access Management
  Leverage the powerful user permission management system that allows crafting of access permissions to certain sections, pages and even page objects in the most flexible manner.
- Automatic updates
  Click-away security updates with real-time notifications about new patch availability.

There are a number of additional security features that can increase the overall protection level. For example, Activity Control can protect the system from profusely active users, obtrusive bots, DDoS attacks and prevent brute force attempts on passwords. IP-based authentication for administrative accounts acts as a second level of password verification in addition to the primary login/password protection. Regular session ID change and SSL-encryption make ID hijacking pointless. The CAPTCHA feature stops spambot activity.

The Bitrix security system has other facets, which are no less attractive. These features lower total project cost and shorten installation time: not only is it unnecessary to purchase additional software, which would usually be required, but the valuable time of an IT specialist is also lessened.

The table below shows a calculation of average expenses on acquiring a full complement of software for a typical organization of 100 users. It is important to note that these costs do not include any costs associated with integration, installation, or maintenance.

Application	Cost (US$)
Web Application Firewall	500
Back-up	200
Integrity Control	500
Anti-virus	800
One-Time Password	500
TOTAL	2500

The PRO+PRO™ framework holds a third-party independent certificate from respected web-security firm Positive Technologies, confirming that it fully meets the Web Application Firewall Evaluation Criteria as established by the Web Application Security Consortium.

The excellence of PRO+PRO™ security was confirmed during the real-time "Chaos Constructions CC9 Festival", when Bitrix products successfully repulsed 25,000+ hacker attacks.

Bitrix also adheres to a strict policy of certification and performance of regular security audits on the third-party plug-ins that can be purchased either from the Bitrix marketplace or from Bitrix authorized partners.

ALWAYS HAVE A PLAN 'B'

Without regard to the episodic claims about the creation of universal protection based on nothing less than artificial intelligence, we must admit that for the time being, the security industry lags behind the – what shall we call it? – the threat industry. The heuristic analyzer, behavior blocker, and other proactive methods of protection significantly reduce risk. Even so, observing proper web hygiene is still one of the most important factors in reaching maximum security.

Based on its many years of experience in development of security systems for web resource management, Bitrix offers the following ten guidelines for your consideration. Our experience shows that in combination with software protection, these guidelines allow virtual exclusion of the possibility of a successful attack on a website or intranet/extranet system.

This is not an absolute, but it is another significant step in the quest for total security.

- Timely security updates. Check both the website managements system's updates and third-party plug-ins you may use. It is best to subscribe to prominent security-related newsletters that will keep you up with the latest security challenges. For example, secunia.com.
- Remember: being a bit paranoid in the web is good! If you suspect abnormal activity, it is better to perform deep scanning of your system and consult with security professional.
- Keep as many logs in your system as possible. Logs will help you or a security specialist identify infection and clean the system.
- Do the backup. Do the backup. Do the backup. Alas, people tend to say "I'll do it two times tomorrow" when talking about backup – you cannot imagine how they regret it when an infection happens. Do it as soon as possible and as often as possible. This is something you will never regret.

- Use the integrity control tools integrated in your CMS or acquire some created by a third-party.
- Use IDS/IPS systems. Even if your CMS is equipped with a best-of-breed security framework, you cannot be too careful in the modern web!
- Switch on the web application firewall integrated in your CMS and other security features like one time passwords, IP-based authentication, abnormal activity blocker, etc.
- Use reliable web applications that are proven to be as secure as possible.
- Consult a security professional for website maintenance, regular inspections and consulting about third-party plug-ins and proper software deployment.
- Follow best practices and web hygiene rules: keep your login/password in a safe place, use one-time passwords, and properly configure your system (e.g. switch off the global variables feature in PHP).

CONCLUSION

The importance of web security to ensure uninterrupted business continuity is probably a tired theme by now. But clearly, the damage of downtime resonates well beyond the actual event, leaving a bad taste in the mouth of clients and site visitors, paralyzing internal and external communications, and leaving a lasting stain on the corporate image. We therefore want to focus attention maximal attention on this single, but extremely important variable which has the power to torpedo all your business development efforts.

In addition to business-as-usual, reliable protection from web attacks ensures compliance with the countless laws and international norms which regulate the security of sensitive data. Examples include HIPAA (Health Insurance Profitability and Accountability Act)[16] in the area of healthcare, GLBA (the Gramm-Leach-Bliley Act)[17] in finance, SarbOx (the Sarbanes-Oxley Act)[18] concerning protection of investors, and a host of others. Failure to comply with these laws can cause significant financial and legal risk from regulator bodies.

Targeted attacks directed on particular web resources and their applications are often extremely complex and obscure analysis and complicate neutralization. Furthermore, constantly developing methods of 'social engineering' and manipulation of users create the necessity for developing systems that are more and more fool-proof.

The *security level* of a system has ceased to be a static condition. It has become a composite of many dynamic processes which all demand constant attention and maintenance. Protection is not a single point effort – it covers the whole spectrum of potential threats to increasingly complicated and accessible IT systems. Failing to understand this concept will inevitably lead to a hot air balloon-like effect: a single hole causes the wreck of the whole vessel.

In summary, an absolute truth: prevention is less trouble than treatment. Security measures are obligatory from the very creation of a web resource. Emergencies that arise from initial security shortcomings are by definition unsystematic and the resulting 'fire-fighting' can become a regular routine, worsening each time, until there is no choice but to start completely from scratch.

---

[16] U.S. Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[17] Federal Financial Institutions Examination Council: http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf

[18] U.S. Securities and Exchange Commission: http://www.sec.gov/about/laws.shtml#sox2002

ABOUT THE AUTHOR

Marcel Nizam is Head of Web Security Development at Bitrix, Inc., supervising implementation of best security-oriented programming practices, certifying and auditing third-party plug-ins, and leading the development of the PRO+PRO™ framework for Bitrix Intranet Portal and Bitrix Site Manager.

Marcel is an authoritative security professional with 10+ years' experience and a number of published security-related articles and reports, as well as being the author of the highly-acclaimed bestseller "Hacker Web Exploitation Uncovered".

ABOUT BITRIX

Bitrix is a privately-owned company developing an advanced business communications platform to bridge SMBs with their customers (Internet), partners (Extranet) and employees (Intranet). Founded in 1998 and headquartered in Alexandria, VA, Bitrix now incorporates 70+ staff, 30,000+ customers and 4,000+ partners worldwide. The customer list includes Hyundai, Volkswagen, Panasonic, Gazprom, Xerox, PricewaterhouseCoopers, DPD, VTB, Samsung and Cosmopolitan. Localized into 13 languages, the company's products are distinguished for their pioneering technology, unique security features, extreme performance capacity and unmatched ease-of-use.

CONTACTS

BITRIX US HEADQUARTERS
901 N. Pitt str
Suite 325
Alexandria VA 22314
USA

Tel./Fax: +1 703 740 8301

BITRIX RESEARCH & DEVELOPMENT
261 Moskovskiy Prospekt
Kaliningrad
236001
Russian Federation

Tel./Fax: +7 4012 51 05 64

SKYPE: consult.bitrixsoft
TWITTER: http://twitter.com/bitrixsoft
E-mail: info@bitrixsoft.com

www.bitrixsoft.com