

## VULNERABILITY STATISTICS FOR CORPORATE INFORMATION SYSTEMS



## CONTENTS

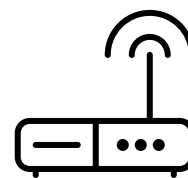
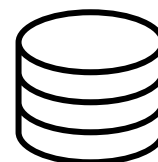
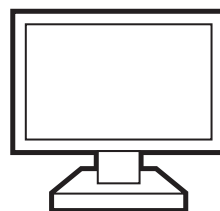
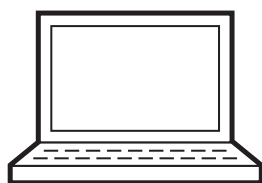
<b>Contents</b>	2
<b>1. Introduction</b>	3
<b>2. Summary</b>	4
<b>3. Source Data</b>	5
<b>4. Statistics as of 2013.</b>	
Comparative Analysis of Results of 2013 and 2011-2012	6
<i>4.1. Overall Penetration Testing Results</i>	6
<i>4.2. Security Analysis of Network Perimeter</i>	10
<i>4.3. Security Analysis of Intranet Resources</i>	12
<b>5. Attack Vectors Used</b>	17
<b>6. Protection Mechanism Assessment</b>	18
<b>7. Assessment of User Awareness in Information Security</b>	19
<b>8. Conclusion</b>	20

## 1. INTRODUCTION

Penetration testing is an information security auditing method that simulates potential attacks, both from the Internet and from an organization's intranet. This enables an assessment of the system's real security level and the discovery of flaws in current security mechanisms including flaws missed if other auditing techniques are used.

This report includes statistics on penetration testing carried out by Positive Technologies in 2013 and compares them to a earlier study completed in 2012. This report shows how modern corporate systems are evolving with regard to information security, how the main vectors used to penetrate organizations' intranets are detected, and how the most typical vulnerabilities are exploited to access critical resources.

The report is based on 14 systems tested in multiple countries. We excluded the results of security analysis carried out on a limited number of hosts at their owner's request, as these results do not reflect the security level of the corporate information system as a whole.



## 2. SUMMARY

### Perimeter security flaws:

- + Any outside intruder acting from the Internet can access internal hosts of 9 out of 10 systems. A malicious user can conduct an attack to obtain full control over a company's whole infrastructure in 55% of cases.
- + On average, an outside intruder needs to exploit two different vulnerabilities to come through the network perimeter. Even low-qualified programmers can conduct such attacks in 82% of cases.
- + Weak password protection causes 40% of internal network penetrations and continues to be the most widespread vulnerability. It was found on the network perimeter in 82% of systems tested. Dictionary passwords were found in web applications and used for privileged accounts in 67% of the companies.
- + Web application vulnerabilities were detected in 93% of the systems studied. The internal network of every third system could be accessed through web application vulnerabilities. Such vulnerabilities as Unrestricted File Upload and SQL Injection are common for 55% of the systems. The average security level of web applications remains as low as it was in 2011-2012.
- + The average security level of a network perimeter is lower than in 2011-2012. The number of systems with easily accessible intranets has increased from 74% to 91%. An intruder now requires lower qualification to conduct attacks because only two vulnerabilities must be exploited to penetrate a security perimeter, compared to three in 2011-2012. It is evident that designing new attack methods takes less time than implementing new security measures, and such security measures cannot ensure a high security level.

### Intranet security flaws:

- + An unprivileged insider present in a network's user segment can escalate their privileges and gain unauthorized access to critical resources in all the systems studied. Such an insider can obtain full control over a company's whole information infrastructure in 71% of cases.
- + Only 17% of the systems require high qualification of an insider to access critical resources, and half the systems studied can be attacked by any unqualified internal user. On average, an attacker needs to exploit five different vulnerabilities to obtain control over critical resources, if access to an internal network is provided.
- + Weak passwords, discovered in 92% of the systems, are still the most common vulnerability of intranet resources. Less frequent vulnerabilities include filtration flaws and service protocol (ARP, STP, CDP, etc.) protection flaws that can trigger hijacking and redirecting traffic and storing of sensitive data unencrypted. Such vulnerabilities were detected in 67% of the systems.
- + The security level of internal networks has decreased compared to 2011-2012. Full control over critical resources can be obtained from an intranet in 100% of the systems studied, compared to 84% in previous years. Similar to attacks conducted from outside, the average number of vulnerabilities required to complete internal attacks dropped from seven to five. More malicious attacks can be conducted by users with low qualification. Despite a number of improvements (e.g., the level of antivirus protection has increased), the protection measures taken against attacks are far from sufficient.

### Lack of information security awareness:

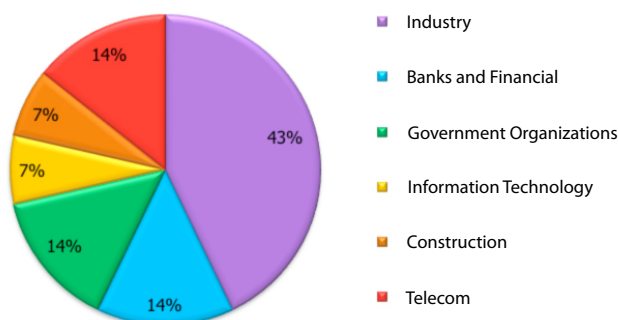
- + The study of users' information security awareness revealed various mistakes in 66% of cases. One third of system users had a low awareness level. More than 20% of employees, who received an email with phishing links, followed the links and started files enclosed or entered their credentials.
- + On average, one user in ten followed a link offered, 3% tried to begin a dialog, and 4% downloaded executables or specified their credentials in an authentication form provided.
- + The level of employees' information security awareness has increased. Every third system was assessed to have an acceptable awareness level in 2013.



### 3. SOURCE DATA

This research considered corporate information systems of 14 large-scale companies in multiple countries. Similar to 2011-2012, the research included organizations of different industries: manufacturing, telecom, government organizations, banking and finance, and construction. A series of geographically-distributed systems with numerous branches and subsidiaries located in different cities and countries were investigated.

Industrial control systems (ICS) were often the aim of penetration tests. Analyzing the security of ICSs is important because their operation is critical and attacks against them have been increasing in number. This is why information security researchers, regulating authorities and system owners are paying more attention to ICS security, and also why Positive Technologies is finding ICSs in penetration tests more often.

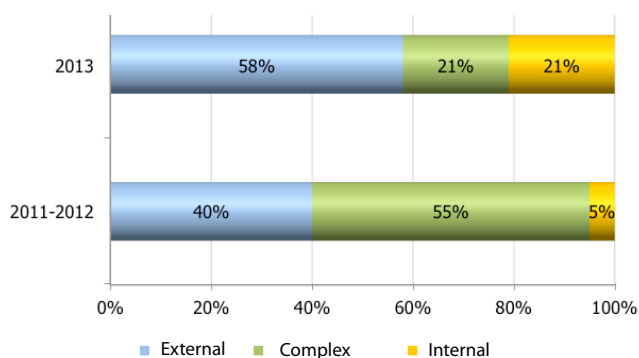


**Figure 1. The ratio of the industries studied**

The services provided within the specified period included several types of penetration tests:

- + External penetration testing
- + Internal penetration testing
- + Complex penetration testing (both external and internal pentesting)

More than half of the companies made use of the external penetration testing service. Complex penetration testing, which included not only network perimeter security analysis and investigation of potential attacks from the Internet, but also internal penetration testing, was carried out for 21% of the systems studied. The internal penetration testing is performed from a defined segment of an intranet (as a rule, connection to a user segment is considered). Internal penetration testing was carried out individually for 21% of the systems studied.



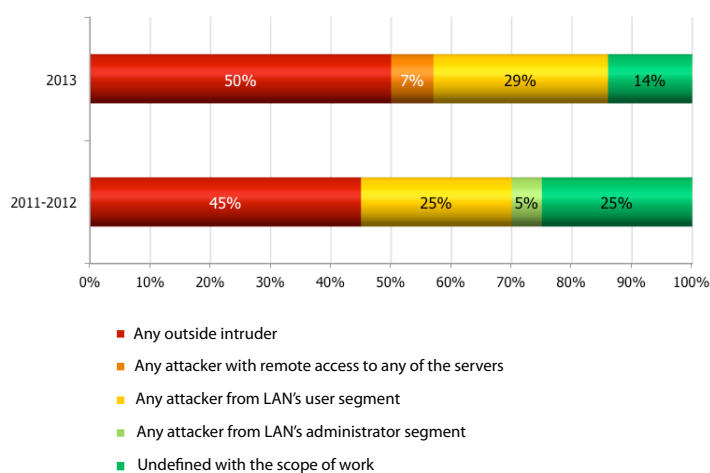
**Figure 2. Systems compared by type of penetration testing service**

As part of our security analysis, staff awareness in information security was assessed for a number of the companies. Positive Technologies performed various checks emulating well-known social engineering attacks (e.g., phishing, pharming) in the course of the study. Statistics on user awareness are provided in section 7.

## 4. STATISTICS AS OF 2013. COMPARATIVE ANALYSIS OF RESULTS OF 2013 AND 2011-2012

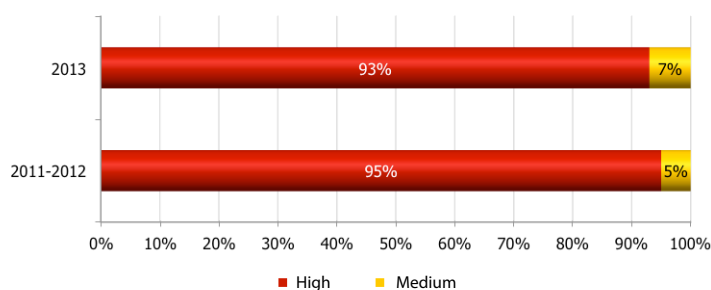
### 4.1. Overall Penetration Testing Results

In 2013, 86% of the systems appeared to be exposed to vulnerabilities that allow obtaining full control over critical resources (Active Directory, ERP systems, email systems, network equipment control systems, etc.). Half of the systems studied allowed any outside intruder to gain full control over critical resources. In 29% of systems, attackers only needed access to the intranet's user segment to get control over such resources. We observed similar statistics in previous years, when full control over important resources was obtained in 45% of the systems on behalf of an outside intruder and in a quarter of the systems on behalf of a LAN user.

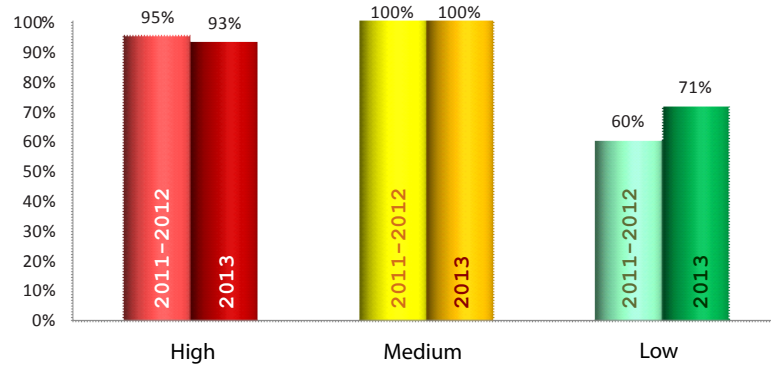


**Figure 3. Minimum privileges required to obtain full control over critical resources**

Practically all systems studied in 2013 appeared to be exposed to high-severity vulnerabilities, as only 7% of such systems had no critical vulnerabilities. Moreover, medium-severity vulnerabilities were detected in all systems. The data obtained in 2013 and 2011-2012 had insignificant differences.

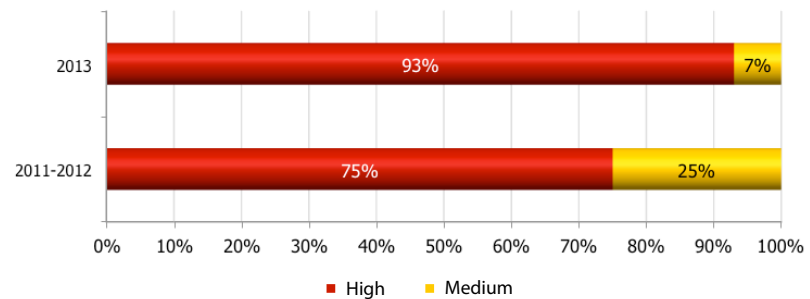


**Figure 4. Systems compared by maximum vulnerability severity**



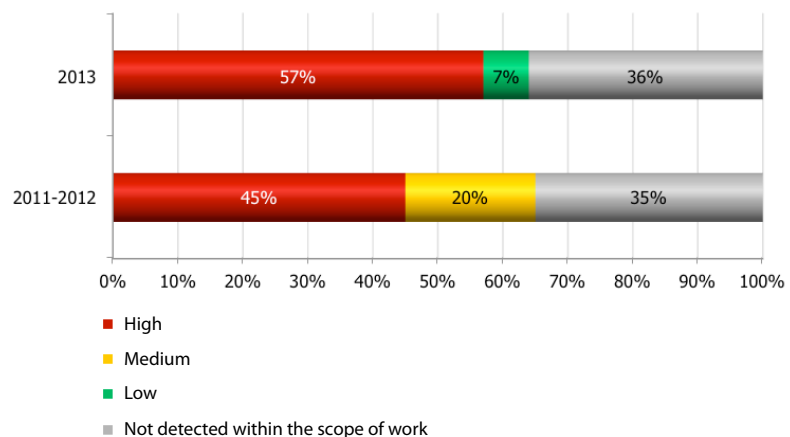
**Figure 5. Systems exposed to vulnerabilities of specified severity**

Only 7% of systems do not include critical vulnerabilities related to configuration flaws. This figure is much worse than in 2011-2012, when 25% of systems assessed contained no critical configuration flaws.



**Figure 6. Vulnerable systems by the maximum severity of configuration flaws detected**

More than half of the systems analyzed in 2013 had critical vulnerabilities since they used out-of-date applications and OS versions. This result is worse as compared to previous years (45%). The average age of the most out-of-date applications is 32 months. One system was found to contain a nine-year-old vulnerability (as of 2004), which made a DoS attacks against the Windows OS possible (CVE-2004-0790).



**Figure 7. Systems compared by the maximum severity of vulnerabilities caused by the lack of security updates**

**"...only 9% of systems assessed blocked our attempts to get through an external network perimeter."**

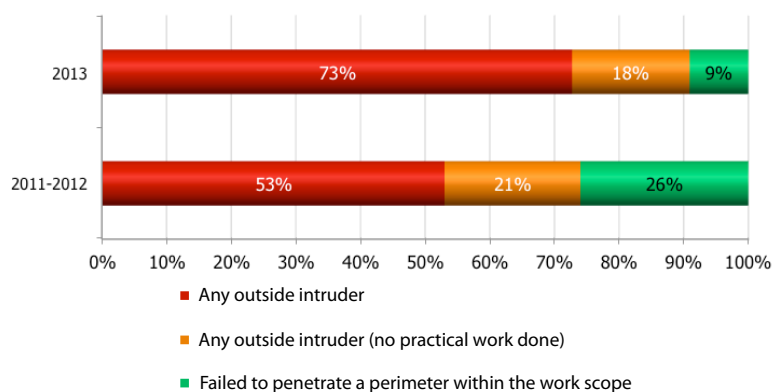
One third of systems studied in 2013 had no vulnerabilities caused by a lack of necessary updates. This is consistent with data of the previous years. While this type of vulnerability may not be detected during testing, the systems analyzed may still contain them. This is because of specific features of penetration testing, which is targeted not at the complete audit of all network resources but at the search of attack vectors that can ensure access to critical resources.

Using out-of-date software versions allows an attacker to implement well-known exploits available on the Internet. To avoid such a threat, system and application software must be kept up to date.

## 4.2. Security Analysis of Network Perimeter

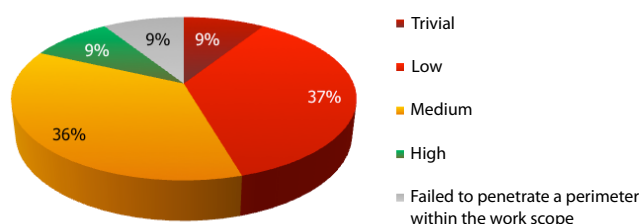
According to data obtained in the course of analysis in 2013, only 9% of systems assessed blocked our attempts to get through an external network perimeter. The LAN resources of the other 91% of systems were exposed to attacks from external networks, and the experts even demonstrated how to access intranets in 73% of the companies. These results are much worse than those of the previous years. The analysis of 2011-2012 showed that a network perimeter could be penetrated in 74% of the systems.

In the 2013 study LAN accessibility was detected in 18% of cases, but the experts did not conduct relevant attacks since they were beyond the scope of work.



**Figure 8. Minimum privileges required to get through a network perimeter**

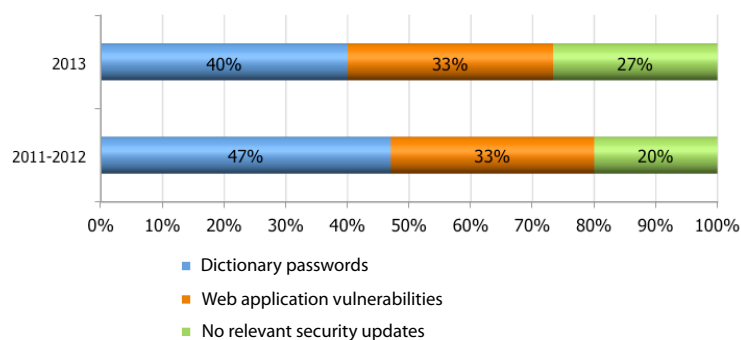
An attacker hardly needs advanced skills to get through a perimeter in the majority of cases (82%), and 9% of the systems required extremely simple actions to penetrate.



**Figure 9. Perimeter penetration difficulty**



On average, two different vulnerabilities must be exploited to penetrate a perimeter. The results of the previous years' analysis showed that at least three vulnerabilities were required. An attack was initiated with dictionary password brute-force in various systems in 40% of cases. One third of intranet penetration vectors are based on the exploitation of web application vulnerabilities; another 27% of such vectors are based on vulnerabilities resulting from the absence of necessary security updates. The results of the 2013 study are similar to the previous years, as the percentage of dictionary password flaws dropped insignificantly (by 7%) allowing for outdated software.



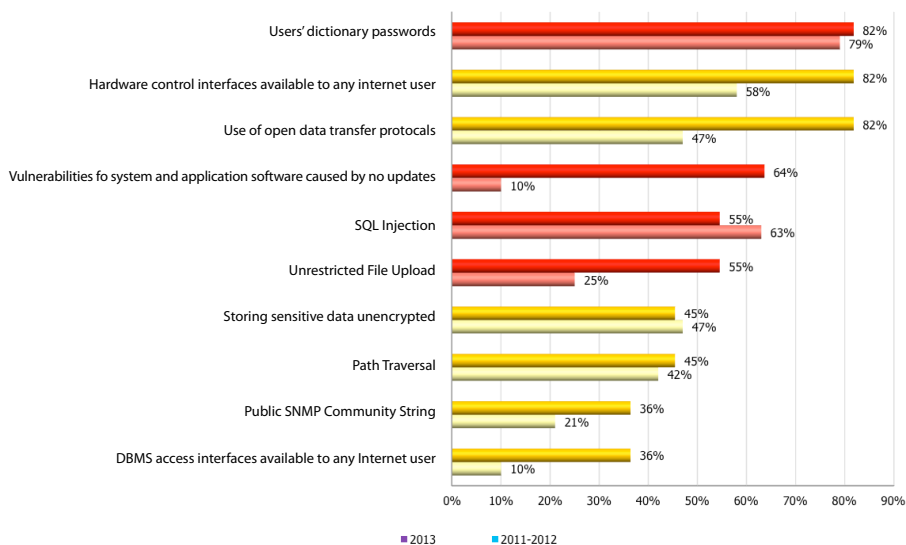
**Figure 10. Attack vectors to penetrate a network perimeter**

Vulnerabilities most typical of a network perimeter are:

- + Use of dictionary (including default and empty) passwords
- + Interfaces for remote access and control over network equipment and servers, which must be available to a restricted number of administrators, located on a network perimeter
- + Use of open data transfer protocols (Telnet, FTP, HTTP, etc.)

Each of these flaws was detected in 82% of the systems studied.

Compared to the previous two years, the 2013 study resulted in a large number of high- and medium-severity vulnerabilities. Low-severity vulnerabilities were less frequent.



**Figure 11. Top 10 vulnerabilities typical of a network perimeter**

**As a result, 82% of the systems examined using external pentests were discovered to contain dictionary credentials used to access web applications.**

### 4.2.1. Dictionary Passwords

Penetration testing applies different methods to obtain user passwords:

- + bruteforce of default users' (Administrator, admin, root) passwords
- + password bruteforce for accounts whose names were gained due to previous exploitation of various vulnerabilities
- + hash bruteforce
- + use of encrypted values to retrieve credentials
- + other methods

This report includes analysis of all passwords obtained in the course of penetration testing. Only passwords that attackers could bruteforce within a short time using common password dictionaries with only the user ID known were recognized as dictionary passwords.

Again, the use of dictionary passwords tops the rating. Despite security policies with specific requirements for password complexity and length adopted by organizations everywhere, practical experience reveals that dictionary passwords remain common. Usually, the reason for this vulnerability is a password policy that is not strict, for example, restricting a minimum length to six characters and ignoring requirements to password complexity and age. This flaw often results when there is no technical control for compliance with the requirements.

Web application compliance with a password policy is rarely verified. Administrators often do not know how to set password requirements in an application system since they may need to ask a developer. System owners often do not pay attention or believe that once users are acquainted with a password policy, it is enough to ensure security.

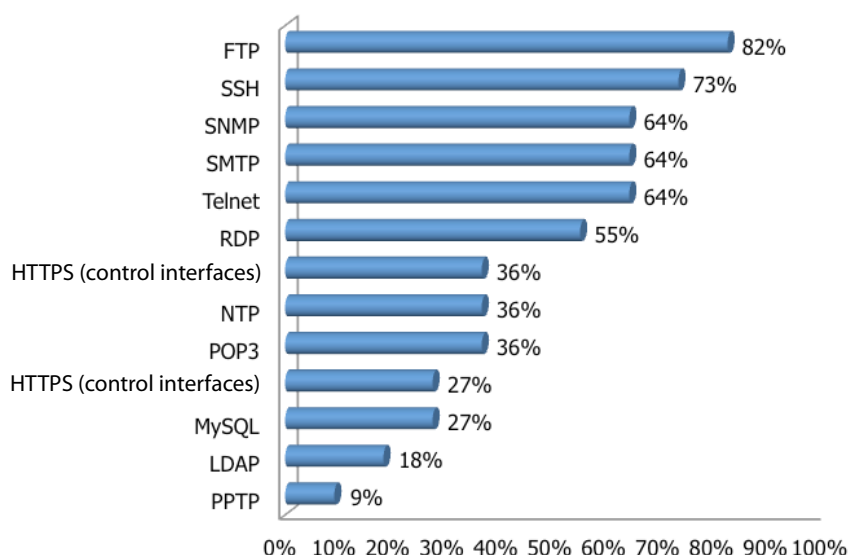
As a result, 82% of the systems examined using external pentests were discovered to contain dictionary credentials used to access web applications. Privileged users were found to use dictionary identifiers and passwords in 55% of such systems.

### 4.2.2. Available Control Interfaces and Open Data Transfer Protocols

Penetration testing applies different methods to obtain user passwords:

- + bruteforce of default users' (Administrator, admin, root) passwords
- + password bruteforce for accounts whose names were gained due to previous exploitation of various vulnerabilities
- + hash bruteforce
- + use of encrypted values to retrieve credentials
- + other methods

This report includes analysis of all passwords obtained in the course of penetration testing. Only passwords that attackers could bruteforce within a short time using common password dictionaries with only the user ID known were recognized as dictionary passwords.



**Figure 12. Statistics on the use of various protocols, including remote access interfaces, on a network perimeter**

The percentage of systems with available management and remote access interfaces (SSH, Telnet, RDP, SNMP, etc.) and open data transfer protocols (FTP, Telnet, HTTP) increased in 2013 compared to the previous years. In 2011-2012, the most typical protocols FTP, SSH and Telnet were detected in half of the systems studied, but in 2013 all network perimeter systems contained at least one of these protocols. Network equipment and server control interfaces accessible via HTTPS were present in 36% of the network-perimeter systems, and these control interfaces were available via HTTP in 27% of the systems.

Isolation flaws of access to network equipment control interfaces are made worse by the common use of dictionary credentials. In 2013, large companies still used network equipment control interfaces with default credentials. Moreover, administrators often keep default settings for network hardware with default SNMP Community String with read and write permissions. Default SNMP Community String with read permissions (public) was detected on a network perimeter in 36% of the systems examined, and with write permissions in 27% of the systems.

Hardware control should not be available from external networks. It is better to use secure protocols (SSH, HTTPS, etc.) to transfer data and to control equipment in particular. Configure access control lists to restrict remote control to only those network addresses that are used by administrators.

#### 4.2.3. No Relevant Security Updates

The percentage of vulnerabilities caused by the absence of relevant security updates increased significantly, from 10% in 2011-2012 to 64% in 2013. Access to the LAN of a large company resulted from the exploitation of the PHP vulnerability CVE-2012-1823 that allows executing arbitrary OS commands on a server. This is a good example of how urgent the problem is. Developed in an intranet, this attack vector allowed Positive Technologies to obtain control over the company's network infrastructure. Therefore, even if application code has no vulnerabilities, malicious users can exploit

outdated software vulnerabilities to attack a server on which the application is based. Another example of obtaining access to critical resources is escalation of privileges to a maximum level on a server with an out-of-date FreeBSD version (CVE-2010-2693), which resulted in an attack on an internal network.

#### 4.2.4. Web Application Vulnerabilities

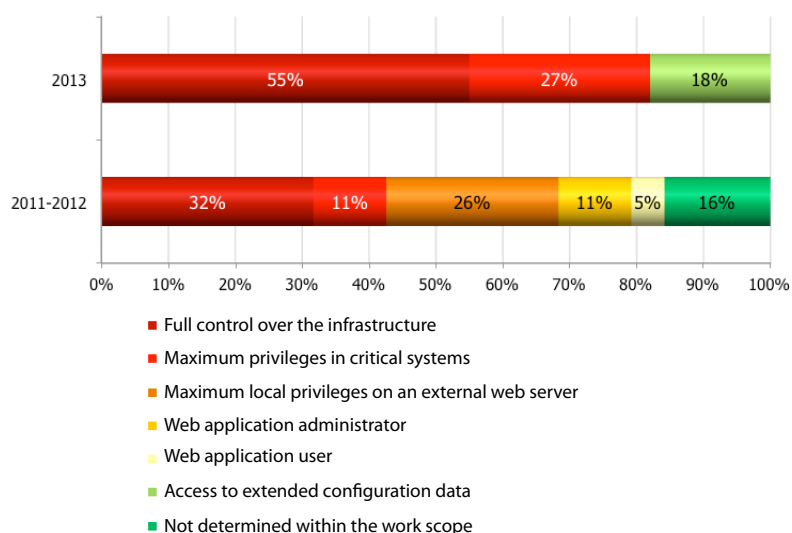
Overall, the level of web application security dropped in 2013, according to the research "Web Application Vulnerability Statistics (2013)" conducted by Positive Technologies.

While the critical vulnerability SQL Injection dropped from second place to fifth, it is still very common. Positive Technologies specialists detected 13 various web applications exposed to this vulnerability at one company. Exploitation of the vulnerability made it possible to demonstrate how to access the LAN in five of the 13 applications.

Another critical vulnerability typical of web applications is Unrestricted File Upload. It has become twice as frequent, with more than half of the systems tested (55%) exposed to it.

#### 4.3. Security Analysis of Intranet Resources

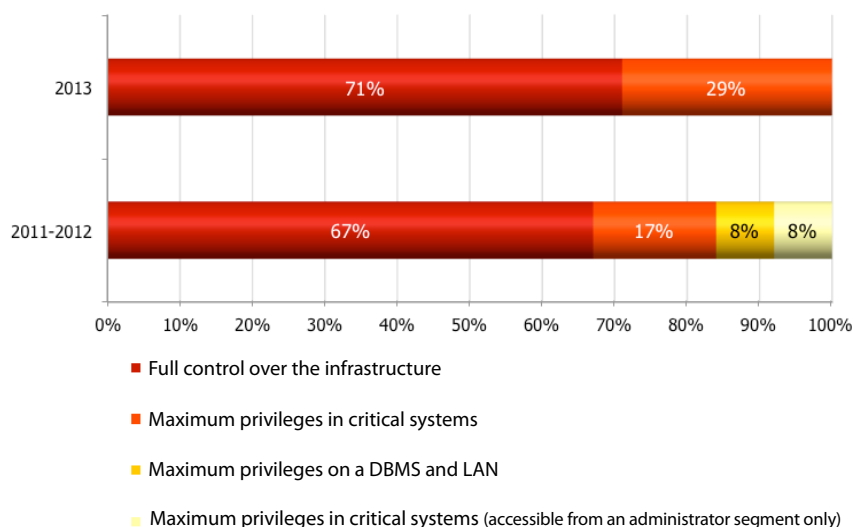
Once a malicious user accesses an intranet, he or she can develop an attack and obtain full control over the whole IT infrastructure in more than half of companies evaluated. The experts were able to obtain full control over critical resources in 82% of the systems tested. These results are much worse than those of 2011-2012.



**Figure 13. The ratio of systems by the level of privileges obtained by an outside intruder**

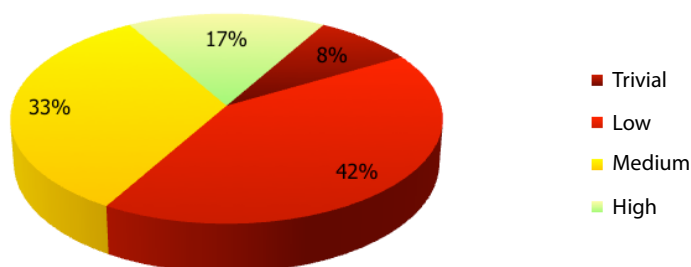
The situation is the same with attacks carried out by insiders (e.g., an employee within a network's user segment). Positive Technologies' specialists obtained maximum privileges in critical LANs within every penetration testing project fulfilled in 2013.

However, a number of systems required attackers to have advanced qualifications and to exploit unknown vulnerabilities (0-day vulnerabilities) to obtain such privileges. Full control over the whole infrastructure was gained in 71% of cases.



**Figure 14. The ratio of the systems by the level of privileges obtained by an insider**

To access critical resources of half the systems, the experts did not apply any special skills, specific hardware or software. Only 17% of the systems required high qualification to access important components.



**Figure 15. Accessibility of critical resources to an insider**

During the study, every system was detected to contain unknown web application vulnerabilities (penetrating a perimeter and attacking within a network). Not only was a customer's proprietary software vulnerable, but also well-known vendor-provided systems were discovered to contain new (0-day) vulnerabilities in 36% of the systems. The system analysis as of 2011-2012 showed the same results.

Once detected, these vulnerabilities were reported to the appropriate vendors by Positive Technologies' specialists.

On average, an attacker needs to exploit five different vulnerabilities to obtain control over critical resources, once access to an internal network is achieved. This is two steps faster than it used to be. The longest attack took nine stages, but the quickest took only three:

1. Accessing Active Directory resources with user permissions as a result of credential bruteforce.

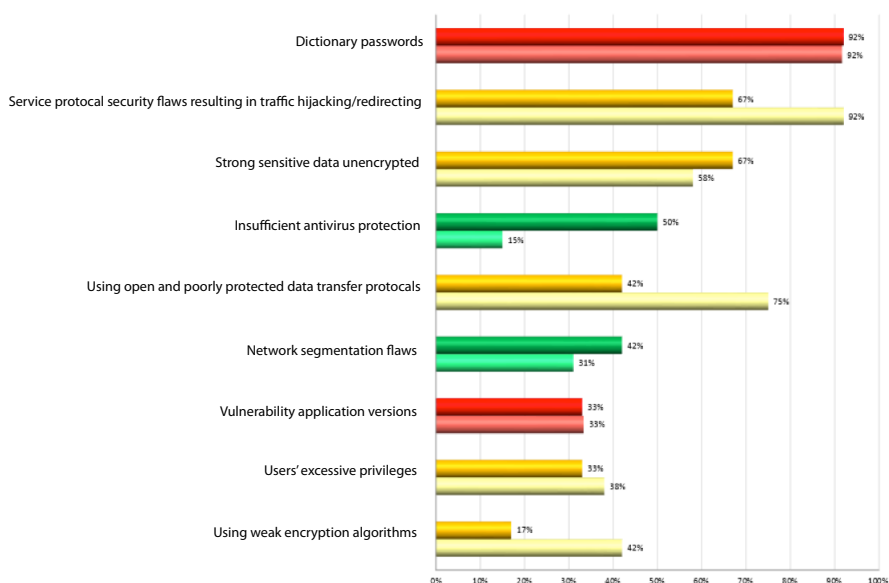
2. Obtaining maximum local privileges on users' workstations as a result of retrieval of local administrator's password from an automated script detected in a domain controller's shared network directory.
3. Uploading specialized software on workstations and obtaining the credentials of a domain administrator with an active session.

Privileged users' security is neglected as in the previous two years. Even administrators' strong passwords can be hijacked in clear-text using software designed to exploit OS vulnerabilities. To provide security, use properly configured antivirus solutions that prevent suspicious software from running and require two-factor authentication for privileged users. Pay attention to the mechanisms that set passwords for privileged users and to various automated processes that require a password.

Windows usually implements Active Directory to solve these tasks using either special scripts created by an administrator, where local administrators' passwords are set in clear-text or group policy tools, where passwords are encrypted with a shared encryption key and can be easily guessed. In either case, all domain users have access to network directories with scripts or group policy settings, so any user can escalate their privileges to the administration level.

According to the analysis as of 2013, the most common vulnerabilities are caused by the use of dictionary credentials (92%), no protection and filtering of channel- and network-level protocols (67%), and storing data unencrypted (67%). The percentage of various vulnerabilities in systems has hardly changed. As compared to data from previous years:

- + Filtering and protocol protection flaws, which result in hijacking and redirecting network traffic — dropped from 92% to 67%
- + Insufficient antivirus protection — increased from 15% to 50%
- + Use of open and poorly-protected data transfer protocols — dropped from 75% to 42%
- + Use of weak encryption algorithms — dropped from 42% to 17%

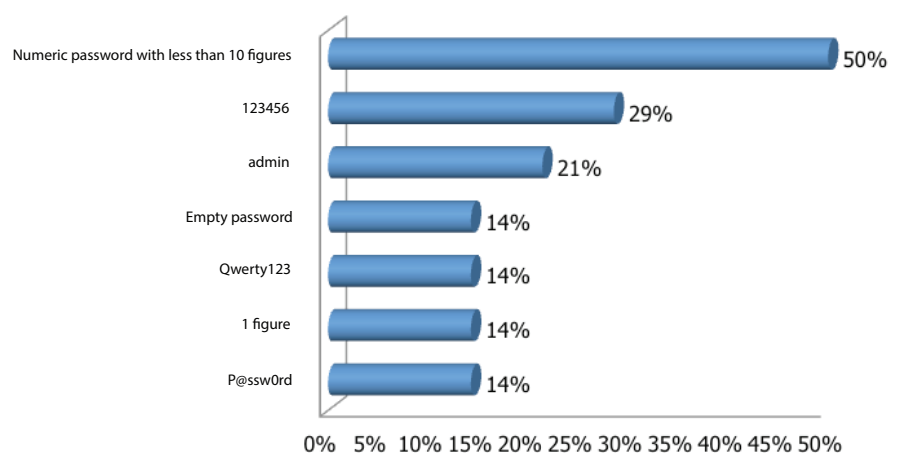


**Figure 16. Vulnerabilities most typical of an intranet**

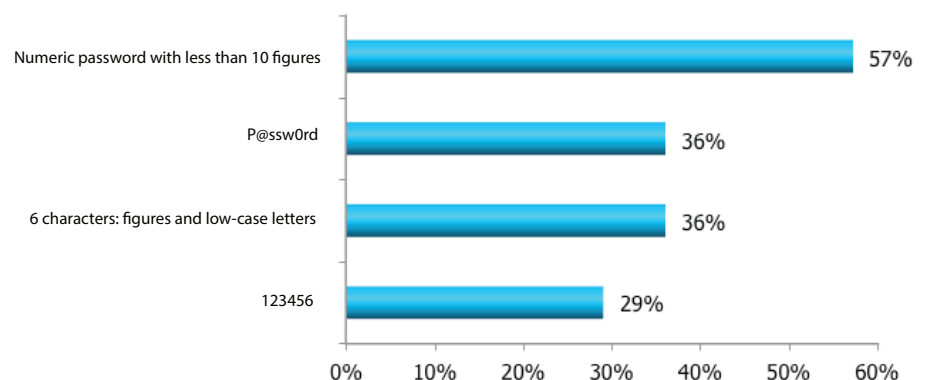
### 4.3.1. Dictionary Passwords

Dictionary passwords were detected in internal networks of 92% of the systems analyzed in 2013. Every system was discovered to use dictionary identifiers and passwords for privileged accounts.

The diagram includes privileged users' most typical dictionary passwords. The administrators in half of the systems with weak passwords used numeric passwords with fewer than ten digits, and the most common numeric password is 123456 (discovered in one third of systems). This dictionary password is very popular among unprivileged users as well (29% of systems). Other numeric passwords with fewer than ten digits are applied by different users in 57% of the systems. Users of 45% of the systems analyzed in 2012 used such passwords. In 36% of the systems, the password cisco is used for network equipment.



**Figure 17. The ratio of systems with dictionary passwords used for administrator accounts (the percentage of systems with weak passwords)**

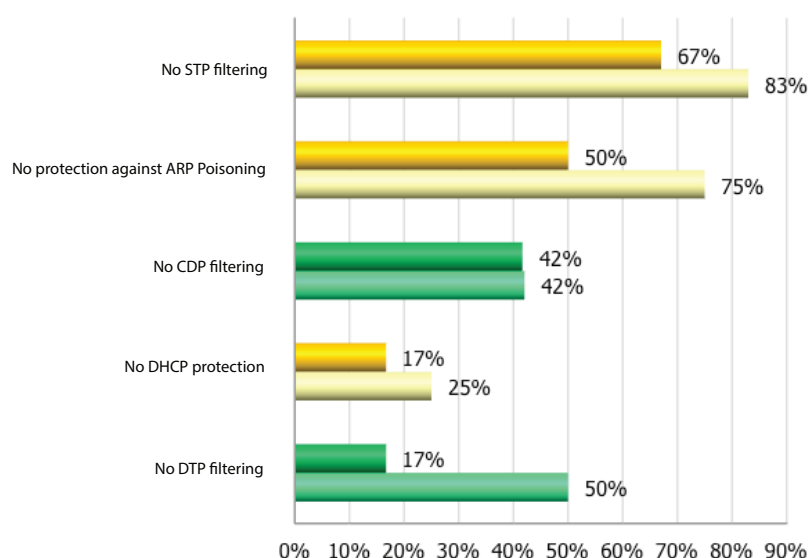


**Figure 18. The ratio of systems with dictionary passwords (the percentage of systems with weak passwords)**

### 4.3.2. Service Protocol Protection Flaws Resulting in Traffic Hijacking and Redirecting

Alongside weak password protection, security weaknesses of various service protocols (STP, CDP, ARP, DHCP, etc.) that trigger traffic hijacking/redirecting and DoS attacks are still quite common. On a large scale, these protocols are at the channel and network levels. No STP protection or filtering was detected in 67% of the systems. The analysis as of 2013 displays a small drop in such weaknesses, but internal networks are still poorly protected from attacks against service protocols.

Alongside weak password protection, security weaknesses of various service protocols (STP, CDP, ARP, DHCP, etc.) that trigger traffic hijacking/redirecting and DoS attacks are still quite common.



**Figure 19. Service protocol protection weaknesses triggering traffic hijacking and redirecting (the percentage of vulnerable systems)**

### 4.3.3. Storage of Unencrypted Sensitive Data

Another vulnerability typical of corporate networks in 2013 was storing sensitive data unencrypted. In the course of security analysis, Positive Technologies' experts detected numerous systems that stored important data in clear-text: automated scripts with administrators' passwords, network equipment configuration files, database backups, users' personal data, and financial information on public resources.

Thus, testing one of the systems, the specialists discovered a text file on a server that included a password to a crypto container where encrypted files with sensitive data were stored. As a result, they managed to access administrators' credentials and other information, and developing this attack vector, they accessed different critical systems. In this case, the cryptographic security tools were rendered useless since the encryption key was stored in clear-text on the same resource.

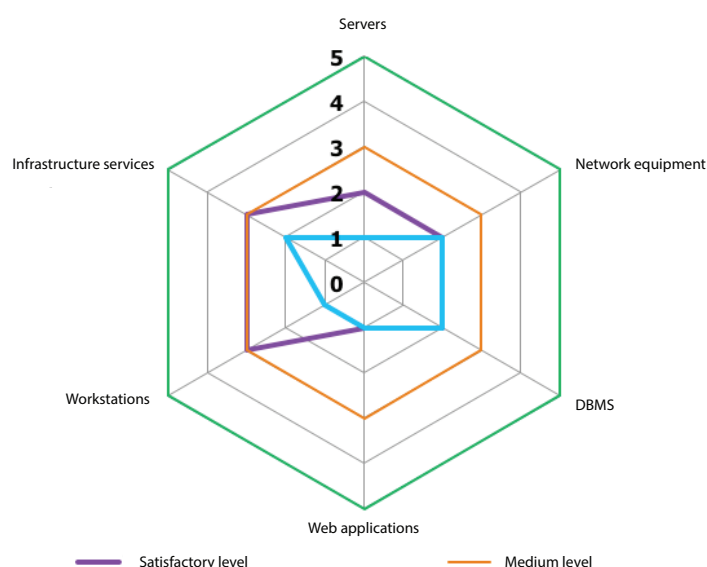
To protect critical data from unauthorized access, encrypt sensitive data, do not store resource passwords or encryption keys unencrypted and if you cannot apply cryptographic techniques, isolate access to the resources where sensitive information is stored.



## 5. ATTACK VECTORS USED

This section includes assessment of medium-security information systems by various attack vectors. Attack vectors were classified according to system components and which vulnerabilities allowed unauthorized access to resources.

A security level was assessed as follows: every system was graded from 0 to 5, where 0 was the lowest security level (vulnerabilities of this category ensured direct access to critical resources or there were numerous critical vulnerabilities) and 5 was a satisfactory security level (no vulnerabilities, correctly deployed protection tools).



**Figure 20. Medium-level security dynamics for various system components as of 2011-2012 and 2013**

In general, companies paid more attention to information security in 2013. Information systems with no protection mechanisms for any component are getting rare. As a rule, large companies use many security tools, but for many reasons, they are insufficient. In 2013, web application protection was the most neglected. As in 2011-2012, the security level was evaluated as extremely low. Web applications are usually custom developments, and programmers concentrate on business functions instead of security. Therefore, internal networks and external perimeters contain numerous web applications with code errors leading to critical vulnerabilities (e.g., SQL Injection and Unrestricted File Upload).

The security level of workstations and infrastructure services (such as directory services and email systems) was assessed as medium. General staff often use such systems, therefore any organization applies at least basic security measures (e.g., regular OS updates and antivirus protection of workstations). Nonetheless, vulnerabilities are still present in these services, and security measures taken cannot provide sufficient protection from attacks.

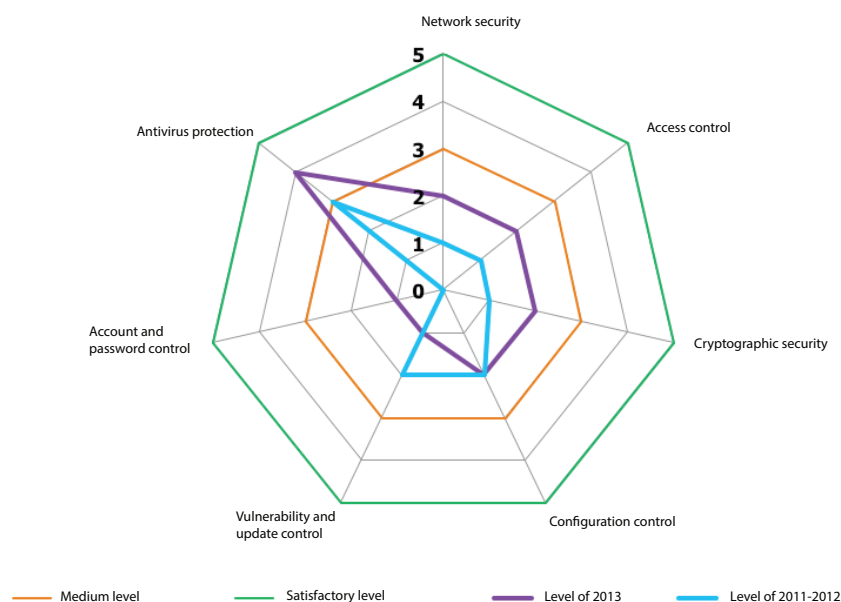
Servers' security level increased a little, but did not exceed lower than medium grade. The security of network equipment and database management systems (DBMS) remained the same and was graded lower than medium.

The following attack vectors were most widespread in 2013: dictionary password brute-force, exploitation of outdated software vulnerabilities and access control flaws (e.g., using a privileged DBMS account on server's operating system).

## 6. PROTECTION MECHANISM ASSESSMENT

Security-level grades for various protection mechanisms used in the majority of the systems indicate certain improvements. The grades for network security, access control and cryptographic protection increased from a low security level to lower than medium. Account and password management was improved as well, but its general security level remained low, which is proved by the fact that the most common vulnerability is still the use of dictionary passwords.

**The situation with outdated software versions worsened in 2013. It resulted in rapid growth of systems with no security updates on network perimeter hosts (from 10% to 64%) and relevant vulnerabilities exploited to penetrate an intranet (27%)**



**Figure 21. Medium-level security dynamics according to protection mechanisms as of 2011-2012 and 2013**

The situation with outdated software versions worsened in 2013. It resulted in rapid growth of systems with no security updates on network perimeter hosts (from 10% to 64%) and relevant vulnerabilities exploited to penetrate an intranet (27%). This situation was probably a result of companies not being ready for quick releases of new software versions. Moreover, new software typically leads to updates and changes to a hardware platform, increasing the costs further.

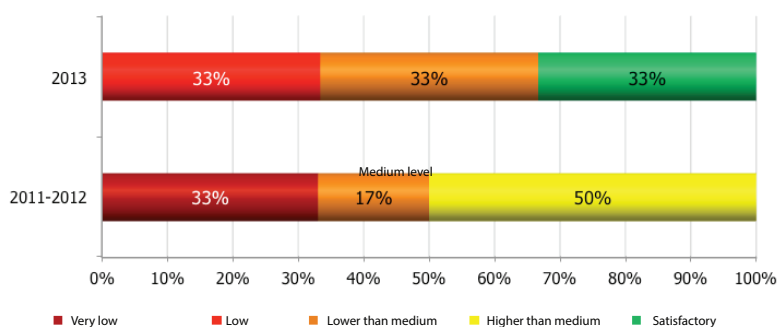
The level of antivirus protection improved in 2013. It is the only category that earned a higher-than-medium grade. Antivirus protection is used everywhere, as opposed to previous years, and antivirus databases are updated constantly in the majority of cases. However, antivirus software usually lacks self-protection features or they appear disabled. Further, privileged users can disable their antivirus program. As a result, we see evidence that a growing number of systems have insufficient antivirus protection.

## 7. ASSESSMENT OF USER AWARENESS IN INFORMATION SECURITY

The scope of penetration testing conducted for a number of companies in 2013 included an assessment of information security (IS) awareness. The analysis consisted of a series of agreed to attacks that emulated the actions of real attackers and tracked their outcomes. The experts applied individual techniques and used email, unified messaging systems, social networks and telephone calls to interact with employees. However, the results only represent those acquired through using email attacks.

The test was performed in the form of email with a file or a link to an external resource attached. Then any evidence of clicking the link, running the executable attached to the letter, entering credentials if a phishing attack was emulated, or attempts to communicate with the sender was tracked. As a rule, emailing was carried out on behalf of an organization's employee.

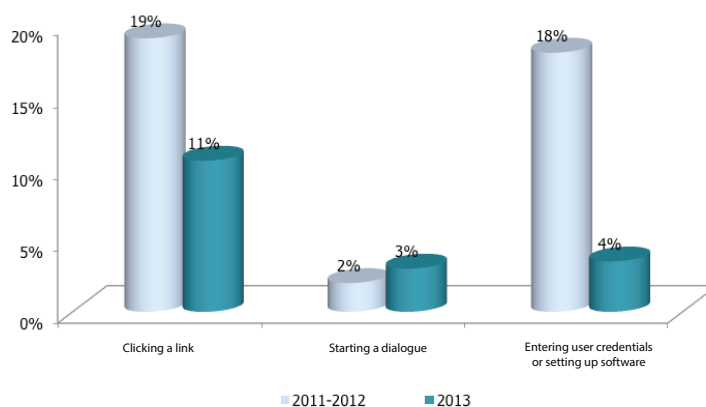
The awareness assessment was based on Positive Technologies' expert opinion according to the results obtained.



**Figure 22. The total results of IS awareness analysis as of 2013 and 2011-2012**

The results obtained indicate an improvement of staff awareness in information security as compared to the results received in 2011-2012. The staff awareness level was assessed as satisfactory in one third of systems tested.

The number of cases when users followed a link attached to an email dropped from 19% to 11% in 2013. With entering credentials and running attached files, the number also dropped, from 18% to 4%.



**Figure 23. The ratio of recorded events to the total number of emails sent**

However, the number of users who started dialog with a potential attacker remained the same (3%). Such users' actions cannot cause workstation infection or loss of credentials directly, but by interacting with an employee, a malicious user can obtain additional information to develop further attacks.

## 8. CONCLUSION

Compared to the results of the 2011-2012 research, the results from 2013 show that modern corporate systems have become more vulnerable to attacks from outside intruders as well as insiders. The most dangerous problems were detected in web applications. Serious flaws were also found in the protection mechanisms of servers, DBMS and network hardware. These are the systems that were most frequently exploited to penetrate a network's external perimeter and to access critical resources.

As in 2011-2012, the most typical vulnerabilities were a result of password policy flaws. Vulnerabilities connected with availability of server and network hardware control interfaces (SSH, Telnet, RDP, web interfaces) from external networks were common. Intranet resources demonstrated frequent password policy flaws and service protocol (DHCP, STP, ARP, CDP, DTP) security bugs. Please note that storage of unencrypted sensitive data is getting more common for companies, which eases the work of attackers.

The trend in IS awareness was promising in 2013 as the percentage of companies in which employees followed links attached to emails or ran untrusted software dropped significantly. The awareness level of one third of systems tested in 2013 was assessed as satisfactory.

The main finding of this research was an insufficient information security level of corporate systems, regardless of industry. The growing tendency toward the security improvement of certain system components (access control, network security and cryptographic protection) does not affect the general security level. Protection measures, as compared to vulnerabilities and attacking techniques, have a slower development pace. Therefore, the percentage of systems with accessible critical resources increased.

Using accessibility of critical resources as a benchmark, Positive Technologies concludes that it is necessary to improve information protection tools and security measures, including password policies, web application security, regular security updates and privileged account protection. In addition, you should analyze security on a regular basis, including conducting pentests, to detect security flaws before they are exploited.

---

### About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report\*. To learn more about Positive Technologies please visit [www.ptsecurity.com](http://www.ptsecurity.com).

\*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of \$20M+.



© 2014 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.