SECURITY TRENDS & VULNERABILITIES REVIEW

CORPORATE INFORMATION SYSTEMS

2016

POSITIVE TECHNOLOGIES

Contents

Introduction ... 3

1. Executive Summary ... 4

2. Research Data ... 5

3. Statistics for 2015 in Comparison to 2014 and 2013 ... 7

3.1. Overall Penetration Testing Results ... 7

3.2. Security Analysis of Network Perimeters ... 10

3.2.1. Vulnerable Software Versions ... 12

3.2.2. Open Protocols ... 12

3.2.3. Equipment Management Interfaces ... 12

3.2.4. Dictionary IDs and Passwords ... 13

3.2.5. Unrestricted File Upload ... 14

3.2.6. Storing Sensitive Data in Clear Text ... 14

3.3. Security Analysis of Intranet Resources ... 14

3.3.1. Dictionary Passwords ... 17

3.3.2. Secure Flaws in Service Protocols ... 17

3.3.3. Insufficient Protection for Privileged Accounts ... 17

3.3.4. Insufficient Antivirus Protection ... 19

3.3.5. Storing Sensitive Data in Clear Text ... 19

3.3.6. Vulnerable Software Versions ... 19

4. Attack Vectors ... 19

5. Assessment of Protection Mechanisms ... 21

6. Results of the Assessment of Staff Information Security Awareness ... 21

7. Security Analysis of Wireless Networks ... 22

Summary ... 23

Introduction

Information protection is one of the most pressing issues in a range of industries including IT and banking. Infrastructure of companies and, mainly, large corporations, undergo changes every day: new hosts and systems appear, and network topology and equipment configurations change. Such dynamic systems need regular security analysis and immediate elimination of vulnerabilities. The complexity of infrastructure and correlation within subsystems makes it difficult for large corporations to ensure security 24/7.

Penetration testing is a very effective method to analyze a security level. It allows vulnerabilities to be detected in a corporate infrastructure and establishes an objective and independent evaluation of the current security state. A potential attacker's actions both from the internet and from the company's intranet are simulated during penetration testing. It helps to create a situation that is very similar to those faced during a real hack and to fix defects promptly.

This report provides statistics that were gathered during penetration testing performed by Positive Technologies in 2015. The paper also contains the comparison of recent data with those obtained in 2014 and 2013. Thus it is possible to track the dynamics of information systems development in the context of delivering information security.

The statistics include results of security analysis of 17 systems owned by state and commercial organizations from various industries.

When selecting a system for analysis, we considered the informational value of pentest results in terms of statistics. We excluded results of the security analysis carried out on a rather limited number of hosts at their owners' request as these results do not reflect the security level of the corporate information systems.

1. Executive Summary

General Results:

- 76% of the systems offer an opportunity for a hacker to gain complete control over certain critical resources; an external attacker can obtain such privileges in 35% of the systems.
- An intruder can take full control over a corporate infrastructure in 50% of the systems under analysis (in 19% of cases, an external attacker can gain control, and in 31% of cases, it can be an intruder attacking from a user network segment).

Security Perimeter Flaws:

- In 55% of cases, an outside attacker, upon reaching a corporate network from the internet, can access intranet hosts without using social engineering methods. If, however, the attacker resorts to such methods, he or she can access a local area network in 82% of cases.
- Maximum privileges in critical systems can be obtained in 55% of cases; in 28% of cases, full control over a company's infrastructure is obtained.
- In 55% of the systems, a potential attacker needs a medium or low level of qualification to bypass network perimeter restrictions without using social engineering methods. It is enough to exploit two different vulnerabilities to gain access to intranet resources (the same result as in 2014).
- Attacks aimed at bypassing network perimeter restrictions are based on exploitation of web application vulnerabilities in 47% of cases. Vulnerabilities of various risk levels were detected in 69% of the analyzed web applications. The Unrestricted File Upload vulnerability was found in 56% of cases; SQL Injection — in 44%.
- The other 53% of attacks, where access to internal resources can be obtained, are facilitated by the use of dictionary passwords. This type of vulnerability was the most common according to the 2014 report. In 2015, 78% of systems can be accessed by privileged users with weak passwords. 44% of companies use dictionary credentials to access public web applications.
- Each system under analysis has flaws caused by using vulnerable software; in most cases, these are outdated versions of web servers (78%).
- 45% of all the systems under test do not contain vulnerabilities that allow access to critical resources from external networks. It has become more difficult to perform an attack as well: a low-skill attacker is able to access internal resources only in 46% of cases (as compared to 61% in 2014).

Intranet Security Flaws:

- In 100% of cases, a potential internal attacker is able to gain maximum privileges in critical systems. 71% of tests resulted in full control over the whole infrastructure.
- If attackers have access to the intranet, they need to exploit four different vulnerabilities to obtain control over critical resources, which is one step slower than in the previous year and one step faster than in 2013. A low-skill attacker is able to access critical resources of 82% of the systems, while in 2014, it was only 56%.
- The most common vulnerability in internal networks is weak passwords (100%). Moreover, most systems (91%) have weak passwords for privileged users' accounts. All systems have protocol defects that lead to redirecting and hijacking network traffic. Insufficient

protection of privileged accounts and antivirus protection flaws are still widespread in the companies' internal network: these vulnerabilities were detected in 91% of systems.

- The security level of the intranet is still low. Despite certain improvements (the average level of cryptographic security increased, information security awareness among employees became more acute), methods used to protect against intruders are not sufficient. Since 2014, there has been little change in a common scenario of attacking intranet. Exploiting widespread and well-known vulnerabilities is still enough for a successful attack.

Lack of Staff Awareness:

- Users' information security awareness was tested by means of social engineering and the study revealed various flaws in all the cases. Only 25% demonstrated above-average knowledge. However, the number of companies with a low level of staff awareness halved in 2015 (25% as compared to 50% in 2014).
- It is important to note that in 2015 about 24% of users followed a fake link (compare to 20% in 2014). The number of users who entered their passwords to a specially crafted authentication form or ran an executable file did not change (about 15%).
- The general level of staff awareness of information security issues has moved up since 2014, but it is still low and it is not considered acceptable in any of the systems.

Wireless Network Security Flaws:

- Certain vulnerabilities were detected while testing wireless networks; however, in 33% of cases, the security level is acceptable.
- The most widespread vulnerabilities are the usage of unauthorized access points, the usage of WPS, the lack of wireless network protection, use of default accounts of network devices, and accessibility of wireless networks outside their control zone.
- The general level of wireless network security in 2015 is rated as average. Detected flaws do not allow a potential attacker to gain access to a company's internal network. Still one of the tests revealed that such flaws, when used with network perimeter vulnerabilities, allow an intruder to gain access to a corporate domain controller in a few steps — even from outside their control zone.

2. Research Data

During the research, we analyzed the results of penetration tests of 17 information systems of large companies. Just as in the previous years, the list contains companies of various industries, including banks, large industrial enterprises, telecommunications companies. A transport company and a state organization were also tested. Most of the companies are from the financial sector (35%). Industrial, telecommunications, and information technology organizations hold equal shares (18% each).

More than half of the enterprises were geographically distributed and had many subsidiaries and branches located in different cities and countries. Most systems that went through external penetration testing had hundreds of active hosts available at their network perimeter.

Some industrial control system networks were pentested. The research's results proved the importance of system security assessment and elimination of vulnerabilities in due time.

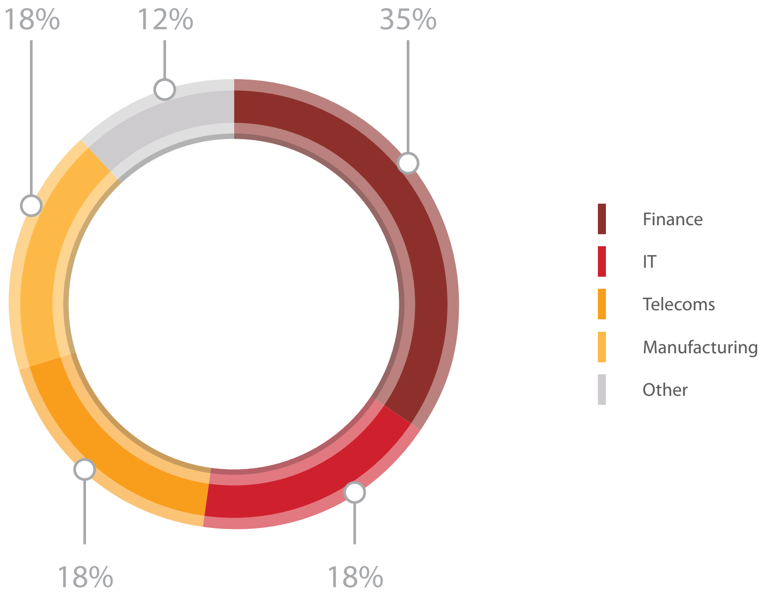

Figure 1. System distribution by industries

During the research, Positive Technologies specialists performed external and internal penetration testing.

In 2015, companies usually requested one type of testing. Only one client purchased complex penetration testing.

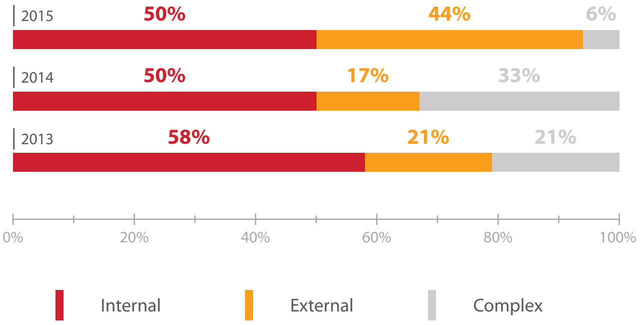

Figure 2. Systems by penetration testing types

24% of the companies asked Positive Technologies to perform security awareness checks, which include a simulation of social engineering attacks (phishing emails). Detailed statistics and analysis can be found in clause 6.

3. Statistics for 2015 in Comparison to 2014 and 2013

3.1. Overall Penetration Testing Results

In 2015, Positive Technologies specialists gained control over certain critical resources of 76% of the systems under test. In 35% of the systems, any external attacker can gain such privileges. In 41% of the systems, these privileges can be obtained by an internal intruder from user or technological segments of a LAN. In 24% of cases, PT specialists did not gain control over critical resources. This shows the tendency towards a rising security level of critical resources, compared to the results obtained in 2013 and 2014.

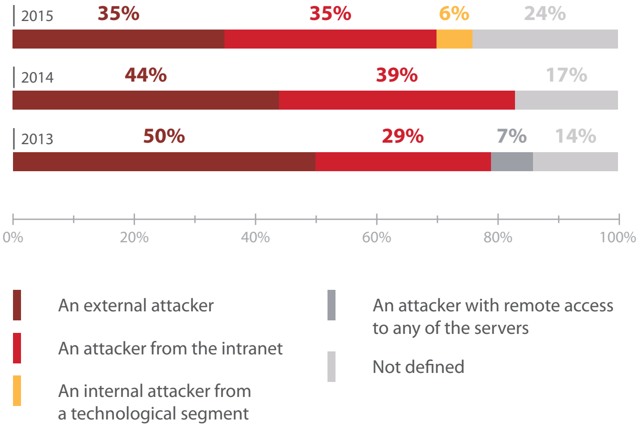

Figure 3. Systems by minimal access privileges an intruder needs to get full control over certain critical resources

Half of the systems' IT infrastructure could be compromised by an attacker (in 19% of such cases, by an external attacker). In 31% of organizations, attackers needed access to an organization's intranet to gain such control.

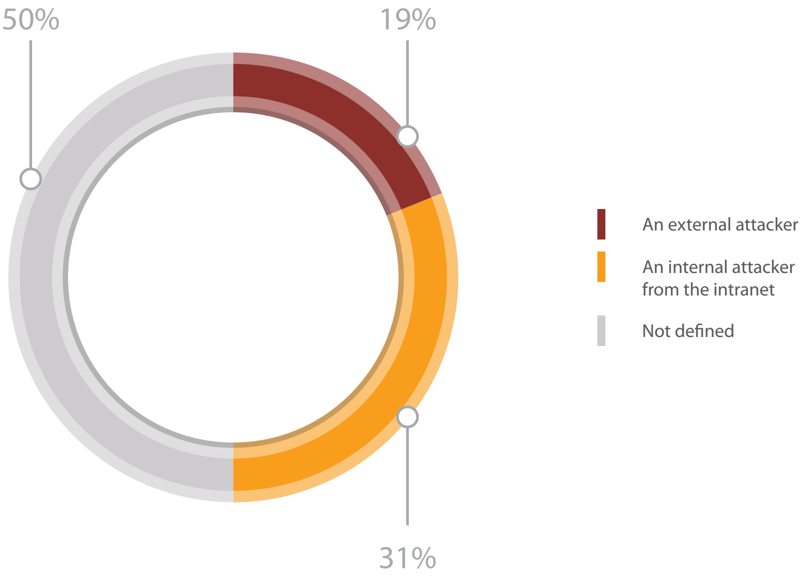

Figure 4. Systems by minimal access privileges an intruder needs to get full control over the whole infrastructure

According to statistics released in 2014, 44% of systems' infrastructure could be controlled by a potential external attacker, while 39% could be attacked by an internal one. It is worth mentioning that in 2015 PT experts did not expand attacks against internal networks in a number of external pentests due to customers' requests. In these projects, an attacker could at most gain administrative privileges for network perimeter servers and then proceed with the attack on internal network resources.

In almost every corporate infrastructure, vulnerabilities of the high-risk level were detected. Only one system did not contain critical vulnerabilities; still it had medium-severity flaws.

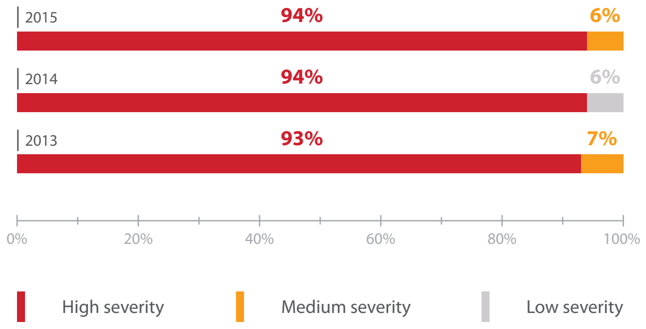

Figure 5. Systems by maximum vulnerability severity

Since 2013, there has been a trending growth in the number of organizations that had infrastructures prone to high-risk vulnerabilities caused by using obsolete software and the lack of security updates. The average age of the most out-of-date applications is 73 months (more than 6 years). The study of 2014 showed the same figures. Information about the oldest vulnerability was published 14 years ago (CVE-2002-0083). The vulnerability in OpenSSH allows local users or remote malicious servers to gain privileges.

13% of the systems did not contain vulnerabilities caused by using obsolete software, according to the research carried out in 2015. The vulnerabilities related to the lack of necessary updates can still be found in these systems, for an external penetration test is conducted with the privileges identical to those of a potential attacker and does not include full audit of all the network resources.

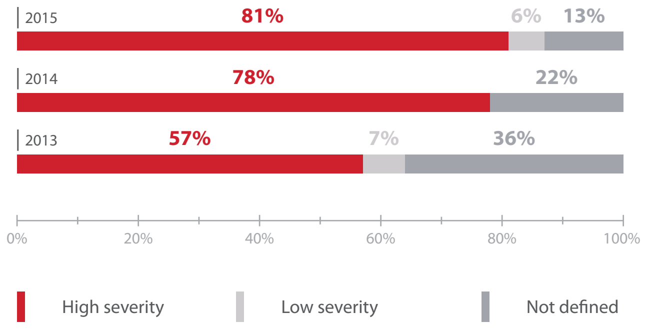

Figure 6. Systems by maximum severity of vulnerabilities caused by the lack of updates (vulnerable systems)

The number of corporate systems that contain severe vulnerabilities caused by configuration flaws has decreased (81%). 19% of all the systems under test contained configuration flaws with a severity level not higher than medium.

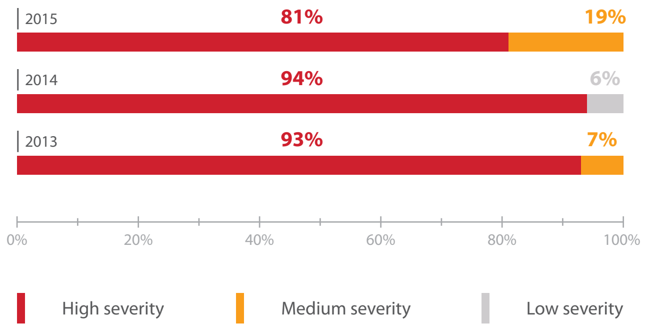

Figure 7. Systems by maximum severity of vulnerabilities caused by misconfigurations

Penetration tests revealed that 68% the systems had vulnerabilities caused by errors in web application code. 57% of the companies had such severe vulnerabilities as SQL Injection, XML External Entity Injection, Unrestricted File Upload. In 2014, web applications' security level was lower: 89% of the systems contained various vulnerabilities in web applications. However, web application vulnerabilities might still be present but not detected since the tests were carried out by using the black-box method.

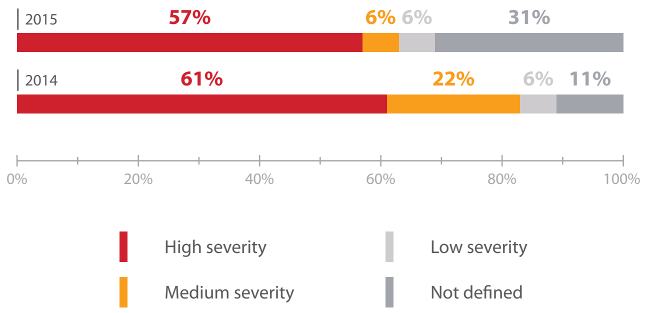

Figure 8. Systems by maximum severity of vulnerabilities caused by web application code flaws

3.2. Security Analysis of Network Perimeters

In 82% of the corporate information systems, the analysis revealed vulnerabilities that allowed bypassing a network perimeter and getting unauthorized access to LAN resources from external networks. In 55% of these cases, it could be achieved by an external intruder without using social engineering methods. The figure is much lower as compared to the results obtained in 2013 and 2014.

According to Positive Technologies specialists, it has become more difficult to bypass a network perimeter than it was in 2014. In 46% of cases, a low-skilled intruder is able to bypass a network perimeter (as compared to 61% in 2014). In 27% of cases, an intruder could bypass a network perimeter only by using social engineering.

To bypass a network perimeter, an attacker still needs to exploit two vulnerabilities on average. For almost each system, PT specialists revealed several attack vectors that led to unauthorized access to LAN resources. 80% of attacks were performed successfully due to at least one attack vector that implied exploitation of only one vulnerability.

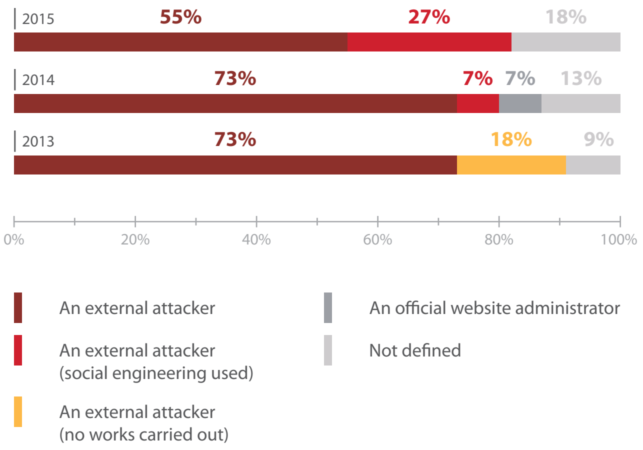

Figure 9. The minimal level of an attacker's qualification required to bypass a perimeter

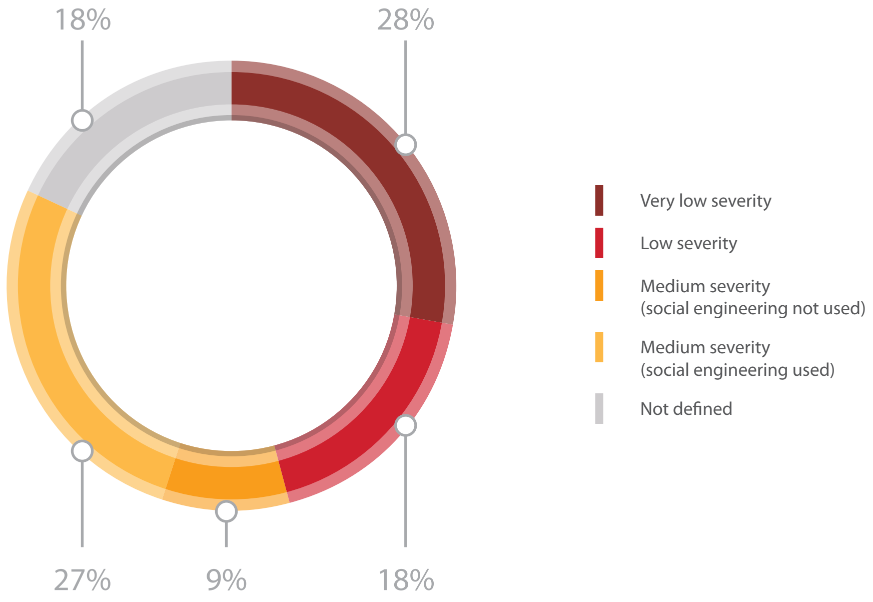

Figure 10. Difficulty of penetrating a perimeter

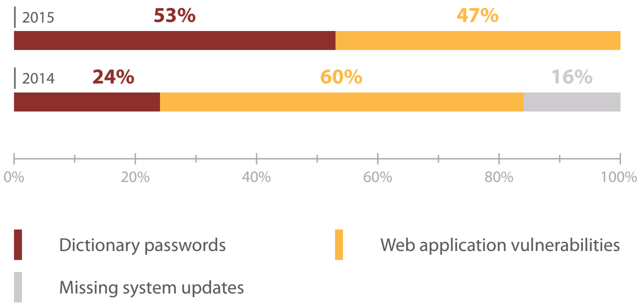

Figure 11. Attack vectors for penetrating a network perimeter

47% of successful attack vectors aimed at a network perimeter were designed to exploit a web application vulnerability, while the other half were based on dictionary passwords. As opposed to 2014, in 2015, researchers did not use out-of-date software vulnerabilities to bypass a network perimeter; however, those vulnerabilities are numerous.

The most widespread vulnerabilities in network perimeters found in 2015:

- Vulnerable software versions
- Data transfer via open protocols (Telnet, FTP, HTTP, etc.)
- Interfaces for remote access and network equipment server control can be accessed from external networks (while should be available to a limited number of administrators)

Each of these problems occurred in more than 89% of the systems studied and they were commonplace in 2014 as well. The number of the systems that had obsolete software on their network perimeter increased by 33%. The number of the systems, which contained interfaces for remote access and network equipment server control that could be accessed from external networks, was reduced to 89%, second most common. Last year, similar vulnerabilities were the most common ones as well. The use of open data transfer protocols increased by 9%, a widespread vulnerability in a network perimeter.

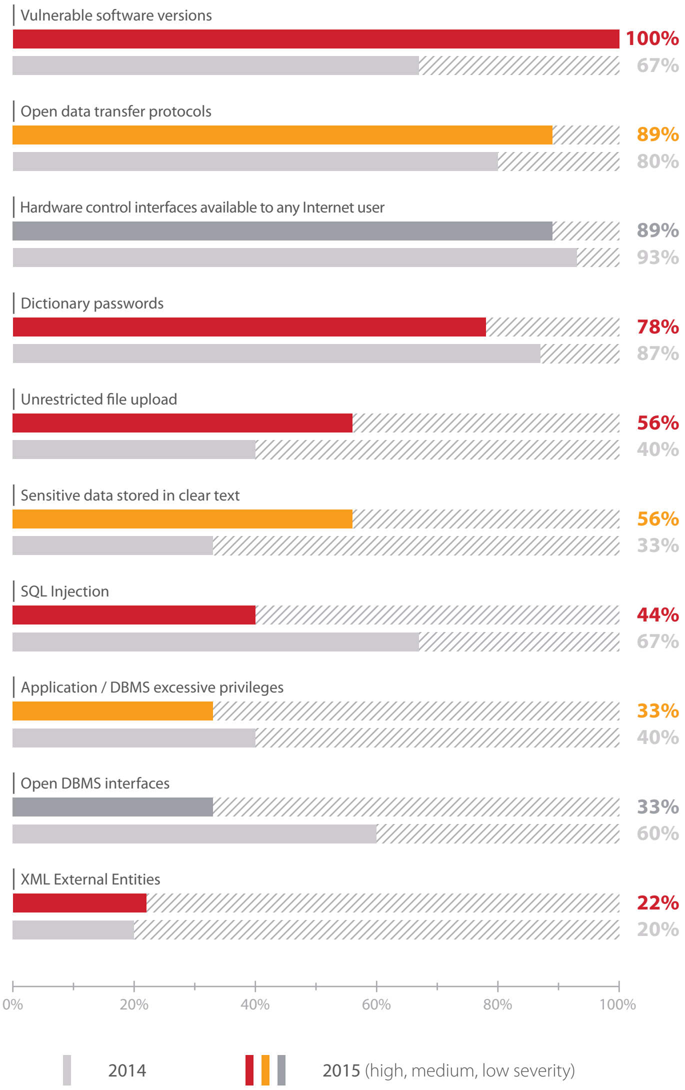

Figure 12. The most common vulnerabilities on a network perimeter

This time, SQL Injection is not listed in the top five common vulnerabilities. This severe vulnerability is caused by web application code errors and allows unauthorized access to a DBMS; however, it is still rated as a high severity threat and it was detected in 44% of the organizations. The general level of web application security is still low, which is confirmed in the results of Positive Technologies' "Security Trends & Vulnerabilities Review. Web Applications".

3.2.1. Vulnerable Software Versions

While testing network perimeters, PT specialists detected vulnerabilities caused by using vulnerable software versions. Such vulnerabilities were discovered in 67% of the companies tested in 2014.

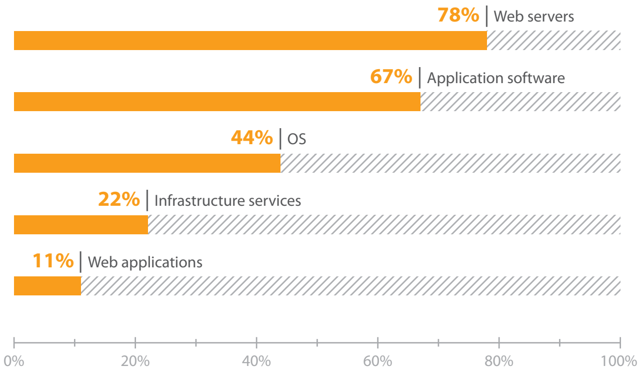

Figure 13. Outdated software versions on a network perimeter

The most widespread problem with network perimeters is still vulnerable web servers (78%). For example, critical vulnerabilities caused by using Apache HTTP Server 1.3.33, which is not supported by the vendor. The number of companies that had a perimeter with vulnerable application software has increased (from 40% in 2014 to 67% in 2015). For instance, some companies used the old version of OpenSSH Server that allowed arbitrary code execution. The number of systems that used vulnerable operating systems also increased (from 33% to 40%). For example, old versions of Windows are vulnerable to remote execution of arbitrary commands (MS08-067). At the same time the number of companies that had vulnerable versions of out-of-the-box applications on their perimeter has decreased.

3.2.2. Open Protocols

The use of open data transfer protocols is still a pressing problem. The flaw was detected in 89% of the systems and is the second most common flaw. All the systems used the FTP protocol. Telnet and HTTP are also widely used for access to a management interface. Due to the lack of data protection, an intruder is able to intercept sensitive information, including privileged users' credentials.

3.2.3. Equipment Management Interfaces

The problem of availability of equipment management interfaces from external networks is still one of the most common deficiencies.

The amount of the systems that had equipment control interfaces available from the internet has not changed (available via SSH protocols — 56%, via Telnet — 56%). 44% of the systems used HTTP to connect to equipment management interfaces from external networks.

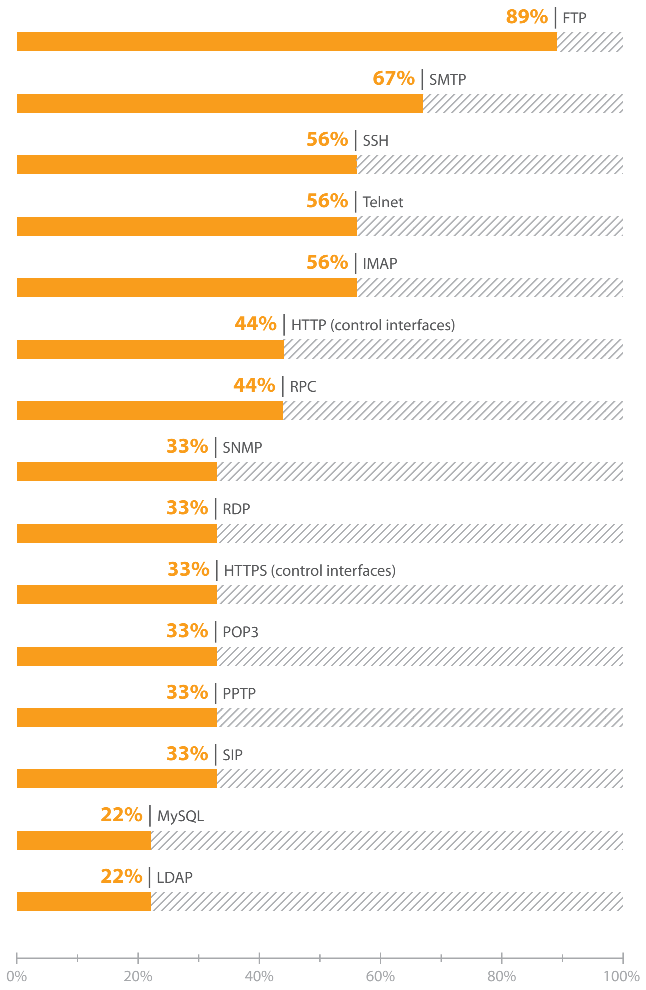

Figure 14. Systems by protocols used on network perimeters

There is a significant decrease (from 80% to 33%) in systems with an SNMP service available from their network perimeter for any Internet user, and one of the systems used the default value of the SNMP Community String (public).

3.2.4. Dictionary IDs and Passwords

The use of dictionary passwords is still one of the main security problem.

Penetration testing applies different methods to obtain user passwords: bruteforcing default users' passwords; bruteforcing passwords of accounts, whose logins were gained through exploitation of various vulnerabilities; bruteforcing hashes; and retrieving credentials out of encrypted values. During the analysis, the specialists used all of the passwords obtained through penetration testing. Passwords that could be bruteforced via common dictionaries within a short time by an attacker knowing only a user ID were considered dictionary passwords.

The number of companies that had such vulnerabilities in their network perimeter has slightly decreased (78% as compared to 87% in 2014). Weak passwords (such as admin) are still widely used (44% of the systems). The number of the systems, in which dictionary passwords (such as 12345678) were used to access a domain or email has halved since 2014 (a decrease from 40% to 22%). However, the number of the systems that used weak passwords for a DBMS (for example, sa) has increased significantly (from 13 to 33%).

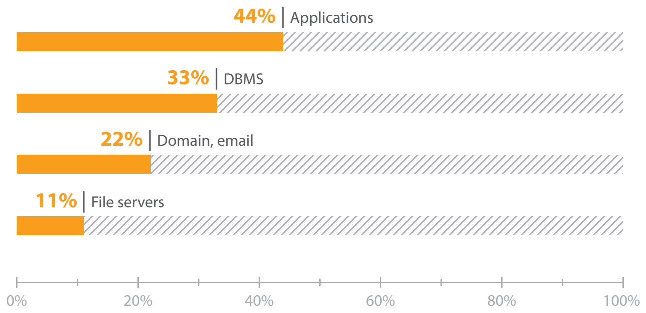

Figure 15. Dictionary passwords that grant access to a network perimeter

Additionally, weak passwords were used in 78% of privileged accounts, which is 11% higher than in 2014. The use of dictionary identifiers and passwords for privileged user accounts is the key stage in getting access to a LAN.

3.2.5. Unrestricted File Upload

According to the research, 56% of the systems allowed unrestricted file upload, which is 16% higher than in 2014. In most cases, by exploiting the vulnerability, PT specialists could not only execute commands on network perimeter servers, but also access LAN resources.

One of the systems allowed unrestricted file upload by exploiting vulnerable software configurations along with specific features of the operating system. PT specialists discovered a way to bypass restrictions on loading files with .php extension and to upload a command-line shell to the server.

3.2.6. Storing Sensitive Data in Clear Text

There has been a huge increase in the number of the systems that had this security flaw (from 33% to 56%). In 44% of these cases, data were stored in public resources. In 2015, it was possible to find personal data of users, domain credentials and credentials for access to a DBMS in companies' public web resources.

3.3. Security Analysis of Intranet Resources

Once a malicious user accesses the intranet, he or she can develop an attack and obtain full control over the whole IT infrastructure. In 55% of the systems, the specialists gained control over critical resources (Active Directory, DBMS, banking or ERP system). 28% of the tests resulted in full control over the whole infrastructure. This figure is considerably lower in comparison to 2013 and 2014. In those years, 80% of the tests led to privileges in critical systems. We should mention that in several analyses the goal was to gain control over certain resources without obtaining maximum privileges in the whole infrastructure (the goal was reached in every one of such tests).

As in 2013 and 2014, the researchers managed to gain maximum privileges in all critical systems by acting as a malicious insider. They gained full control over the whole infrastructure in 71% of cases (the same results were achieved in 2013).

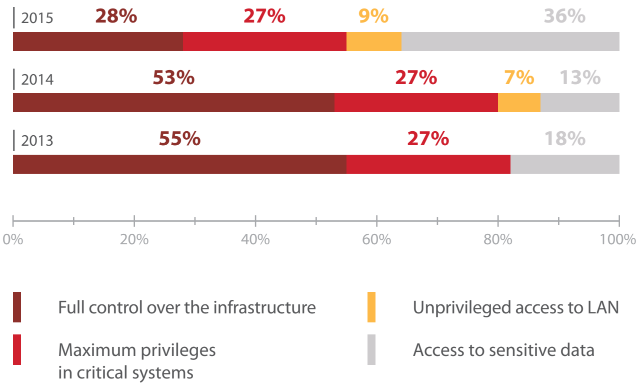

Figure 16. Systems by the level of privileges obtained by an external attacker

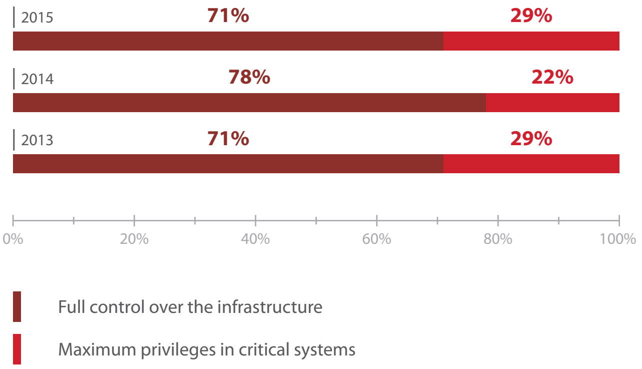

Figure 17. Systems by the level of privileges obtained on behalf of an internal attacker

According to Positive Technologies specialists, a low-skill intruder is able to access critical resources. In 18% of cases, the exploitation difficulty level was medium (as compared to 44% in 2014).

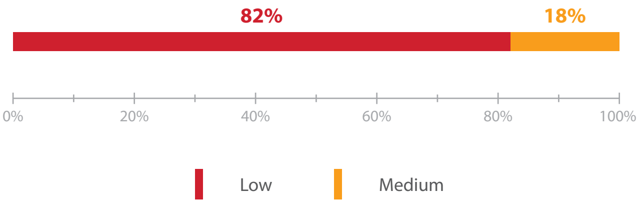

Figure 18. Difficulty of gaining access to critical recourses by internal attackers

If attackers had access to a company's intranet, they needed to exploit four different vulnerabilities to obtain control over critical resources. It is one step fewer than in 2014 and one step faster than in 2013. In 2015, the longest attack took six stages.

As in 2014, a general intranet attack could be conducted in only three steps:

1. Gain access to Active Directory with user rights as a result of credential bruteforcing.
2. Obtain maximum local privileges for user workstations by bruteforcing passwords or getting passwords in clear text from system resources.
3. Upload malware to workstations and obtain credentials of a domain administrator with an active session.

The problem of the use of dictionary credentials is still the largest and most persistent. Each and every system had this vulnerability. In 91% of the systems, they were used by privileged users. Among the most prevalent vulnerabilities were security flaws in network layer and data link layer protocols that might lead to traffic redirection and interception of network configuration data.

In 91% of the systems, the PT specialists detected problems such as weak protection of privileged accounts and insufficient antivirus protection. The use of vulnerable software and storing sensitive information in clear text are the fifth most common problems.

These results follow the same pattern as the previous year. However, there is an increase in the number of systems that contained flaws such as the use of vulnerable software, management equipment interfaces available to any LAN user, and transferring data via insecure protocols.

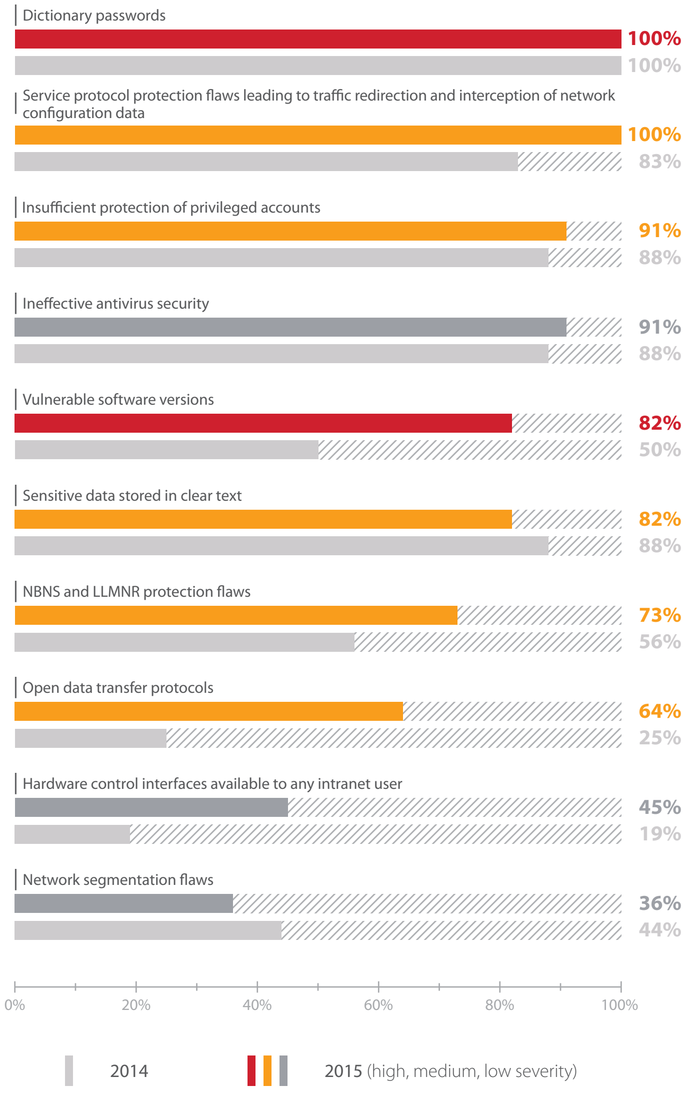

Figure 19. The most common intranet vulnerabilities

3.3.1. Dictionary Passwords

The usage of dictionary passwords was detected in each internal network of the systems under test. More than half of the systems used dictionary passwords to access a DBMS, network equipment, or applications.

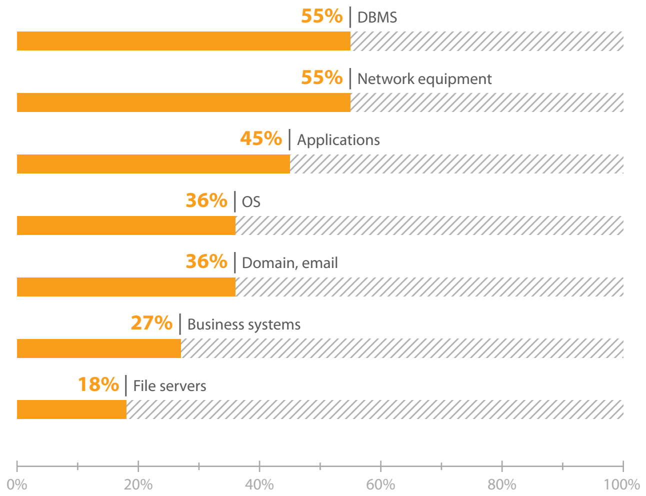

Figure 20. Systems by the usage of dictionary passwords

The most commonly used passwords are combinations of 7 lowercase letters (44%). In 38% of cases, less than 7 characters were used: figures and lowercase letters; combinations of keys that are set closely on a keyboard (1qaz2wsx), or an empty password.

The passwords admin and 123456 were found in one third of systems.

The password admin is the most common flaw among privileged users. It is the most common flaw together with the combinations of less than 7 lowercase letters (the same as in 2014).

3.3.2. Secure Flaws in Service Protocols

Every system contained various defects in service protocols (ARP, STP, NBNS, LLMNR). Each analysis of LAN traffic revealed the lack of protection against ARP Cache Poisoning. PT specialists detected a lack of protection for NBNS (in 73% of the systems) and LLMNR (36% of the systems). Both protocols are used by default in Windows systems to resolve names when a DNS server is not available. In general, the number of the systems with vulnerable service protocols increased in 2015. Companies' internal networks are still not protected against data link layer and network layer attacks.

If there is no need for specific protocols, it is better to disable them. If their use is required, and no alternative can be used, then use preventive security measures.

3.3.3. Insufficient Protection for Privileged Accounts

Insufficient protection for privileged accounts is one of the most common flaws in corporate infrastructure (91%). The protection of privileged accounts against attacks conducted by intruders with local administrator privileges is not sufficient. As a result, an intruder is able to gain full control over the domain infrastructure. This flaw was detected in every corporate system that is based on domain architecture.

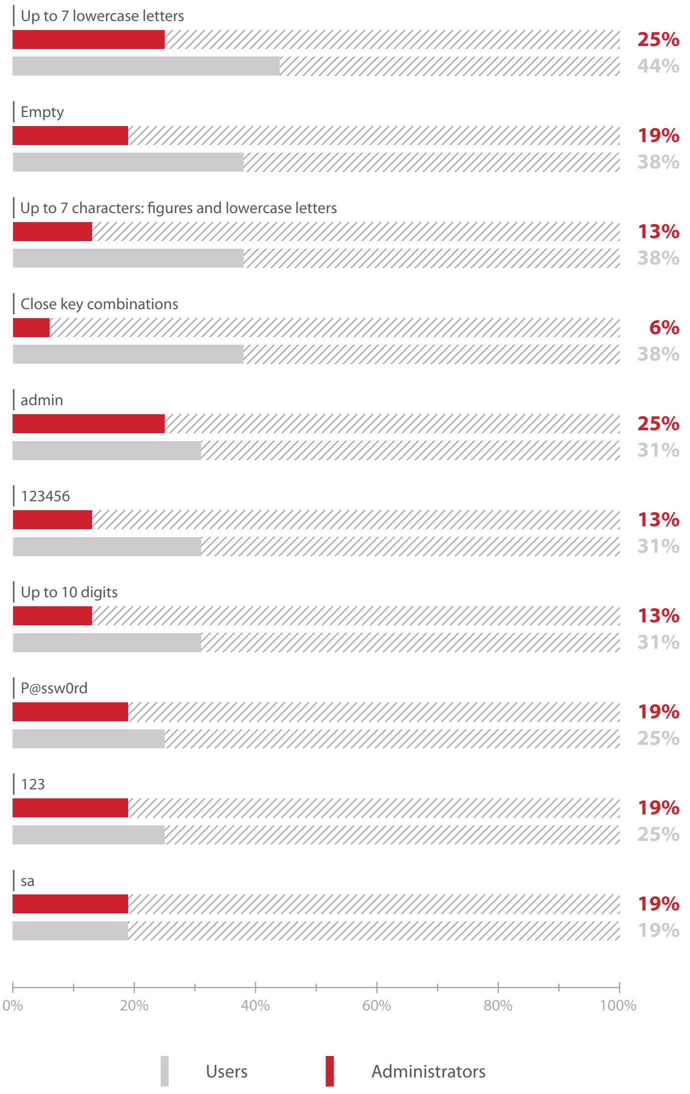

Figure 21. Dictionary passwords in internal networks

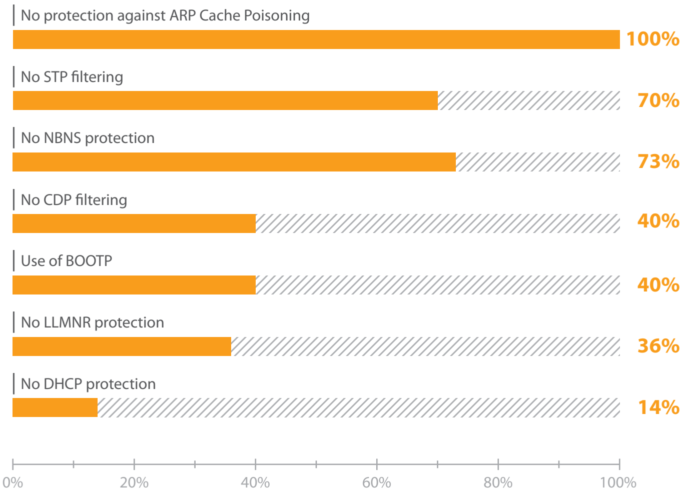

Figure 22. Systems by service protocol security flaws

3.3.4. Insufficient Antivirus Protection

The number of the systems that lack antivirus protection is the same. Antivirus protection methods that are used in these systems are weak and allow an attacker to run malicious software.

Even if antivirus software detected attacks and blocked malware, local administrator privileges allowed an attacker to disable the protection system, include this software to the exception list, or copy server process memory.

By exploiting this vulnerability, an intruder can obtain Windows users' credentials (domain administrators, in particular) in clear text.

3.3.5. Storing Sensitive Data in Clear Text

Storing sensitive data in clear text is common in 82% of the systems. Files that contained credentials for access to critical resources, private keys for access via SSH, credentials for privileged access to a database, personal data of users, financial and other sensitive information were discovered during the security analysis.

3.3.6. Vulnerable Software Versions

The use of vulnerable software versions became more common (82%) in comparison to 2014.

Almost half (55%) of all the systems under test used vulnerable software versions. 45% of the systems used operating systems without security updates installed.

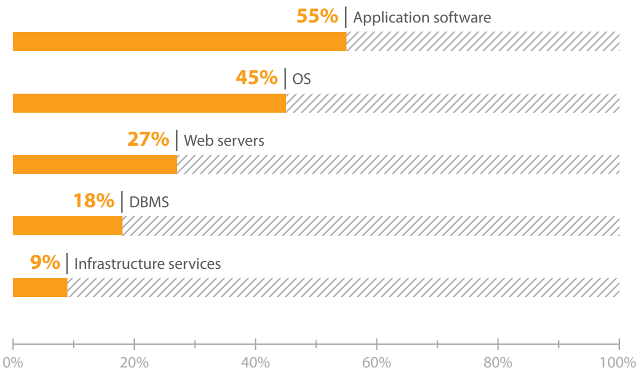

Figure 23. Obsolete software in internal networks

4. Attack Vectors

This section includes assessment of medium-security information systems by various attack vectors. They were classified according to vulnerable system components that allowed unauthorized access to resources.

The security level was evaluated 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, protection tools deployed correctly).

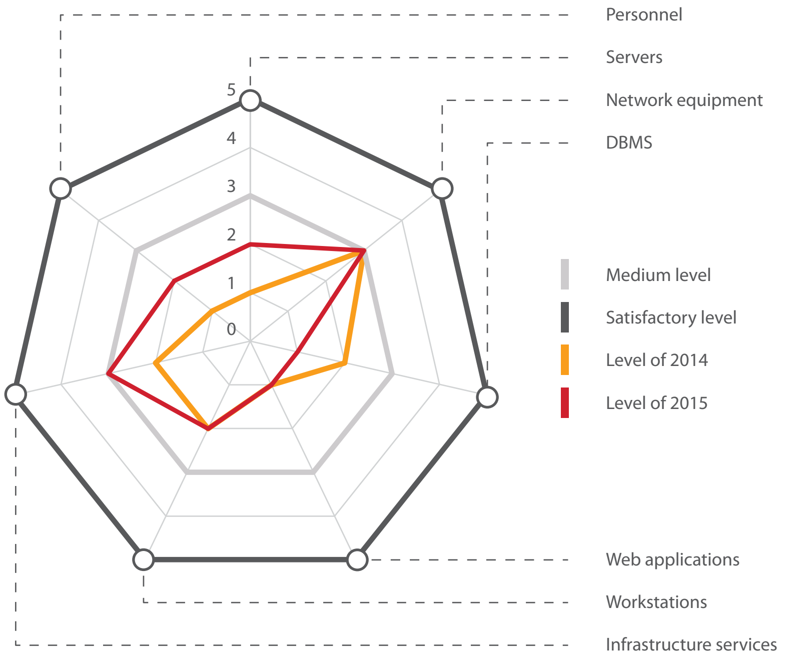

Figure 24. General security level of specific system components

The overall security level is higher than in 2014. A decrease in the security level is observed only in the DBMS: most attack vectors were based on vulnerabilities in these systems. The infrastructure service and network equipment security level is ranked as medium. Web applications are still poorly secured. Their multiple vulnerabilities allow an intruder to bypass a network perimeter and gain control over critical resources. The security level of such categories as Personnel and Servers has increased, but it is still low.

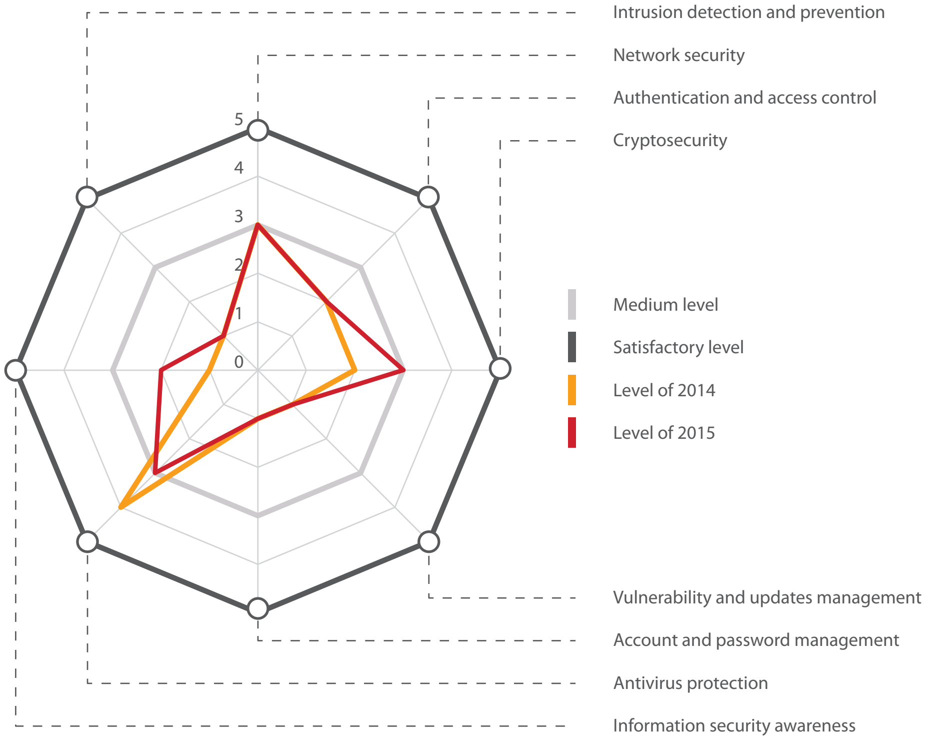

Figure 25. General security levels depending on a protection mechanism

5. Assessment of Protection Mechanisms

The level of staff's information security awareness and cryptographic protection became higher; though the lack of antivirus protection was detected in almost every system in 2015.

The Intrusion Detection and Prevention category still has a low rating. No measures against attacks were taken by system administrators, according to 2015 research. Automated systems (such as application firewalls) were found on network perimeters of a number of companies, but their features did not provide protection against attacks.

6. Results of the Assessment of Staff Information Security Awareness

As part of the penetration testing conducted in 2015, IS awareness checks were carried out among users. They consisted of a series of hacker attacks agreed upon with the appropriate customer and further tracking of staff responses. The checks were based on emailing messages containing an attachment or with a link to an external source. The test monitored the number of links opened and files run, as well as the number of credentials entered. Messages were emailed on behalf of both a company's employee and unknown individual or organization.

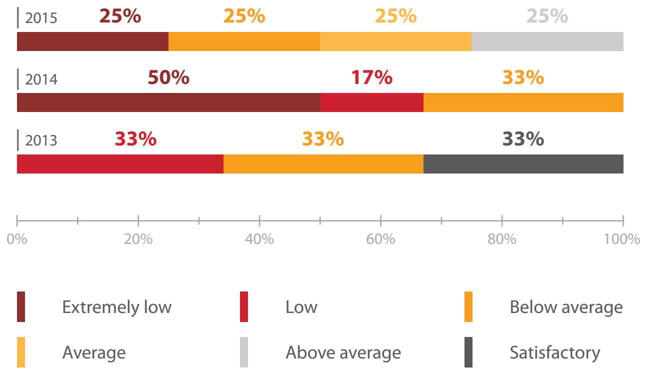

Figure 26. Users' information security awareness

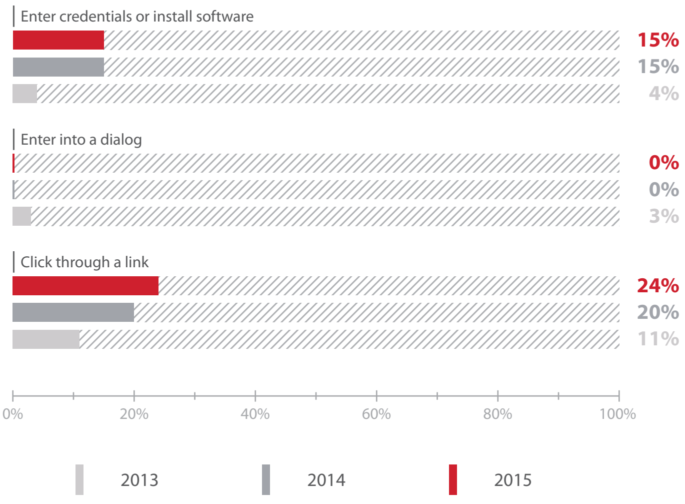

Figure 27. Successful attacks by the total number of messages

The awareness check was based on Positive Technologies' expert opinion.

The results obtained during the test revealed an increase in information security awareness. The number of companies that showed a low awareness level has halved. The awareness level was assessed as not less than medium in 50% of the companies.

It is important to note that the number of users who followed the link increased in comparison to the previous years, while the number of users who loaded and ran the file did not change. Most of such cases were detected in companies with a low awareness level.

This graphs show the general awareness level has risen (though it is still too low).

7. Security Analysis of Wireless Networks

Security analysis of wireless networks was also carried out in 2015. Wireless network security analysis is aimed at detecting flaws in access points and clients' Wi-Fi devices with ranges of 2.4 GHz and 5 GHz via 802.11a/b/g/n and flaws in architecture and wireless access organization. 67% of the systems demonstrated security of a medium level or below.

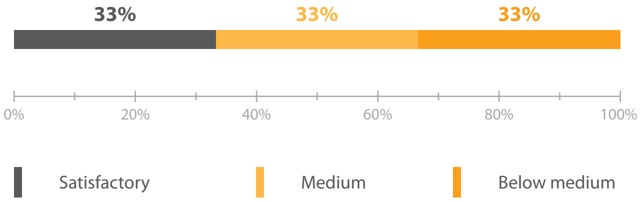

Figure 28. Systems by the wireless networks security level

Among the detected vulnerabilities was the use of the WPS mechanism to simplify the wireless setup process. To connect to an access point, a user needs a PIN that consists of figures only. An intruder is able to bruteforce the PIN and connect to the access point.

PT specialists also revealed the use of unauthorized access points. By connecting them to a LAN, an intruder is able to access internal networks. In a number of the systems, the lack of protection of separate wireless networks has been detected. The lack of network traffic encryption mechanisms may lead to traffic interception. An intruder is able to obtain sensitive information (e.g., credentials of privileged users). Among common vulnerabilities is also the use of default user accounts to access a web-based interface for network equipment management.

One of the tests revealed that almost all wireless networks are available outside of the controlled area, while credentials of a domain user were stored on public resources of the network perimeter in clear text. Thus any external intruder outside the controlled area is able to connect to a wireless network of a company and attack LAN resources.

Summary

The study carried out in 2015 shows that companies' information infrastructure is still vulnerable to attacks by both an external intruder and a malicious insider. The number of systems that allow bypassing their network perimeter and gaining unauthorized access to critical resources decreased in comparison to the previous year. The difficulty level of performing an attack is higher for an external intruder. Nevertheless, the level of protection against attacks by an external intruder is still quite low. The level of protection against insider attacks remains very low. In the majority of cases, attacks could be conducted by exploiting the same vulnerabilities that were common in the previous years.

The most common vulnerabilities of a network perimeter are vulnerable software versions, the use of open communication protocols, and accessibility of equipment management interfaces to any internet user. The use of dictionary credentials (even among privileged users) is still a large problem.

Flaws in account and password management and the lack of protection for service protocols were the most common problems in internal networks of the systems studied. The number of systems that have vulnerabilities caused by the lack of protection for privileged accounts, insufficient antivirus protection, storage of data in clear text, and the usage of obsolete software is still high.

The level of user security awareness in 2015 is rated higher than in 2014. However, the number of employees who followed the fake link has increased, and a quarter of the companies demonstrated a very low level of awareness.

During wireless network security analysis, security issues were detected in all the systems studied. Considering the risk level of identified deficiencies, the general level of wireless network security can be assessed as medium.

Finally, it is worth noting that the safety of corporate systems requires a complex approach. Without taking into account all components of a system, it is impossible to create a secure infrastructure. In 2015, as in the previous years, the vectors of attacks on companies' corporate infrastructure from external networks and by a malicious insider were based on exploitation of common vulnerabilities and weaknesses, to eliminate which it is enough to apply the most general principles of information security. It is important to pay special attention to the password policy, protection of privileged accounts, and protection against attacks on public web applications. It is also necessary to ensure regular updating of used software and automated installing of security patches.

To reduce the risk of compromising critical systems by external intruders, it is important to pay special attention to resources available from external networks. In practice, the vast majority of successful attacks that result in gaining access to critical resources and bypassing a company's network perimeter are not based on exploitation of vulnerabilities that are officially published on official websites of organizations and their servers. Such attacks are performed by using other resources of the target company, which should not be available on its network perimeter (e.g. databases, unused debug interfaces, remote access or management interfaces, infrastructure services interfaces, such as LDAP). Interfaces that provide for access to such resources can be opened because of administrators' mistake.

Representatives of large companies who are responsible for the security of information infrastructure usually don't know exactly what kind of resources are available from external networks. Such "forgotten" resources are the most vulnerable, because their software might not be updated for several years, their privileges and accounts are not managed. Attacks on these resources can all be overlooked if the company does not engage effective means of detecting and preventing them. In particular, to protect against attacks on web applications, it is necessary to use application firewalls with effective correlation rules. To control the resources of a network perimeter, it is key to perform regular scanning of resources available from external networks (for example, once a month). For early detection and elimination of vulnerabilities in critical web applications' code, you must regularly analyze their security, both by black- or gray-box or white-box methods with a detailed analysis of the source code. Such works should be carried out not only at each stage of application development, but also in terms of systems put into operation (for example, twice a year), followed by elimination of identified vulnerabilities.

As for the protection of corporate systems against attacks by an insider, the picture in this area has not changed. The most common insider attack that allows an intruder to gain full control of a company's information infrastructure is based on the same vulnerabilities as two years ago. Basic recommendations in such case are the same. It is necessary to follow basic principles of information security: develop and comply with a password policy that prohibits the usage of simple passwords, implies mandatory two-factor authentication for privileged users of critical systems, requires regular changing of passwords (for example, every 60 days). Make sure to pay special attention to such problems as old versions of software, open communication protocols, storage of sensitive information unencrypted on servers and employees' workstations.

Aside from basic measures, we highly recommend performing regular security audit of information systems and penetration testing, both internal and external. According to Positive Technologies specialists, in order to decrease the risk of compromising corporate systems and reach an accessible level, it is necessary to perform such check as often as twice a year and then ensure that identified vulnerabilities are fixed. Moreover, it is recommended that all of a company's employees are trained in order to raise their security awareness level, as well as to estimate the effectiveness of such training.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions that include vulnerability and compliance management, incident and threat analysis, and application protection solutions. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control Systems (ICS), Banking, Telecom, Web Application, and ERP security. Recognition from the analyst community, including Gartner, IDC, and Forrester have seen us described as '#1 fastest growing* company in vulnerability management' and 'most visionary in web application protection**'. To learn more about Positive Technologies please visit 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+.

**Source: Gartner Magic Quadrant for Web Application Firewalls 15 July 2015.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com