SECURITY TRENDS & VULNERABILITIES REVIEW 2015

CORPORATE INFORMATION SYSTEMS

POSITIVE TECHNOLOGIES
2015

Contents

1. Introduction

State-of-the-art technology allows companies to create complex corporate infrastructures made up of many subsystems. Sometimes, network architecture is so complex, that even large corporations that appropriate funds for the protection of their resources cannot provide full security. Security analysis helps to detect the most vulnerable system components and fix security flaws as quickly as possible.

Penetration testing is one of the methods used in information system security analysis. Penetration testing simulates a potential attacker's actions from both the Internet and the company's intranet. This approach to security analysis assesses the system's real security level and discovers flaws in current security mechanisms.

This report includes annual statistics on penetration testing carried out by Positive Technologies in 2014 and a comparative study of results obtained in 2014 and 2013. This report assesses the evolution of information security at the major companies analyzed.

The report is based on 18 systems tested in 2014. The research covers major state and commercial companies (including those in the Fortune Global 500 [1], a ranking of top 500 corporations worldwide). To select a system, we relied on self-reported statistics around pentesting results. We excluded the results of 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 system as a whole. In order to avoid disclosure of information concerning vulnerabilities, the report did not include systems whose owners announced Positive Technologies was conducting testing during the specified period.

[1] http://fortune.com/global500/

2. Executive Summary

General Results:

- In 2014, 94% of systems studied contained vulnerabilities allowing an attacker to gain full control over some critical resources — Active Directory, ERP, e-mail, and network equipment control systems. In 67% of cases, an external attacker could gain full control over the most critical resources.

- An internal attacker can gain full control over a company's whole information infrastructure in 44% of cases. In 39% of organizations, attackers only needed access to the intranet to get control over such resources. The results are similar to those obtained in 2013.

Security Perimeter Flaws:

- In 73% of systems, an outside attacker accessing the network from the Internet could access intranet hosts without using social engineering. When combining the use of technical methods with social engineering, outside access to the system was gained in 87% of cases.

- In 80% of cases, an external attacker can get maximum privileges in key business systems and in 53% of systems — gain full control over the whole company's infrastructure.

- On average, an outside intruder needs to exploit two different vulnerabilities to come through the network perimeter without using social engineering; even low-qualified programmers can conduct such attacks in 74% of cases.

- In 60% of all cases, the penetration vector is based on web application code vulnerabilities.
For example, SQL injection appears in 67% of systems, and unrestricted file upload — in 40% of systems. Different web application vulnerabilities were detected in 89% of the systems investigated. The average security level remains as low as it was in 2013.

- As in the previous period, dictionary IDs and passwords remain one of the most common vulnerabilities that was detected in 87% of systems studied. Moreover, 67% of companies used simple passwords even for privileged user accounts. About half, 53% of companies used dictionary credentials to access public web applications.

- Heartbleed and Shellshock vulnerabilities, both of which garnered media scrutiny in 2014, were not so widespread due to the information available and updates installed in time by most large companies. However, those actions were selective: 78% of systems had critical vulnerabilities related to outdated software updates. The average age of the most outdated patch was 73 months (over six years).

- The average level of network perimeter security in 2014 remained similar to 2013. Additionally, a low qualification is enough to conduct an external attack: a low-qualified attacker could successfully attack 61% of systems, compared to just 46% in 2013. Penetrating the perimeter in 2014 (as in 2013) requires exploitation of only two vulnerabilities on average.

Intranet Security Flaws:

- All the systems tested from the inside showed that an internal attacker located in the user segment of the network can expand his or her privileges and gain unauthorized privileged access to critical resources (banking and ERP systems, and some other key network components). Such an insider can obtain full control over company's whole information infrastructure in 78% of cases.

- In 56% of cases, low internal attacker qualification is enough to access critical resources. If there is access to the internal network, an attacker needs to exploit three different vulnerabilities, on average, to gain control over critical resources, which is worse than the 2013 results when an attack usually had five stages.

- Weak passwords are still the most common intranet security vulnerability detected in all the systems studied. Every system had weak administrator passwords. Less frequent vulnerabilities occur due to improper protection of privileged accounts, sensitive data in clear text, and insufficient implementation of antivirus protection. Vulnerabilities from each category were detected in 88% of systems.

- The security level of internal networks has decreased as compared to 2013: the average number of attack stages has dropped, and the qualification needed to conduct an attack has also dropped. Despite some improvements (for example, the average level of network security has increased), the protection means used are still not enough to counter attackers. Exploiting widespread and well-known vulnerabilities is enough for a successful attack.

Lack of Staff Awareness:

- The study of users' information security awareness by means of social engineering revealed various flaws in all the systems investigated. 67% of systems showed a low or extremely low level of user's awareness. 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 in every five people followed a link offered; 15% of the users downloaded executables or specified their credentials in an authentication form provided.

- The staff awareness level in 2014 was significantly lower than the previous year (in 2013 the awareness level was acceptable in about one third of systems tested). In 2014, none of the companies reached the acceptable level.

3. Inputs

This research utilized information from corporate information systems of 18 large-scale companies. Similar to 2013, organizations from a range of different industries took part in the research: banking and financial services, manufacturing leaders, transport, telecoms, IT leaders, and a governmental organization. Most data comes from manufacturing (44%) and banking (28%).

More than half of the enterprises were geographically distributed and had many subsidiaries and branches located in different cities and countries. Most systems tested for penetration had hundreds of active hosts available at the network perimeter.

Industrial control systems (ICS) were the focus of penetration tests carried out as part of works in the previous years. The results of the research by Positive Technologies prove the importance of system security assessment and elimination of the vulnerabilities detected in due time.

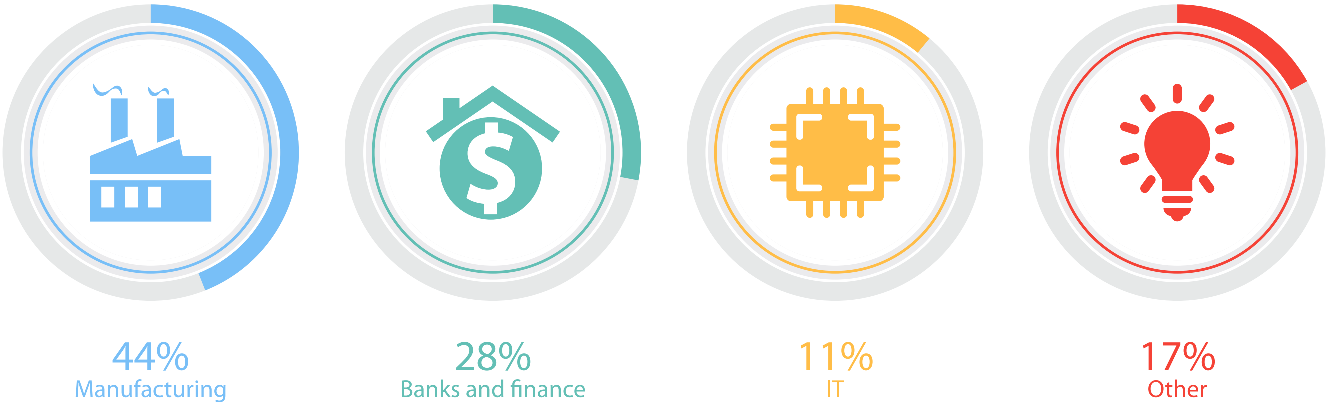


Figure 1. ***System distribution by industries***

The testing within the specified period is made up of several types of penetration tests: external, internal, and complex (the latter included both external and internal testing).

Exactly 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 one third of the systems. 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 17% of the systems studied.

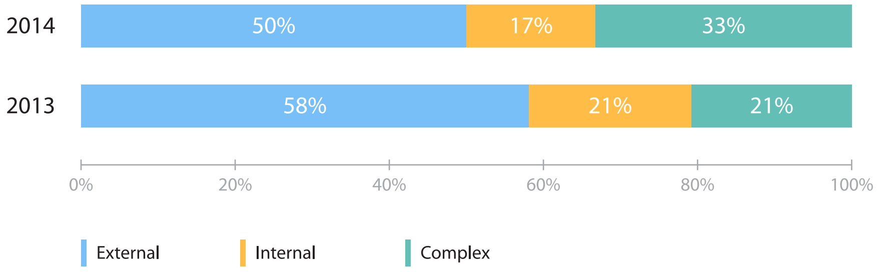


Figure 2. ***Penetration testing types (per system)***

As part of the security analysis service, staff awareness of information security was assessed for 33% of companies. We performed various checks simulating well-known social engineering attacks (e.g., phishing emailing) in the course of the works. Statistics on users' awareness are provided in section 7.

4. Statistics as of 2014. Comparative study of results obtained in 2013

4.1. Overall Penetration Testing Results

In 2014, 94% of systems studied contained vulnerabilities allowing to gain full control over some critical resources — Active Directory, ERP, e-mail, and network equipment control systems. In 67% of cases full control over the most critical resource could be gained by any external attacker, and in 27% of cases having an access to intranet's user segment was enough.

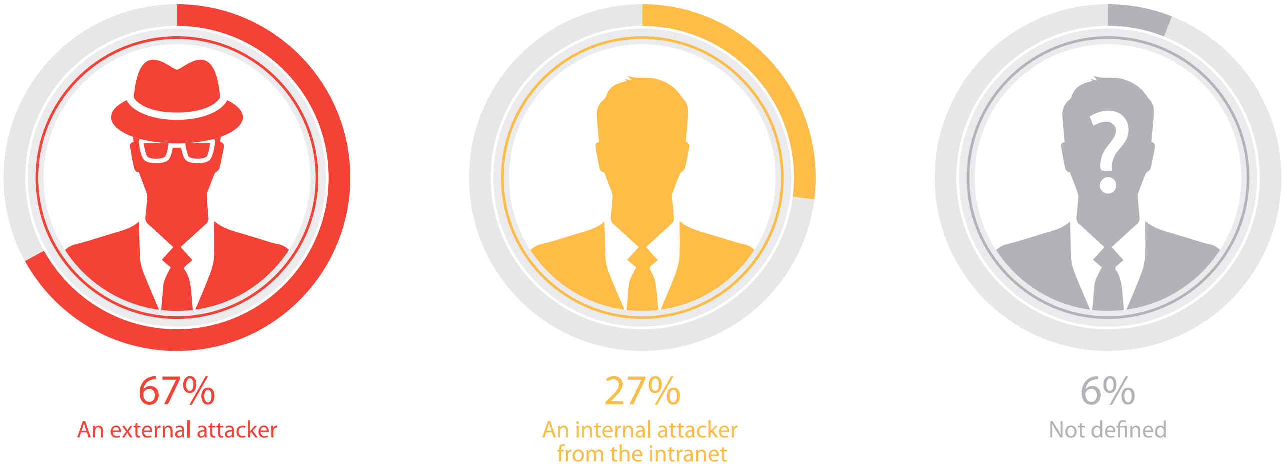


***Figure 3.* Attacker's minimal access level required to gain full control over critical resources**

An external attacker can gain full control over company's whole IT infrastructure in 44% of cases. In 39% of organizations, attackers only needed access to the intranet to get such control. The results are similar to those obtained in 2013.

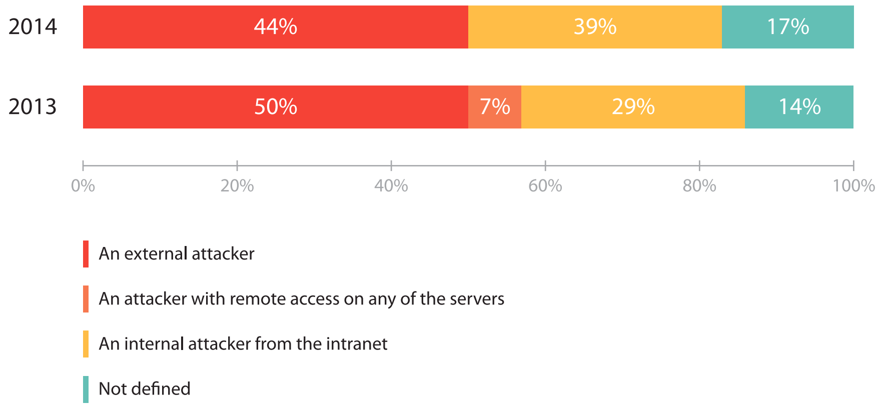


***Figure 4.* Attacker's minimal access level required to gain full control over the whole infrastructure**

Almost all of the systems studied in 2014 appeared to be exposed to high-severity vulnerabilities, only one system had neither critical nor medium-severity vulnerabilities. In 2013, critical vulnerabilities were discovered in more than 90% of the investigated systems. Moreover, medium-severity vulnerabilities were detected in all the systems in 2013.

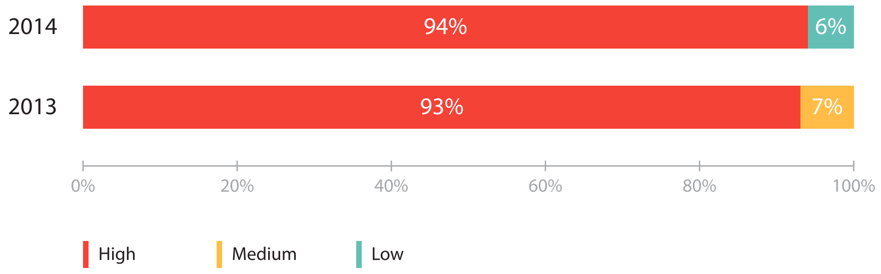


***Figure 5.** Systems compared by maximum vulnerability severity*

The same is true for vulnerabilities resulting from incorrect configuration: only one system (6%) had neither high- nor medium-severity vulnerabilities resulting from incorrect configuration. Such vulnerabilities were detected in almost all systems in both 2014 and 2013.

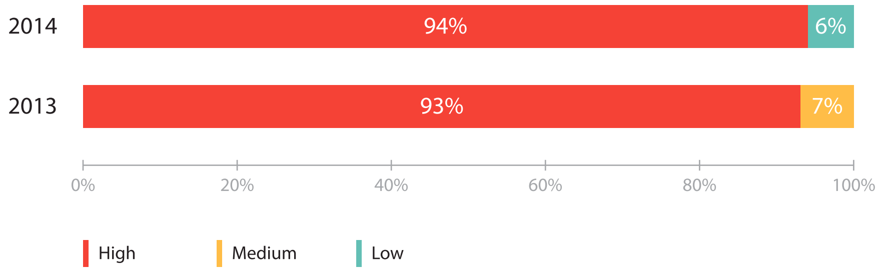


***Figure 6.** Systems compared by maximum severity of vulnerabilities caused by configuration flaws*

Most systems (78%) studied in 2014 had critical vulnerabilities related to outdated OS and application software versions. This figure is much worse than the previous year's results, where slightly more than half of such systems had these types of problems. The average age of the most outdated patch was 73 months (over six years), compared to just 32 months in 2013. In three systems out of 18, you could still find MS08-067 (CVE-2008-4250), 6-year-old OS Windows critical vulnerability widely used not only by hackers, but also by the Conficker network worm.

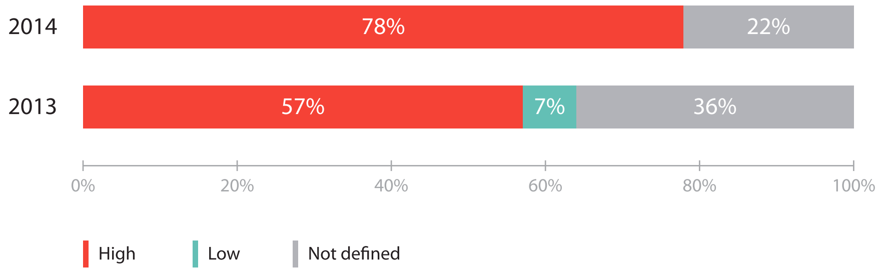


***Figure 7.** Systems compared by maximum severity of vulnerabilities caused by the lack of security updates*

22% of systems in 2014 proved to have no vulnerabilities caused by the lack of necessary updates, which is 14% less than in 2013. Vulnerabilities related to the lack of necessary updates can still be found in all the systems studied. External penetration testing is conducted with the privileges identical to those of a potential attacker and does not include full audit of all the network resources.

Almost every organization (89%) studied in 2014 has vulnerabilities related to web application code errors. More than half of the companies (61%) had high-severity vulnerabilities, such as SQL injection or unrestricted file upload. Nevertheless, it is necessary to take into account, that web application vulnerabilities could still be found in all the corporate networks studied. However, the testing was performed by the black box method, which identifies some but not all flaws.

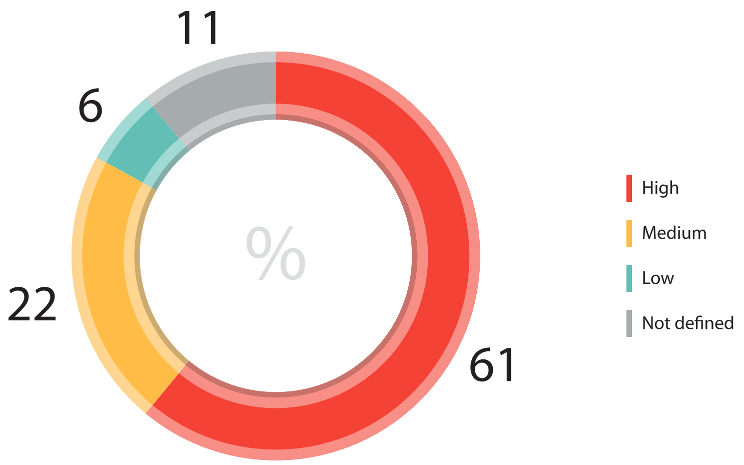


Figure 8. Maximum severity of detected vulnerabilities caused by web application code flaws

4.2. Security Analysis of the Network Perimeter

87% of systems externally tested for penetration had their LAN resources exposed to attacks from external networks. Any external attacker can access the intranet without using social engineering in 73% of the companies, which corresponds, to the level in 2013. In two systems out of 15, breaking through the perimeter from the outside appeared to be possible only via social engineering. Additionally, the administrator of the company's official web site could bypass one of those two perimeters via technical methods.

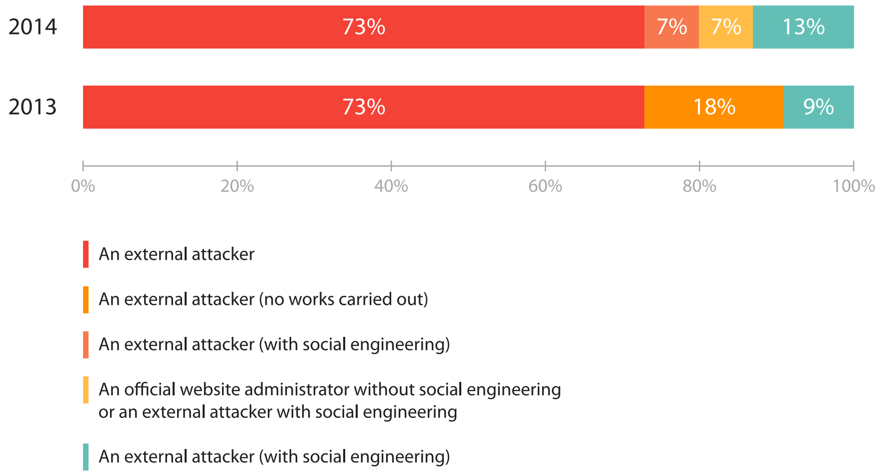


Figure 9. Minimal level of attacker's qualification required to bypass the perimeter

In most cases (87%), a low- or medium-qualified attacker can bypass the perimeter. Only one of the 15 perimeters studied could be bypassed in an obvious way — brute forcing the administrator's dictionary password for the RPD interface available from the external network. In 13% of cases, it was necessary to use social engineering against the company's employees in order to bypass the perimeter. All in all, bypassing the perimeter was more difficult in 2013: very low attack difficulty was enough for 9%, low — for 37%, and medium — for 36%.

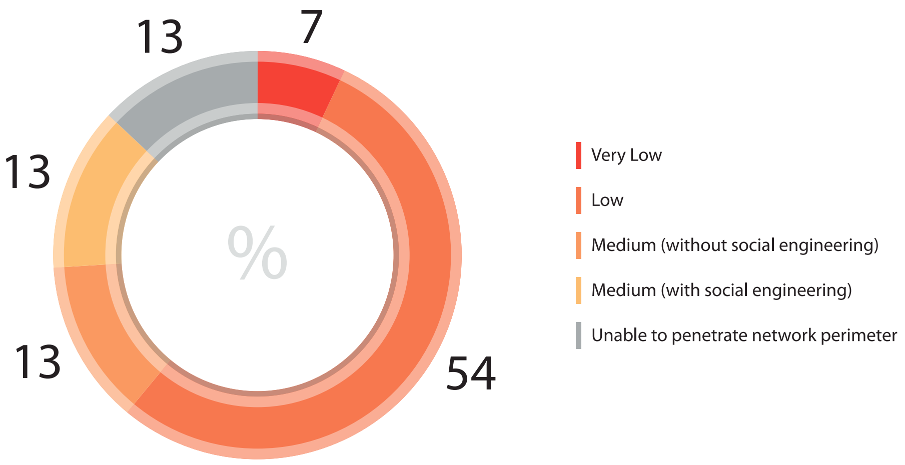


***Figure 10.* Difficulty of penetrating the perimeter**

On average, an attacker needs to exploit two different vulnerabilities to bypass the network perimeter, just as in 2013. However, only one vulnerability was enough to penetrate more than half of the systems (6 out of 11) in 2014. In 2014, 60% of intranet penetration vectors was based on the exploitation of web application vulnerabilities. By contrast, the percentage of penetrations related to dictionary passwords and outdated software vulnerabilities had decreased compared to 2013. On average, there were two intranet penetration vectors detected in every system, whose perimeter could be bypassed without social engineering.

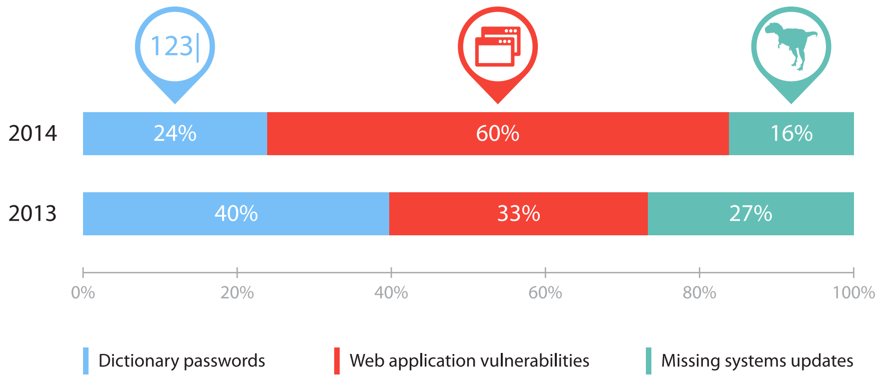


***Figure 11.* Attack vectors for penetrating the network perimeter**

The most common vulnerabilities at the network perimeter are:

- Interfaces for remote access and network equipment/server control that should be available to a limited number of administrators can be accessed from external networks
- Dictionary passwords, including default and empty ones
- Data transfer via open protocols (Telnet, FTP, HTTP, etc.)

Each of those problems occurred in more than 80% of the systems studied.

In 2013, similar vulnerabilities were the most common ones as well. In 2013, a high-severity vulnerability related to dictionary passwords was the most widespread one. In 2014 though, this vulnerability was the second most common, but the percentage of systems containing it has not changed. Almost every system (93%) had network equipment and server control interfaces available for any external user.

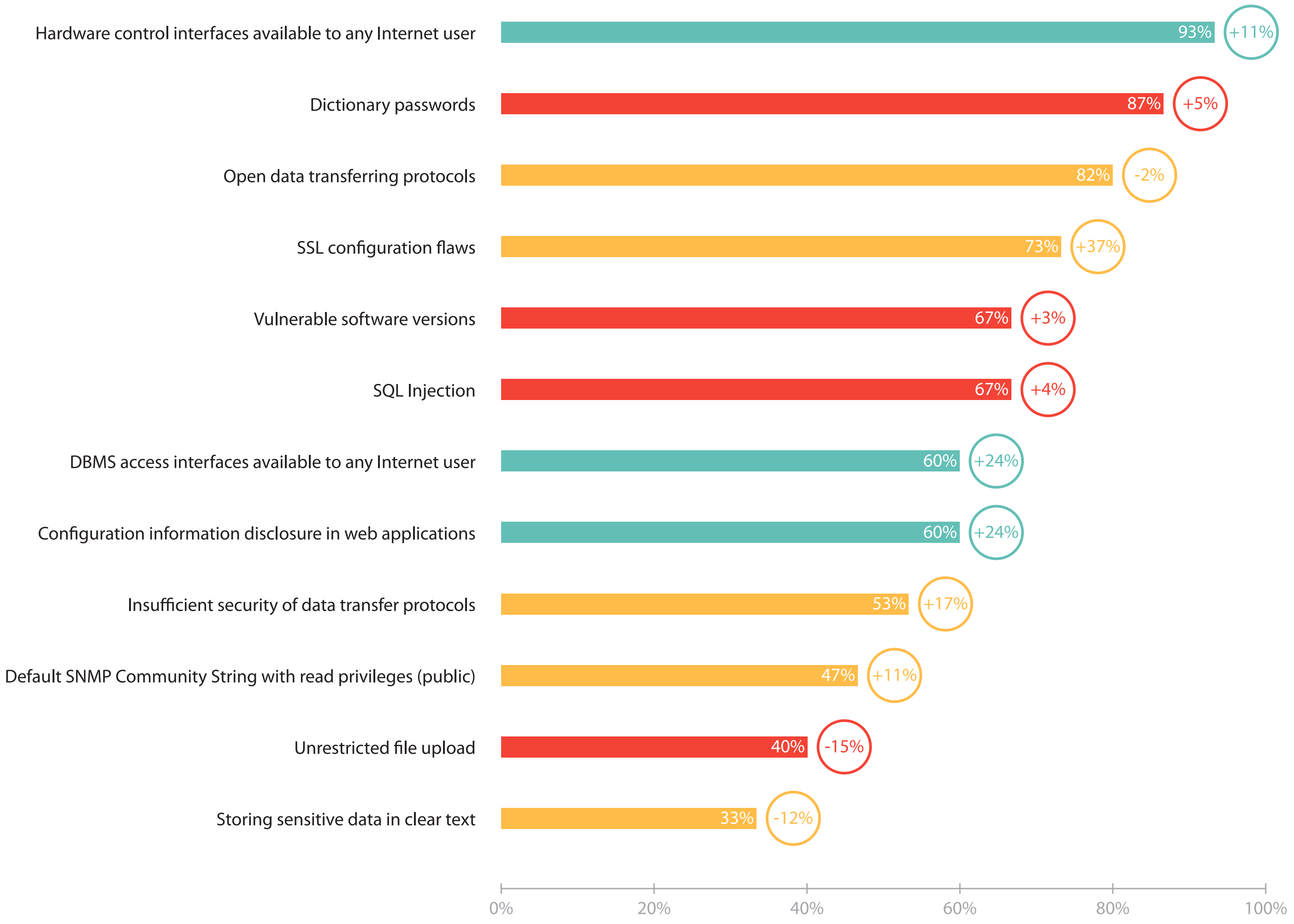


Figure 12. The most common vulnerabilities at the network perimeter

4.2.1. Available Interfaces for Equipment Control

There are a variety of different services available at the company's network perimeter from external networks. Many of those services involve additional risks.

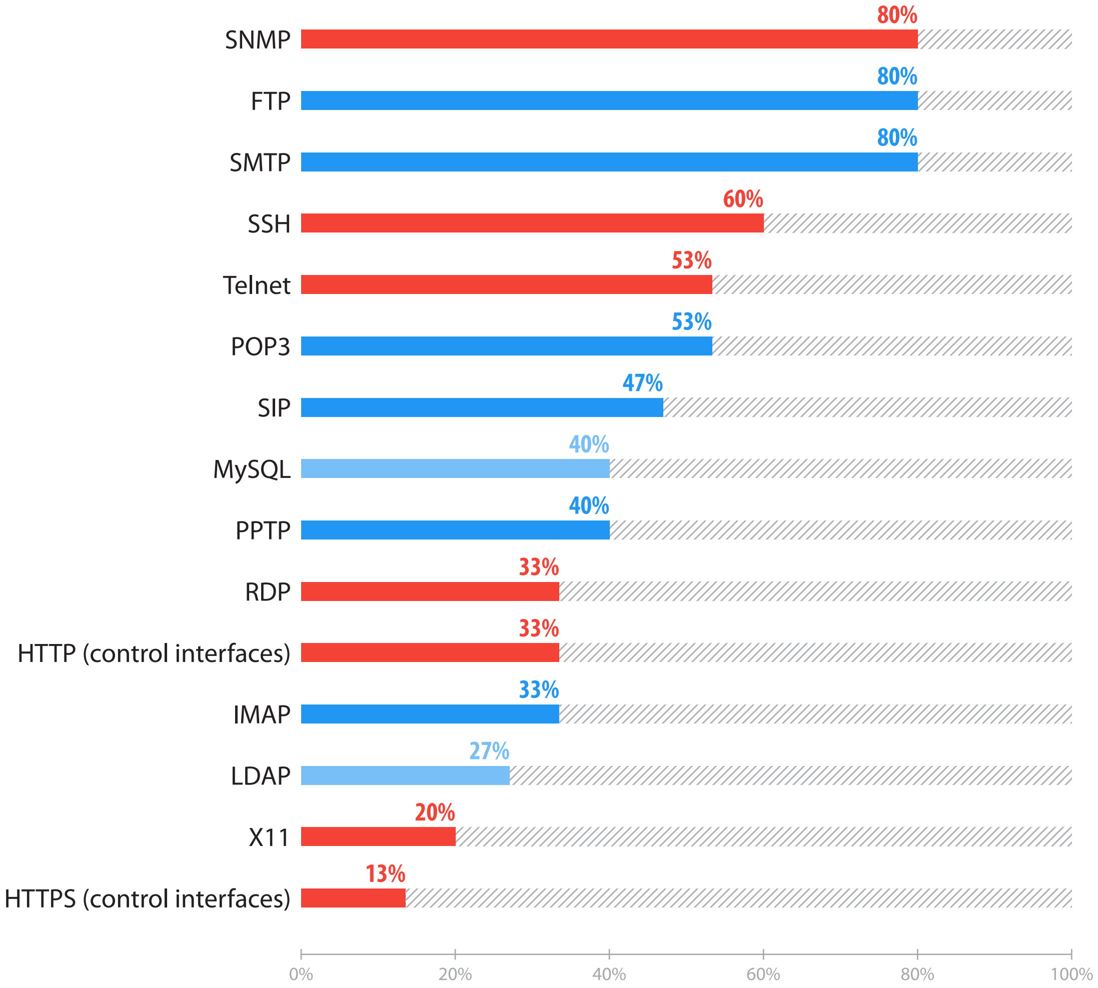


***Figure 13.** Statistical comparison of protocols, including remote access interfaces, used at the network perimeter*

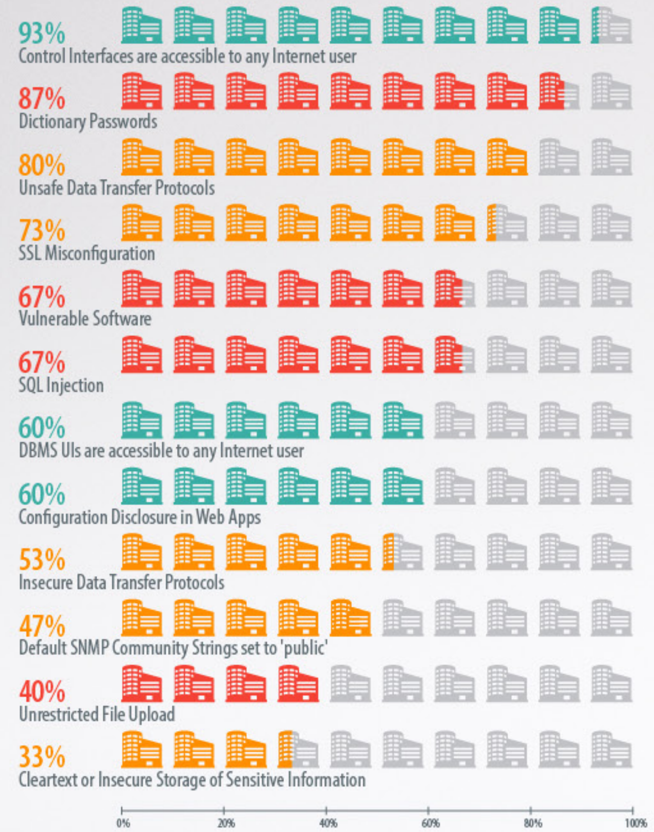
Vulnerabilities related to the availability of the server and network equipment control interfaces from the Internet has increased from 82% to 93% over the last year. There is a significant increase (from 64% to 80%) of systems, whose SNMP service is available at the network perimeter for any Internet user. Administrators often leave default settings of the equipment with the standard values of the SNMP Community String. The default SNMP Community String value with read privileges (public) was detected at the network perimeters of almost the half (47%) of the systems studied, and with write privileges (private) — in one system.

The amount of systems that had equipment control interfaces available from the Internet has slightly decreased: availability via SSH protocols — from 73% to 60% and via Telnet protocols — from 64 to 53%. However, at the same time, the parts of available MySQL and LDAP interfaces have increased (from 27% to 40% and from 18% to 27% respectively). The X11 interface was not explored in 2013, but in 2014 vulnerabilities are present in 20% of systems tested.

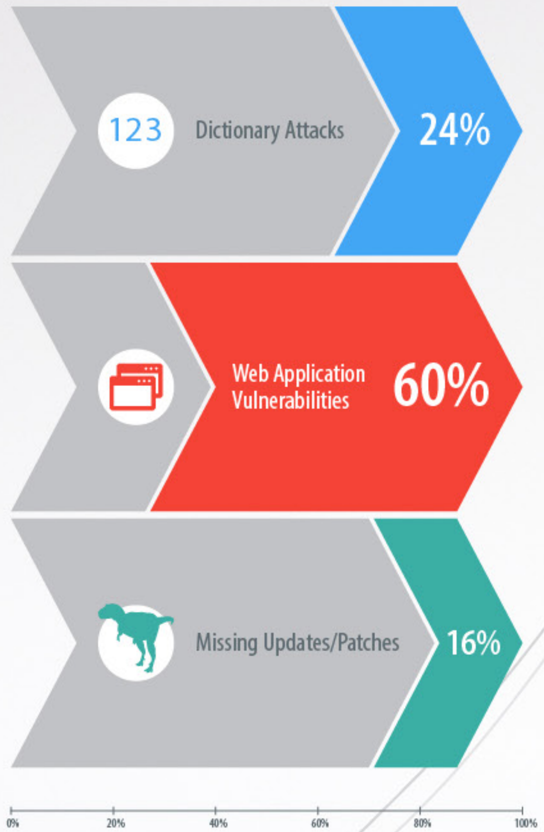
POSITIVE TECHNOLOGIES

VULNERABILITY STATISTICS: ENTERPRISE BUSINESS APPLICATION 2014

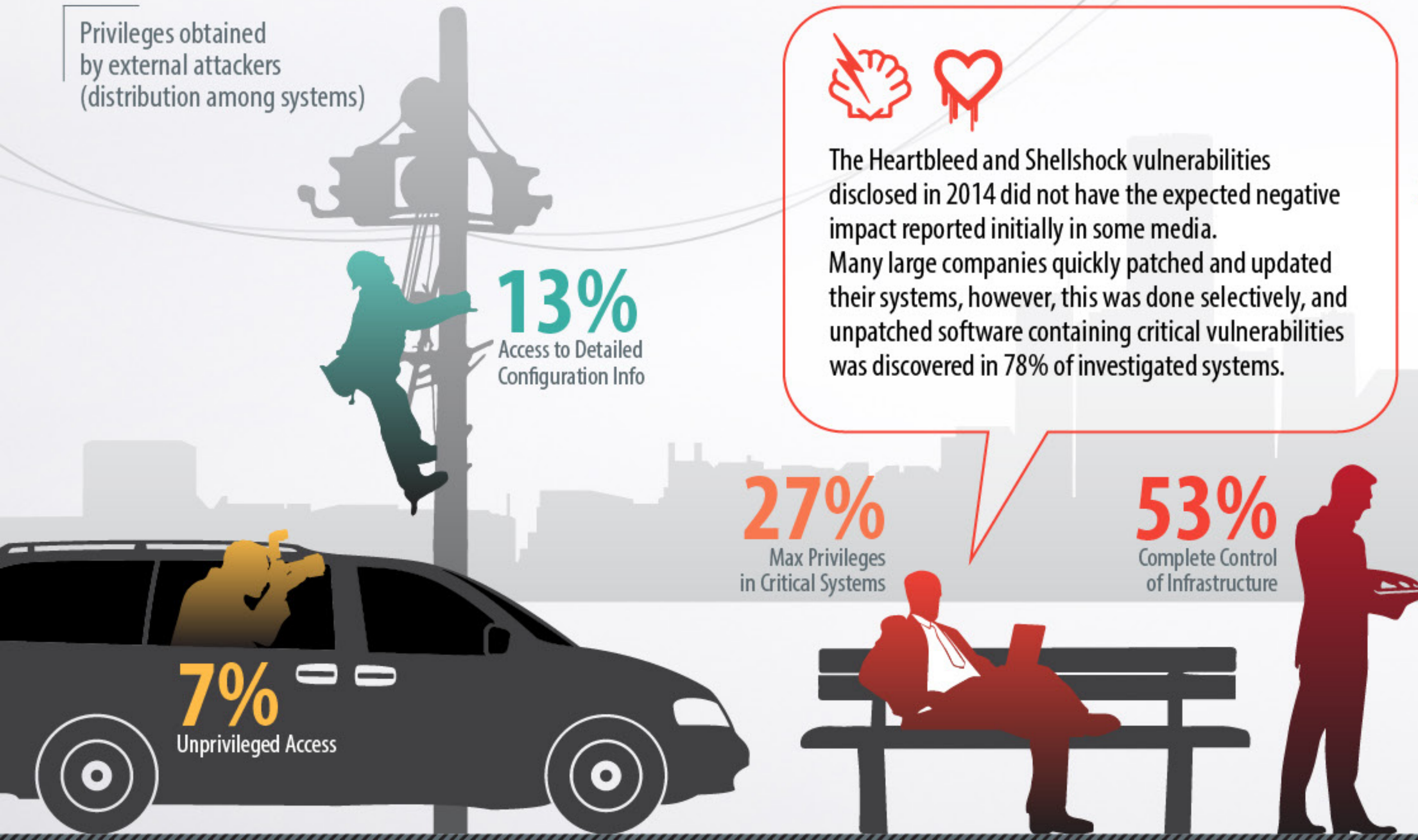
Top Network Vulnerabilities



Access Vectors



Privileges obtained by external attackers (distribution among systems)


13%
Access to Detailed Configuration Info
27%
Max Privileges in Critical Systems
53%
Complete Control of Infrastructure
7%
Unprivileged Access

The Heartbleed and Shellshock vulnerabilities disclosed in 2014 did not have the expected negative impact reported initially in some media.
Many large companies quickly patched and updated their systems, however, this was done selectively, and unpatched software containing critical vulnerabilities was discovered in 78% of investigated systems.

Access Complexity

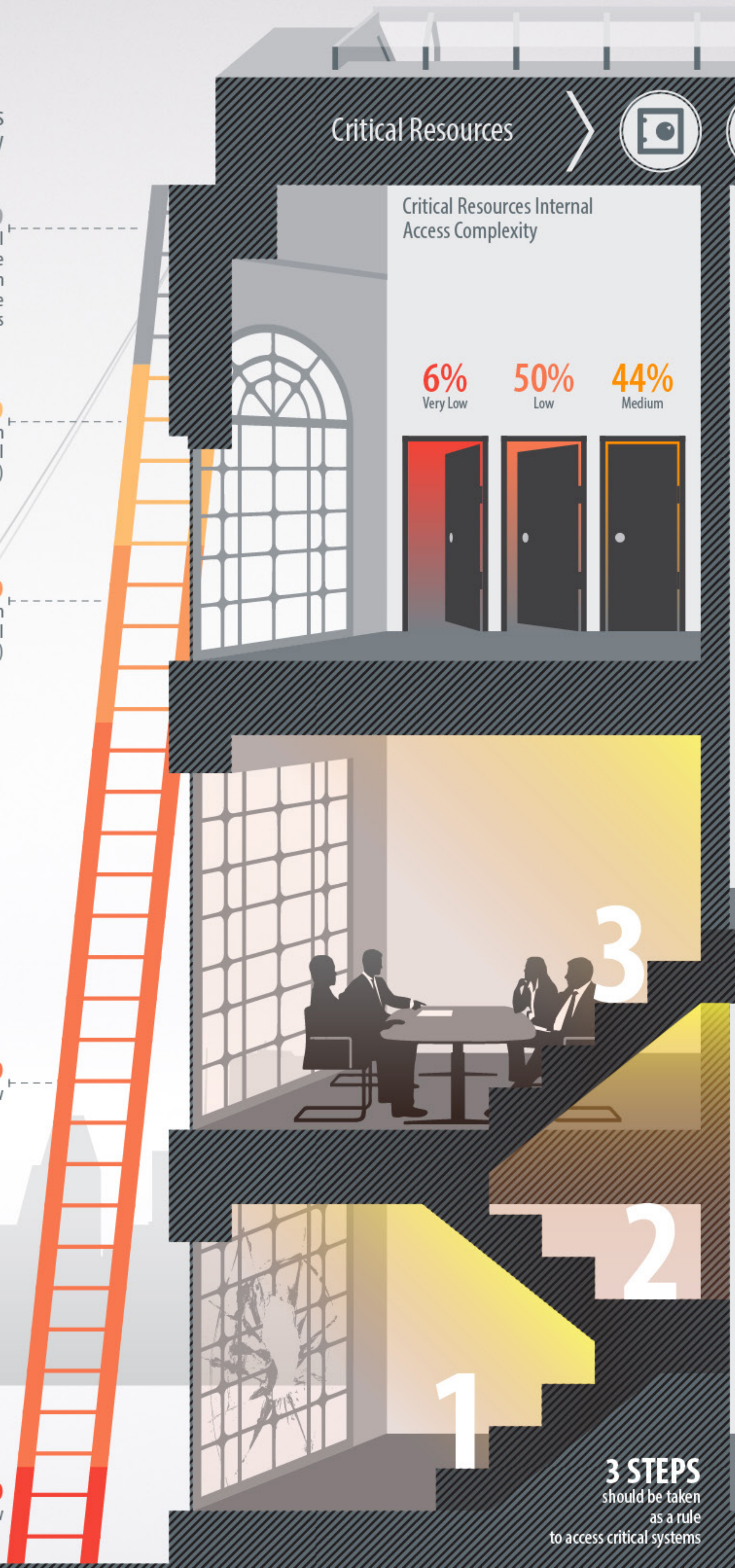
13% Firewall Bypass Failure within Given Scope of Activities

13% Medium (with Social Engineering)

13% Medium (without Social Engineering)

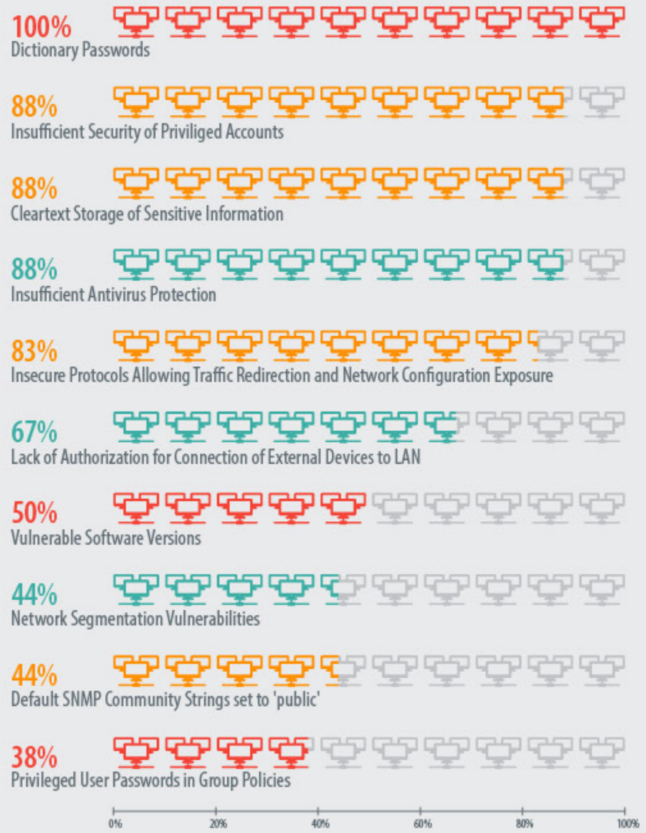
54% Low

7% Very Low

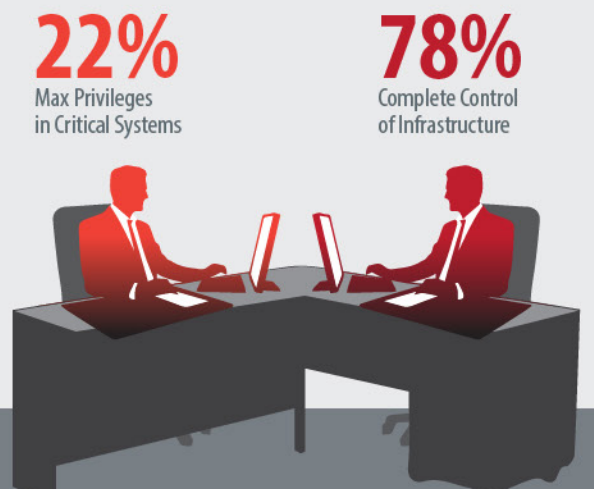


3 STEPS should be taken as a rule to access critical systems

Top Internal Network Vulnerabilities



Privileges obtained by internal attackers (distribution among systems)


22%
Max Privileges in Critical Systems
78%
Complete Control of Infrastructure

4.2.2. Dictionary IDs and Passwords

Penetration testing applies different methods to obtain user passwords including: brute force of default users' (administrator, admin, root) passwords; password brute force for accounts, which names were gained due to previous exploitation of various vulnerabilities; hash brute force; use of encrypted values to retrieve credentials; and other methods. During the analysis of the passwords used, we studied all the passwords obtained through penetration testing. The passwords that could be brute forced via common dictionaries within a short time by an attacker knowing only the user ID were considered dictionary passwords.

Compared to 2013, this vulnerability has dropped to second most common. Other than that shift, the ranking of most vulnerable part of the system has not changed from 2013 to 2014. Dictionary credentials for accessing web applications were the most common vulnerability at the network perimeter that was detected, and found in about 50% of systems. The leader in this category is the "admin" account with the "admin" password. The second most common vulnerability at the external resources in 2014 was dictionary passwords for the Active Directory domain and email, detected in 40% of the systems studied.

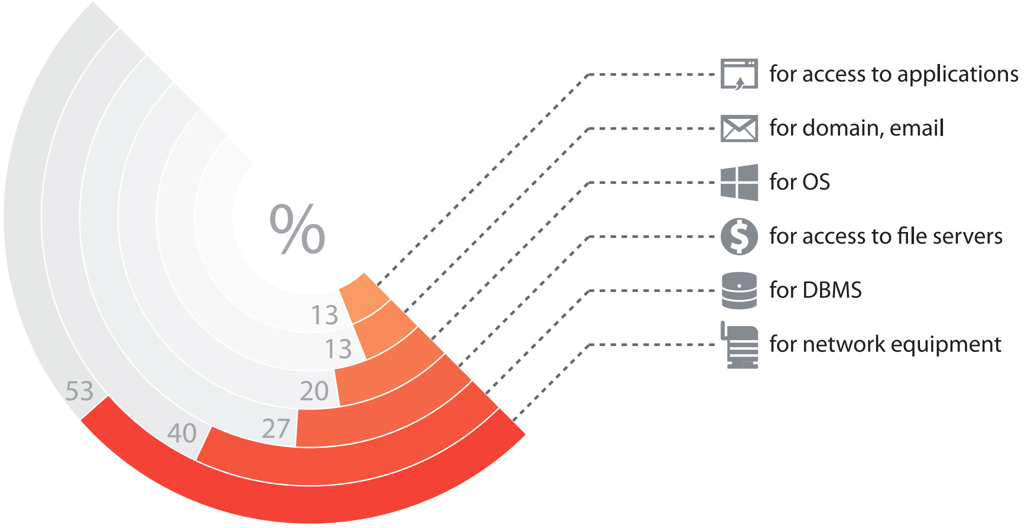


Figure 14. Dictionary passwords at the network perimeter

In 67% of all systems there were dictionary IDs and privileged user passwords detected at the network perimeter. That allowed attackers to access the intranet.

4.2.3. Using Open Protocols

Data transfer via open protocols remains a common vulnerability in corporate information systems and takes the third place among network perimeter vulnerabilities. The part of vulnerable systems remains the same (80%) as compared to 2013. There were a lot of systems with available services (FTP, Telnet) and other open protocols. Exploiting this vulnerability, a potential attacker could intercept information transferred, including credentials of the privileged users.

4.2.4. SSL Configuration Flaws

In 2014, there were many medium-severity vulnerabilities related to SSL configuration flaws. This vulnerability was detected in 73% of systems and was fourth most common. This category includes using self-signed or outdated SSL certificates. Using SSL configuration vulnerabilities, an attacker can conduct a MiTM attack and intercept sensitive data transferred via this protocol.

4.2.5. Lack of Necessary Security Updates

In 2014, the percentage of systems that have a lack of necessary security updates remained the same as in 2013 (67%). Most vulnerabilities of this category were detected at web servers used at the perimeter: 67% of all the organizations studied were vulnerable. In 40% of companies, such vulnerabilities were detected in application software — PHP and OpenSSL. The same percentage of systems had vulnerabilities in outdated versions of various web applications supplied "as is" — content management systems (CMS) and teleconferencing systems. For example, unrestricted file upload in CMS Joomla (CVE-2013-5576) that allows an attacker to upload a command line web interpreter to the server and execute OS command. This vulnerability also allowed our experts to bypass the perimeter of an organization during penetration testing.

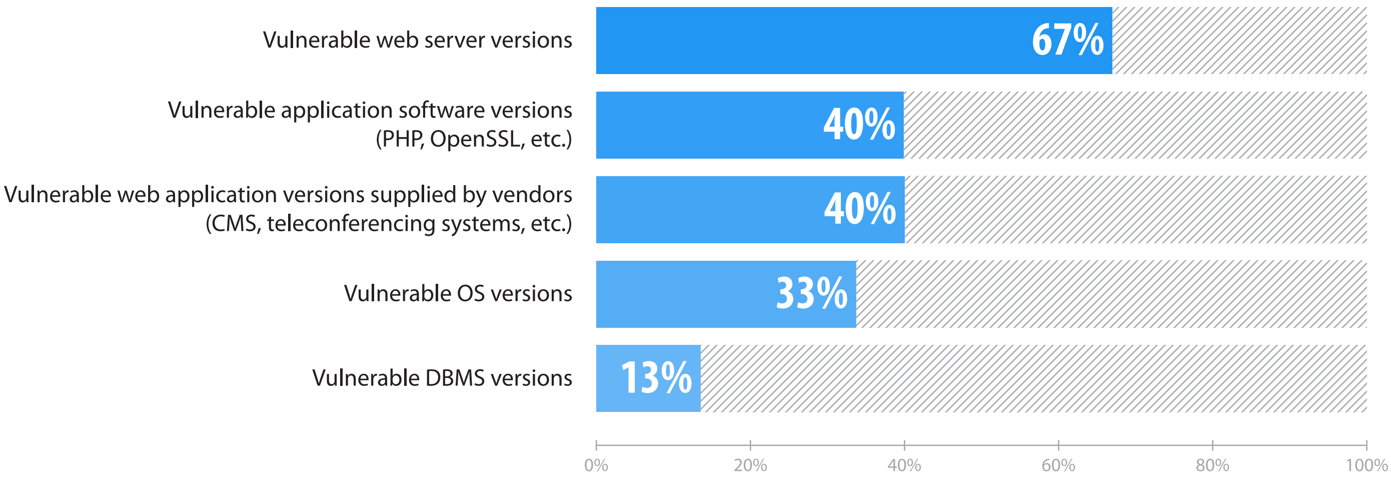


Figure 15. ***Outdated software versions at the system perimeter***

The Heartbleed (CVE-2014-0160) vulnerability (information about it was published in April 2014) allows an attacker to use OpenSSL library errors and obtain sensitive data from the server process memory. After this vulnerability appeared, it was detected in 33% of systems. As of June 2014, there have been almost no vulnerable systems. However, if there was such a vulnerability, it implied serious risks for the system. Thus, there were many company's client credentials obtained intended for accessing an important business application as a result of an attack at one of the projects.

There was also a critical vulnerability — Shellshock (CVE-2014-6271) — announced in 2014, which allowed a remote attacker to use command processing flaws of the Bash interpreter (all the versions before 4.3) and execute arbitrary OS commands, for example, by means of CGI. In fact, during penetration testing this vulnerability was not exploited as Heatbleed was. The vulnerability is dependent on the resource configuration. Most systems were updated so the vulnerability was not found.

4.2.6. SQL Injection

Just as in 2013, the SQL injection vulnerability, a web application code error that allowed unauthorized access to the DBMS bypassing the application logic, was found to be very common and was detected in 67% of organizations. Another critical web application vulnerability — unrestricted file upload — dropped from the 6th to 11th most common problem, but is still quite widespread: 40% of companies are vulnerable.

Overall, the level of web application security continued dropping in 2014 according to the research "Web Application Vulnerability Statistics (2014)" conducted by Positive Technologies.

4.3. Security Analysis of Intranet Resources

After gaining access to the intranet, an external attacker can develop the attack. The simulated external attack gains full control over critical resources in 80% of systems, i.e. in almost all the cases when they managed to penetrate the network perimeter. These results are almost identical to those obtained in 2013.

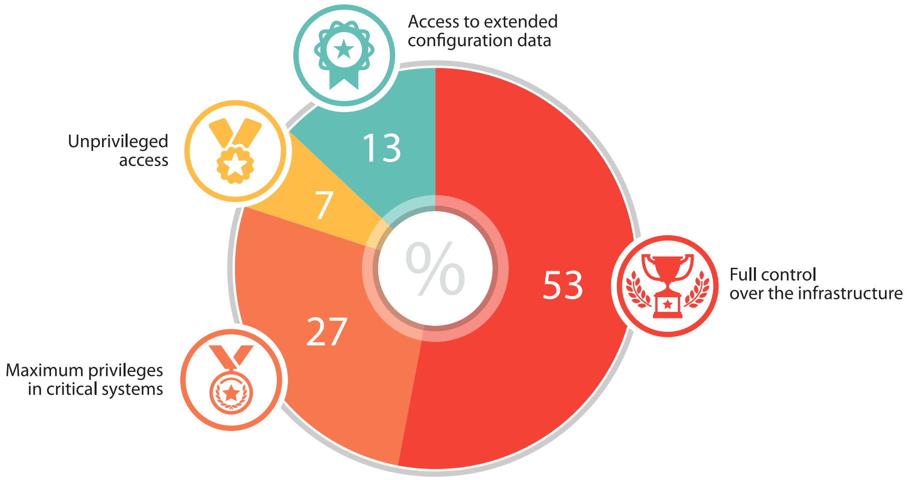


Figure 16. Systems compared by level of privileges obtained on behalf of an external attacker

By contrast, a simulated internal attack (e.g., an employee located in the user segment of the network) resulted in gaining maximum privileges in critical systems (banking systems, ERP systems, and other key network components) in all the cases. Full control over company's infrastructure was gained in 78% of systems, which is also close to the 2013 results.

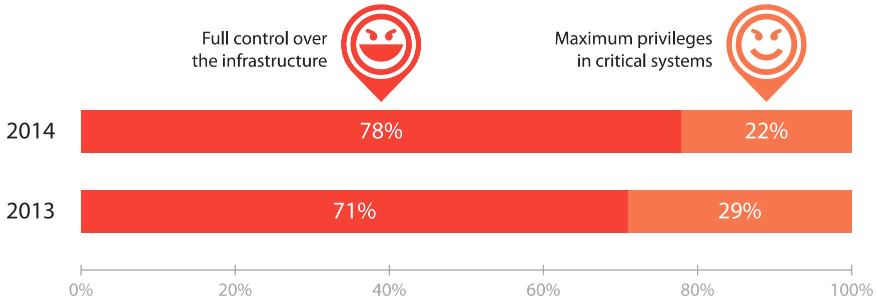


Figure 17. Systems compared by level of privileges obtained on behalf of an internal attacker

It is now easier to gain maximum privileges in a system as a hacker. In 56% of cases, gaining full control over such resources demands little effort from an attacker. The other systems (44%) showed medium difficulty to gain access to critical resources. In 2013, in order to get maximum privileges in 17% of systems, one had to implement complex attack vectors and also use zero-day vulnerabilities, which demands a high attacker qualification.

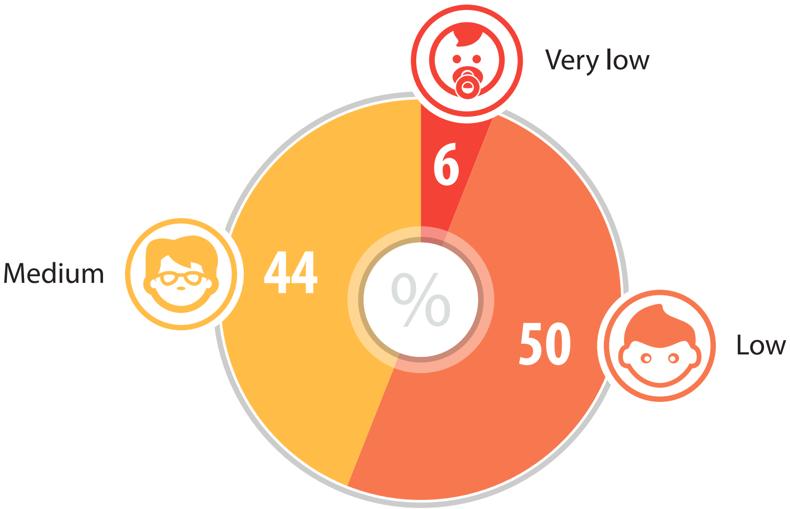


Figure 18. ***Difficulty of gaining access to critical recourses by an internal attacker***

On average, if attackers had access to the intranet, they needed to exploit three different vulnerabilities to obtain control over critical resources. By contrast in 2013, they needed to undertake five steps and seven steps in 2012. In 2014, the longest attack took six stages.

As in 2013, a general intranet attack could be conducted in three steps only:

1. Accessing Active Directory with user rights as a result of credential brute forcing.
2. Obtaining maximum local privileges on user workstations once a local administrator's password was retrieved from group policy settings in the domain controller's shared network directory.
3. Uploading malware on workstations and obtaining credentials of a domain administrator with an active session.

The 2014 research showed that the most typical vulnerabilities were caused by the use of dictionary credentials: all the systems contained dictionary credentials and weak passwords employed by privileged users. Such commonplace security flaws as improper protection of privileged accounts, storage of sensitive data in clear text, and inadequate antivirus protection were discovered in 88% of the systems. In 2014, they were the second, third and fourth most common vulnerabilities respectively.

No service protocol protection and filtering that can lead to traffic redirection and interception or to sensitive data disclosure was detected in 83% of the systems and was the fifth most common LAN vulnerabilities.

The overall results obtained in 2014 demonstrate how the number of vulnerable systems has increased since 2013.

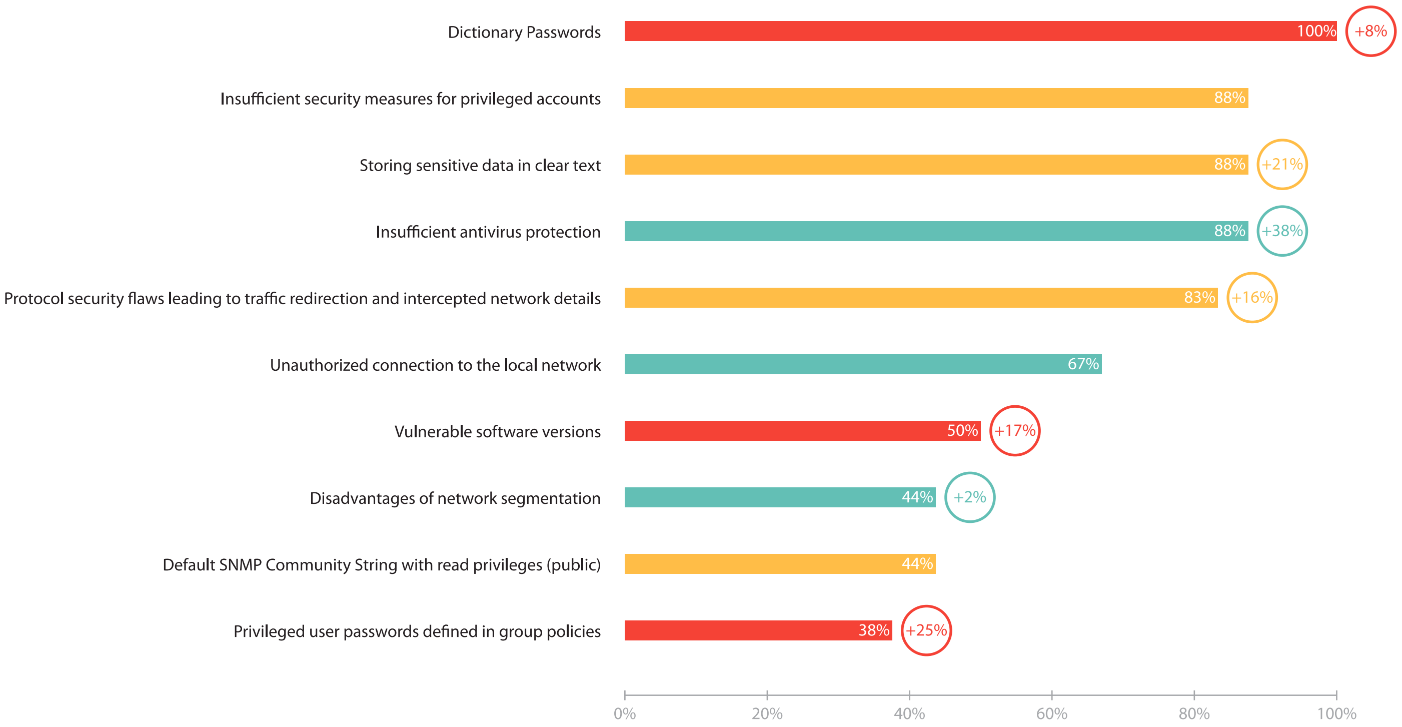


Figure 19. The most common intranet vulnerabilities

4.3.1. Dictionary Passwords

All the systems tested in 2014 used dictionary passwords, also for privileged users, in internal networks. 88% of the systems used dictionary passwords for the Active Directory domain, and 75% of the systems used local accounts to access a variety of operating systems. 38% of companies tested used dictionary passwords to access business critical systems, such as SAP.

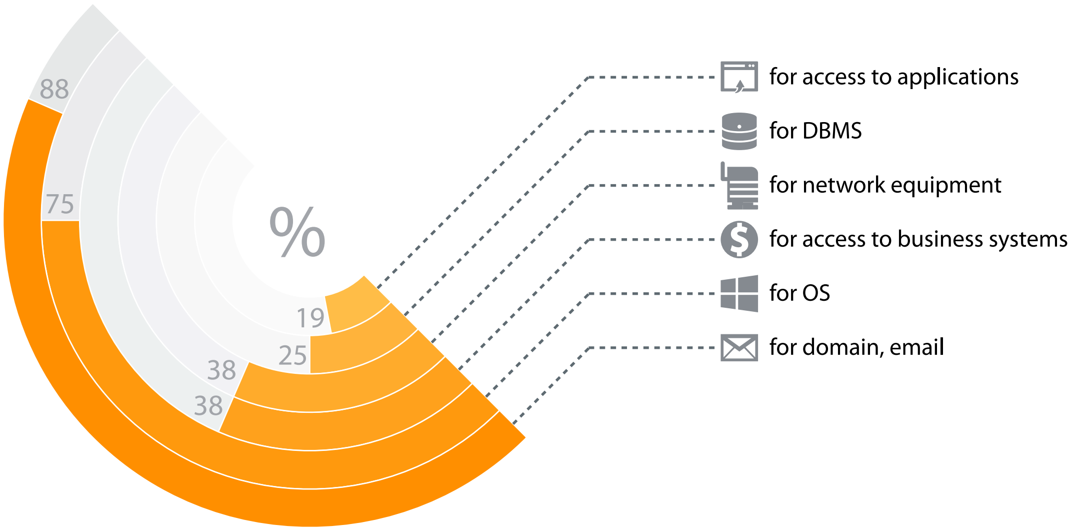


Figure 20. Dictionary passwords in internal networks

Administrators at 56% of systems where weak passwords were detected, used passwords with less than 6 letters; 44% of such systems used "admin" as their password. Privileged users of 38% of systems employed "P@ssw0rd" as their password. These passwords were commonplace in 2013 as well.

In total, 81% of the systems analyzed used numeric passwords up to 10 characters long, and, as in 2013, the "123456" value was the most widely spread (one fourth of all the systems). P@ssw0rd (56%) and passwords comprised of low-case Latin letters only (69%) were popular as well.

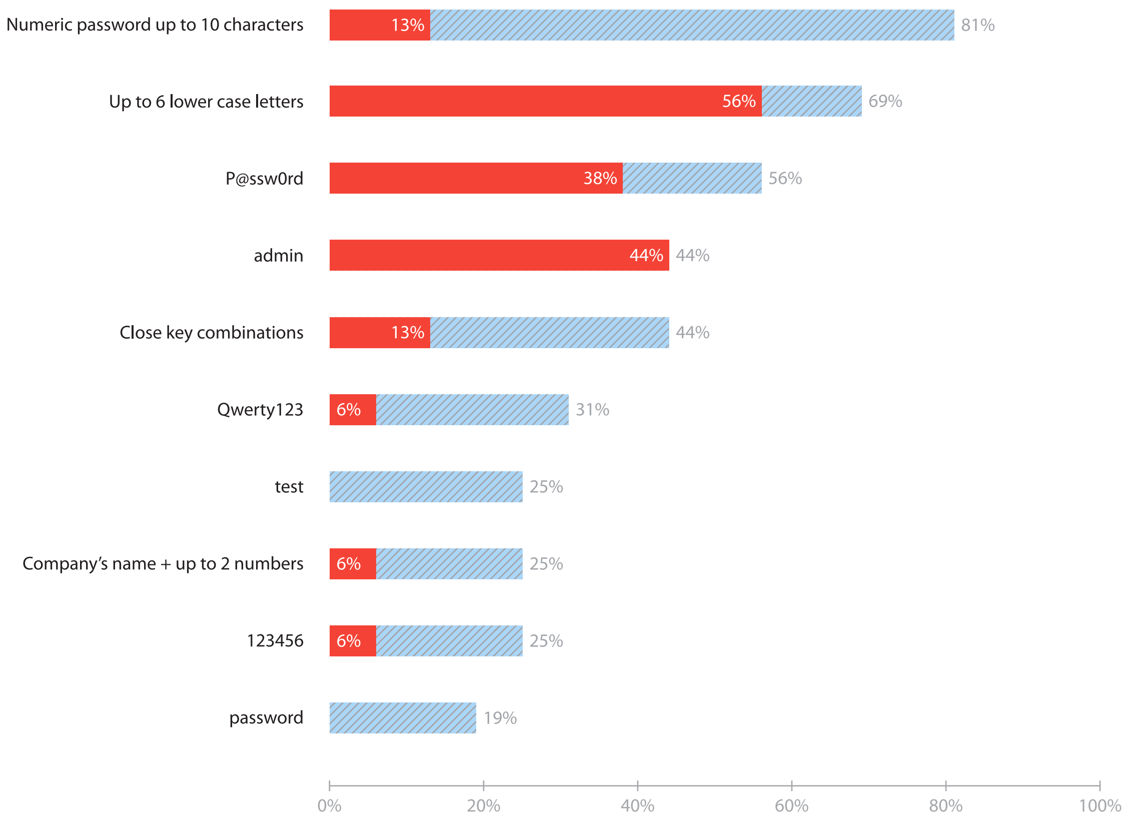


Figure 21. Systems with weak passwords

4.3.2. Insufficient Protection of Privileged Accounts

88% of the systems studied allowed a hacker to leverage weak protection mechanisms for privileged accounts. The root accounts in Linux systems could be accessed remotely, and any user could escalate its privileges up to root without additional authentication.

Active Directory domains did not use two-factor authentication for administrators; therefore, local administrators could retrieve their credentials from the working memory and exploit them to access the domain. As a rule, this flaw is the final attack stage that leads to full control over the Active Directory domain and other critical systems.

Special attention should be given to two-factor authentication for privileged domain users because if high permissions are obtained, hackers can further exploit them to conduct the Kerberos Golden Ticket attack. It allows hackers to access the domain with maximum privileges via Kerberos weaknesses (malicious actions are difficult to detect).

4.3.3. Storing Sensitive Data in Clear Text

As in 2013, storing sensitive data in clear text was another widespread vulnerability of corporate systems (88%). Security analysis conducted by Positive Technologies experts detected numerous systems that stored critical data in clear text: automated scripts with administrators' passwords, network equipment configuration files, text files with passwords to critical resources, users' personal data, and financial information on public resources.

4.3.4. Insufficient Antivirus Protection

88% of the companies studied employed inadequate antivirus protection. This flaw can be exploited by malicious users with admin privileges to run malware on servers and Windows stations. Even if antivirus detected attacks and blocked malware, local administrator privileges allowed disabling the protection system or including this software to the exception list.

In the majority of cases studied in 2014, such actions and insufficient protection of privileged accounts led to disclosure of Windows user credentials, including domain admin credentials.

4.3.5. Service Protocol Security Flaws Exploited to Redirect and Hijack Network Traffic

In 2014, security flaws of such service protocols as ARP, STP, NBNS, LLMNR, etc. were still very common. No ARP Cache Poisoning protection was detected in 83% of the systems tested and no STP filtering — in 42%. Many LANs studied missed protection of such protocols as NBNS and LLMNR, used by default in Windows-based systems (56% and 38% respectively). Attacks on these protocols allowed hijacking password hashes and brute-forcing user passwords.

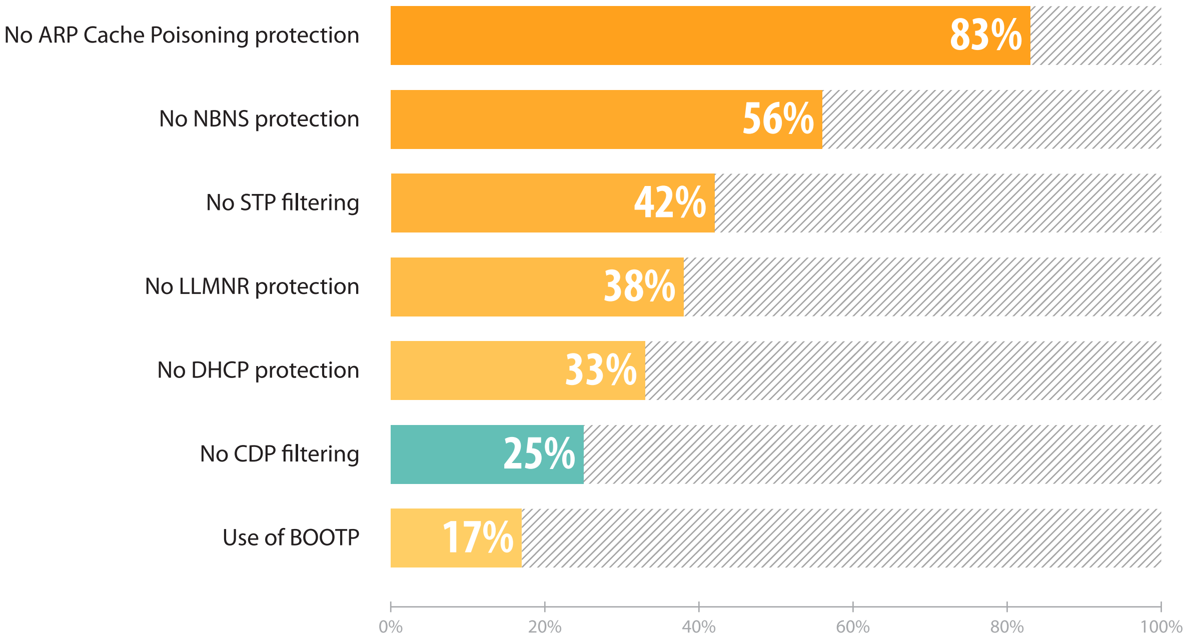


Figure 22. Service Protocol Security Flaws (per system)

If there is no need for specific protocols, it is better to disable them. If their use is required, use preventive security measures.

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, whose vulnerabilities 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, correctly deployed protection tools).

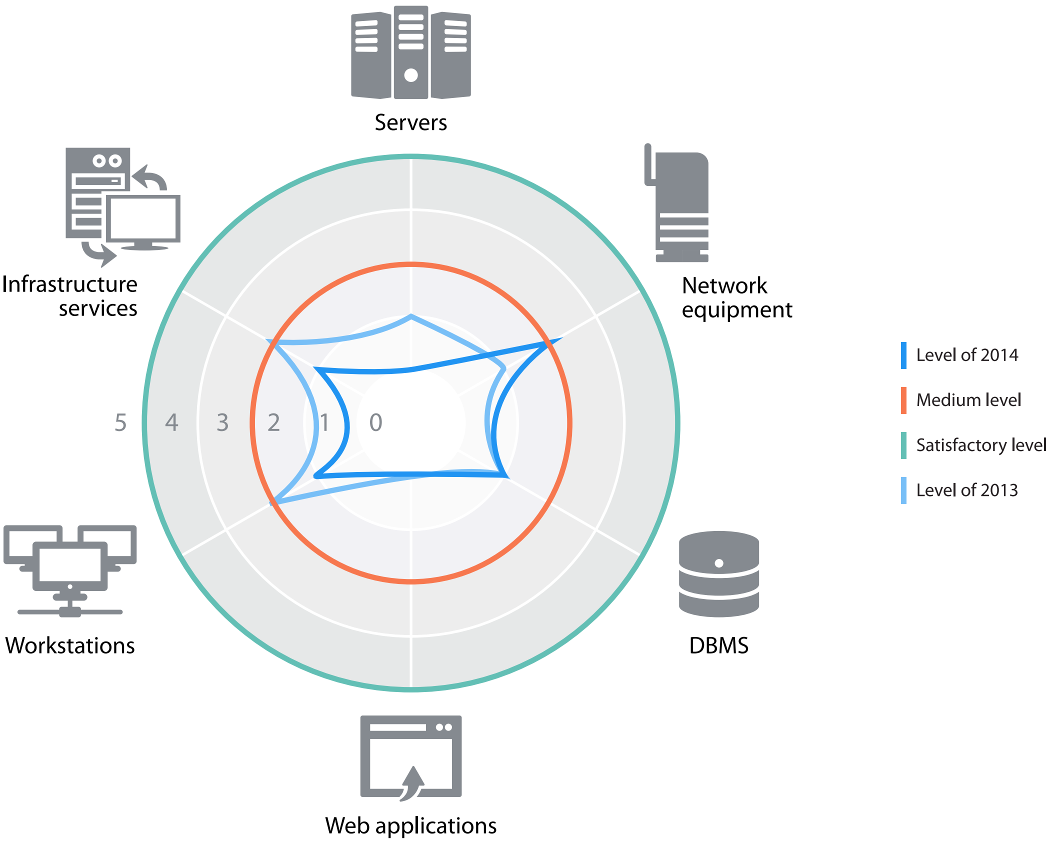


***Figure 23.* General security level of specific system components**

Systems in 2014 appear to have lower levels of security compared to 2013. Apart from the network equipment, whose security level was scored as medium, the security of other spheres either dropped or remained the same.

6. Assessment of Protection Mechanisms

The grade of security for various protection mechanisms used in the majority of the systems have not changed significantly since 2013. Network security has increased to medium. Antivirus protection remained the most correctly implemented security means with a few weak points related to vulnerabilities exploited via privileged users.

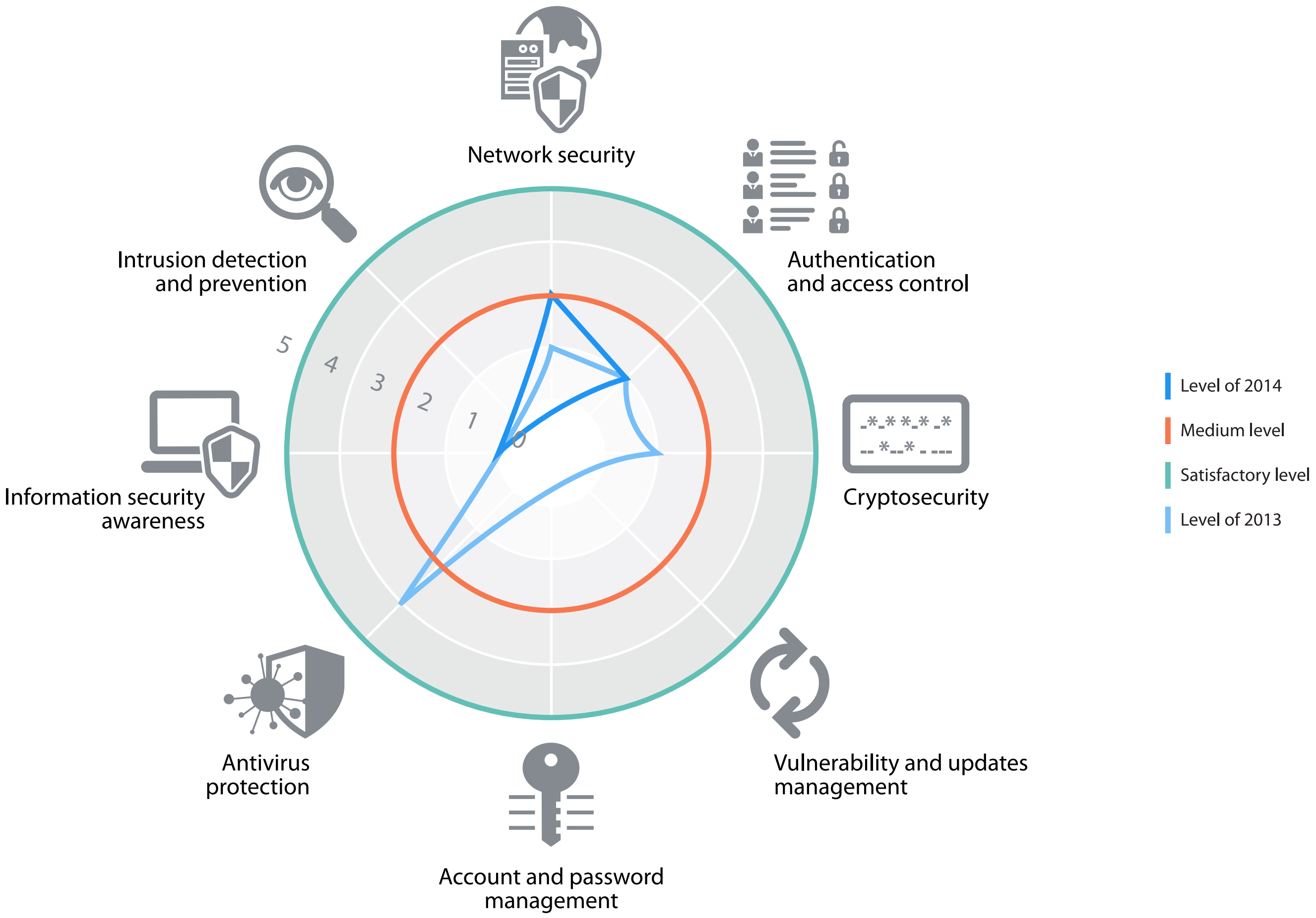


Figure 24. ***General security levels depending on a protection mechanism***

7. Assessment of Information Security Awareness

As part of the penetration testing conducted in 2014, IS awareness checks were carried out among the system users. The checks consisted of a series of hacker attacks agreed upon with the customer and further tracking of staff responses. Penetration testing employed individual techniques and methods, including emails, unified messaging systems, social networks, and telephone conversations. The results were based on the most common hacker method — emailing messages containing an attachment or with a link embedded. The penetration testing monitored the percentage of links opened and files downloaded, as well as the number of credentials entered, to simulate a phishing scam. Messages were emailed on behalf of both a company's employee and unknown individual or organization.

The awareness check was based on Positive Technologies' expert opinion of the results obtained.

As the check showed, staff vigilance about these types of attacks decreased significantly. Half of the companies whose systems were tested showed extremely low awareness level; 17% of the companies tested were estimated as "low" and one third of companies as "below average".

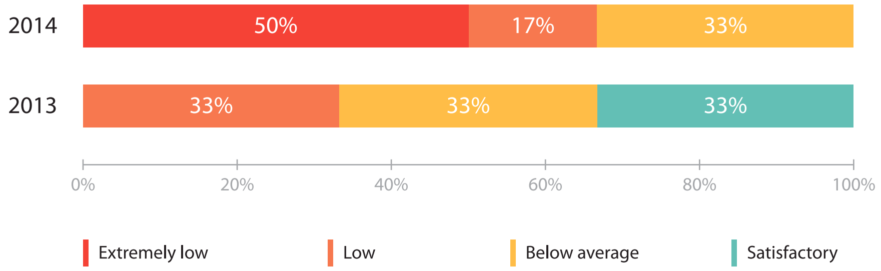


Figure 25. Users' information security awareness

In 2014, the number of users who followed the link, in the simulated phishing scam, increased from 11% to 20% and those who entered credentials in the phishing simulation quadrupled to 15%.

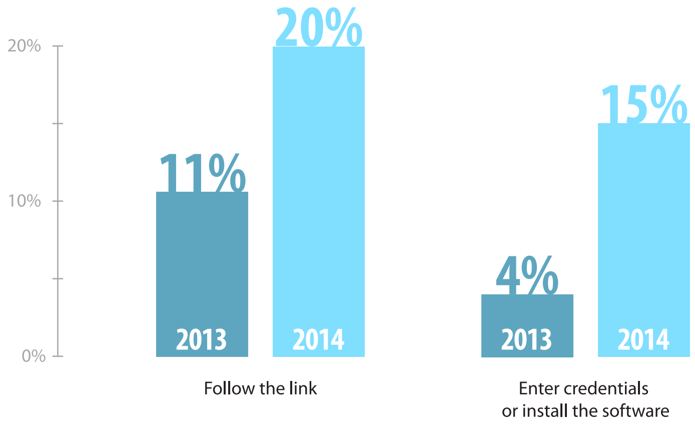


Figure 26. The threat events, total number of messages

8. Conclusion

Information systems of large enterprises did not become less vulnerable to internal and external attacks in 2014. As in 2013, credentials management (a weak password policy in particular) and web applications are the areas most exposed to external attacks. In 2014, the percentage of systems whose network perimeter and critical resources were externally and internally accessible remained the same. However, attack vectors became much simpler than in 2013.

The most commonplace vulnerabilities were availability of server and network hardware control interfaces (SSH, Telnet, RDP) from external networks. The percentage of systems detected to contain dictionary credentials (for privileged users as well) and code flaws was still very high. Maximum severity of detected vulnerabilities caused by web application code flaws.

In 2014, password policy flaws were also typical of intranet resources. The majority of corporate networks studied had antivirus errors and security flaws in privileged accounts protection mechanisms. Very often, sensitive data were stored in clear text; service protocols used to redirect and hijack network traffic remained poorly protected as well.

In 2014, there was decreased awareness among employees regarding security issues, as they were more likely to follow unverified links and open files attached to e-mails from unknown sources. Staff at 67% of companies whose systems were tested showed low or extremely low awareness level.

In the majority of cases, attacks could be conducted via the same vulnerabilities as in 2013. Even if companies quickly fixed the Heartbleed vulnerability, other basic protection means (firewalls, strong passwords, and updates for other system components) were often forgotten.

Accessibility of critical resources argue for the need of improving information security means such as password policies, web application security, regular security updates, and privileged account protection. Regular penetration testing, both internal and external, is also highly recommended.

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

* 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+.