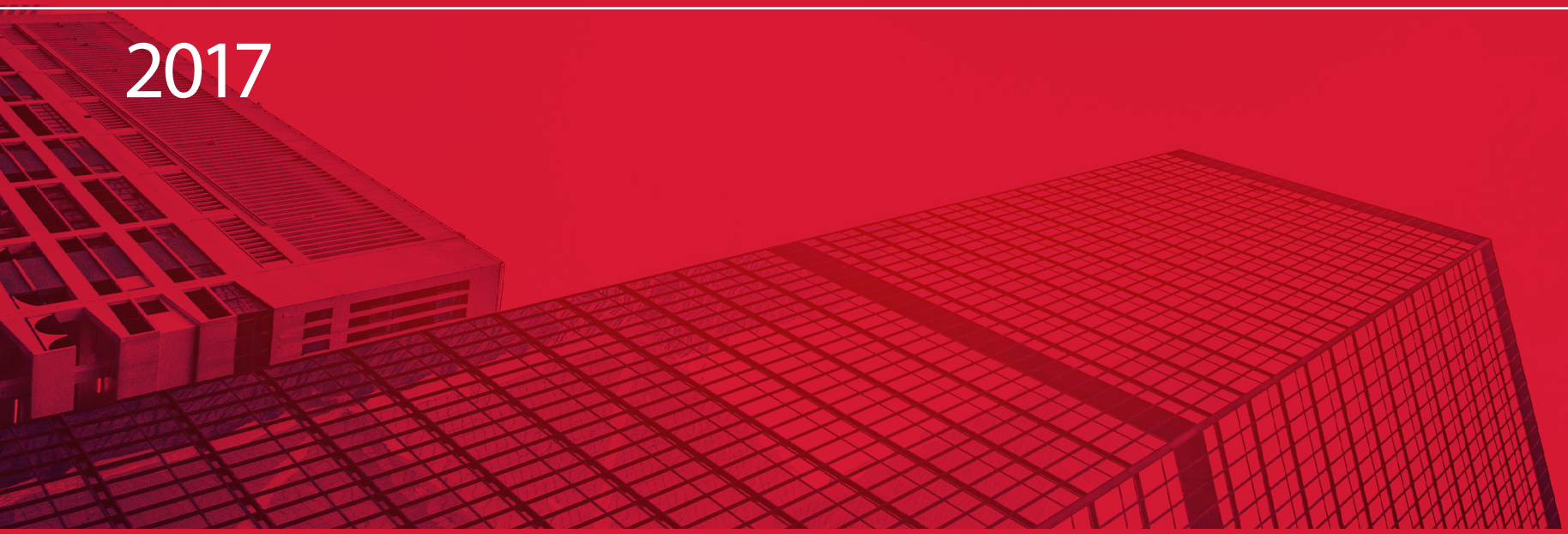
SECURITY TRENDS & VULNERABILITIES REVIEW
CORPORATE INFORMATION SYSTEMS

2017



POSITIVE TECHNOLOGIES

CONTENTS

INTRODUCTION

Information systems at large corporations are like living organisms: they "breathe in" new hosts and systems, grow to accommodate network topology changes, and adapt to new equipment configurations. Ensuring the uninterrupted security of information systems is difficult, with infrastructure scattered across countries and continents, labyrinthine architectures, and a large number of dependencies within and between subsystems.

Here we provide an overview of the most common vulnerabilities detected during security audits by Positive Technologies in 2016. In an audit, our experts simulate how actual attackers (external and internal) would try to penetrate corporate systems. This method identifies a large number of protection flaws, including ones impossible to detect in any other way. Data from the prior year (2015) is provided for comparison. The research reveals the overall protection level of tested systems and the main tendencies, and includes recommendations for improving corporate information system security.

When selecting systems for the final study, the informative value of security assessment results was taken into account. Data gathered during security assessment of a limited number of hosts performed at client request is not included in this report, since such systems are not representative of the overall state of corporate information system security.

1. EXECUTIVE SUMMARY

Critical vulnerabilities were detected on 47% of tested corporate systems.

Bypassing network perimeter is possible on 55% of systems for an intruder with minimum knowledge and skills, and can be done in an average of two steps.

Common perimeter vulnerabilities: dictionary passwords and open data transfer protocols (detected on all systems), vulnerable software versions (91% of systems), and publicly available interfaces for remote access, equipment control, and connection to database management systems (DBMSs, 91%). Although not the largest threat, web application vulnerabilities can be rather dangerous: web application vulnerabilities made it possible to bypass the network perimeter on 77% of systems.

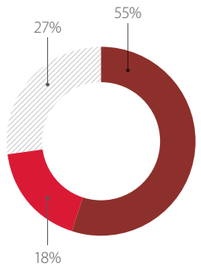
When acting as an external intruder would, our testers could gain **full control over corporate infrastructure** on 55% of systems. As an internal intruder, they were successful on all systems. In 2015, these figures were 28% and 82%, respectively.

Most common internal network vulnerabilities: flaws in network layer and data link layer protocols leading to traffic redirection and interception of information about network configuration (100% of systems).

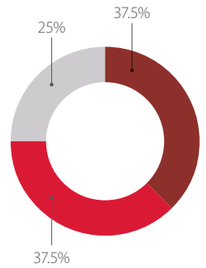
Staff awareness of information security is very low at half of client companies (compared to 25% of systems in 2015).

Wireless network security was extremely poor in 75% of cases. Each second system allowed access to the corporate LAN from a wireless network.

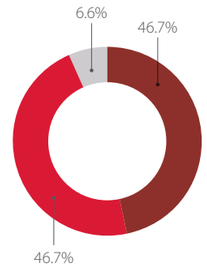
Most often an external intruder needs just **two steps** to penetrate the perimeter.



Difficulty of bypassing the perimeter (percentage of systems)

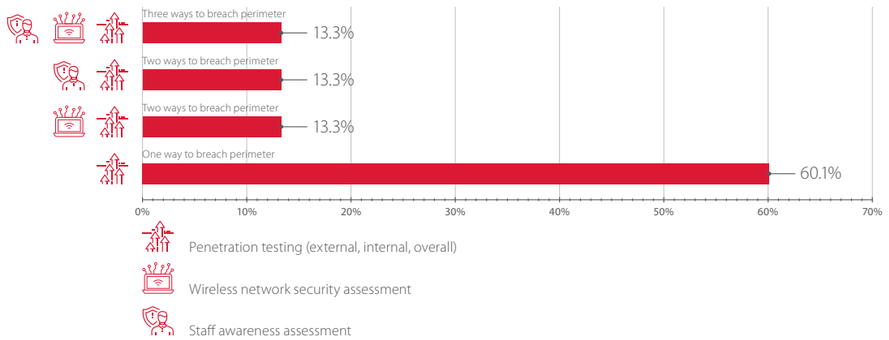


Difficulty of perimeter penetration (percentage of systems)



Maximum severity level of detected vulnerabilities (percentage of systems)

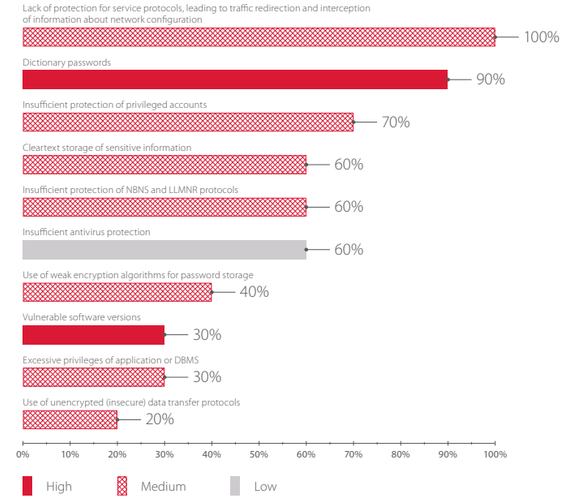
In 2016, almost **half** of tested corporate systems **contained critical vulnerabilities**, based on Common Vulnerability Scoring System (CVSS) v3.0 metrics.



Corporate information system security assessment

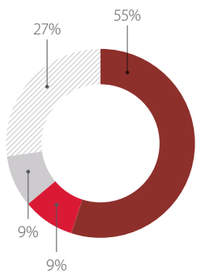
7 out of 10 common network perimeter vulnerabilities were critical.

Company local area network

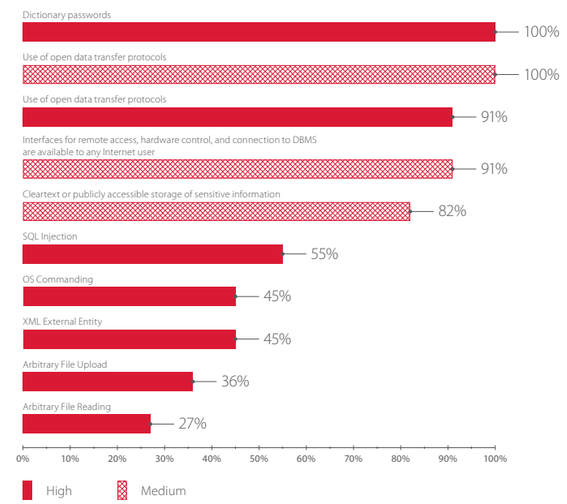


Most common intranet vulnerabilities (percentage of systems)

100% of tests performed as an internal intruder led to obtaining **full control** over corporate information infrastructure and critical resources.



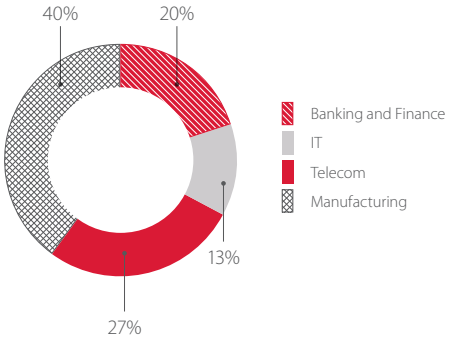
Privileges gained acting as external attacker (percentage of systems)



Most common vulnerabilities on the network perimeter (percentage of systems)

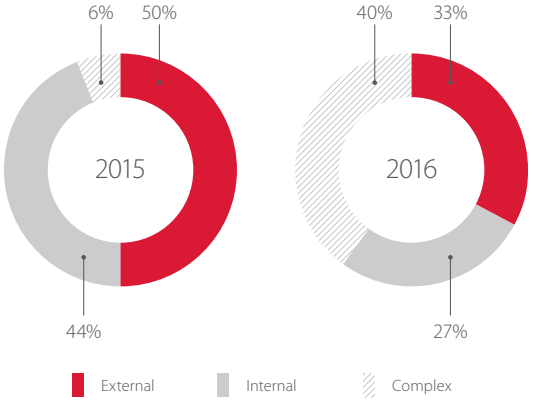
2. RESEARCH DATA

The 2016 data includes the results of security audits of 15 information systems belonging to companies in various industries. Analysis was performed for large manufacturing companies, some of which are state-owned, banks and financial institutions, telecommunications providers, and IT companies.



Sectors of tested sytems (percentage of systems)

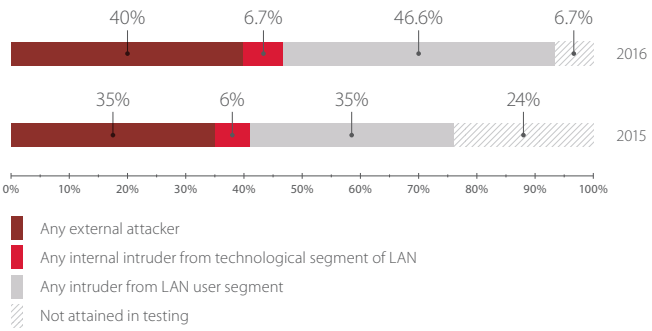
In addition to external, internal, and complex penetration testing, some companies requested assessment of staff security awareness and wireless network (Wi-Fi) security. Complex penetration testing services saw increased demand in 2016.



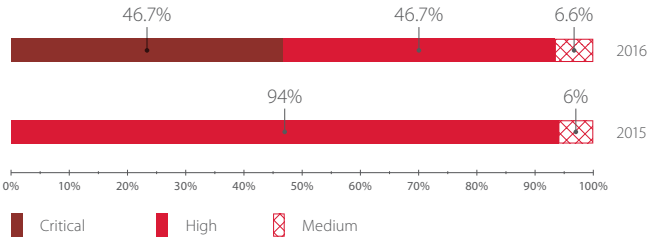
Types of penetration testing (percentage of systems)

3. STATISTICS FOR 2016 IN COMPARISON TO 2015

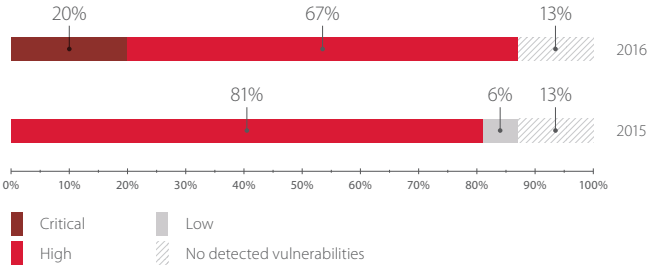
3.1. Overall penetration testing results



Minimum access level an intruder needs for full control over certain critical resources (percentage of systems)

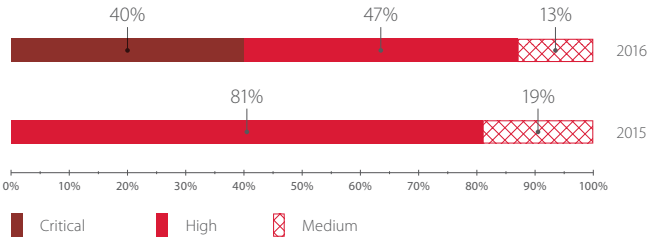


Maximum risk level of detected vulnerabilities (percentage of systems)



Maximum risk level of vulnerabilities related to lack of security updates (percentage of systems)

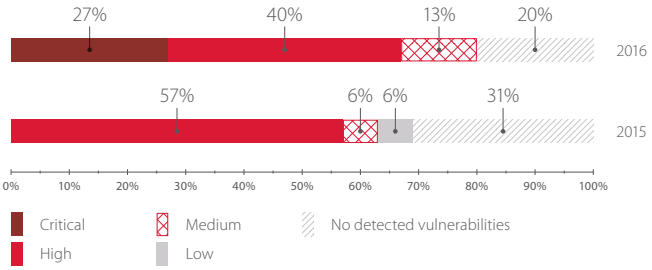
All tested corporate systems could contain vulnerabilities related to web application code errors or lack of security updates. But since penetration testing is performed via the black-box method, such vulnerabilities could not be detected.



Maximum risk level of vulnerabilities related to misconfigurations (percentage of systems)

Interesting fact

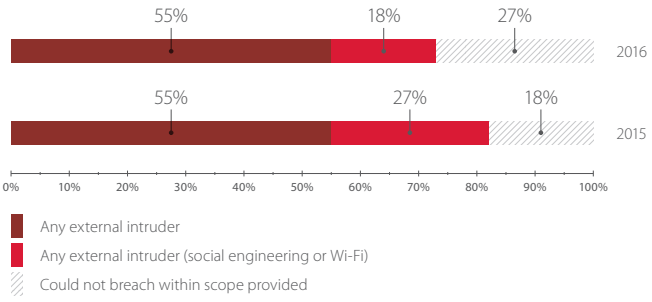
The average age of the oldest uninstalled updates on systems with such vulnerabilities is 108 months (9 years). The oldest vulnerability we found (CVE-1999-0024) **was published more than 17 years ago** and relates to DNS server support for recursive queries. A malicious user could exploit this vulnerability to conduct DoS attacks.



Maximum risk level of vulnerabilities related to web application code errors (percentage of systems)

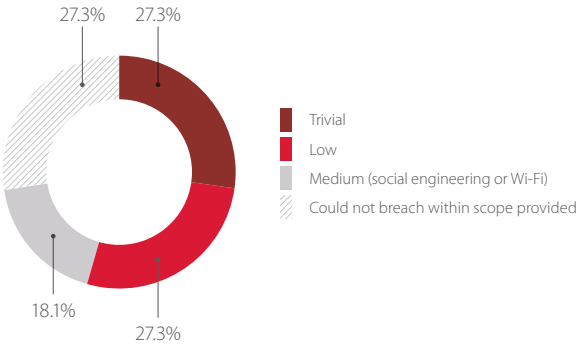
3.2. Security analysis of the network perimeter

The trend towards increased network perimeter security continued in 2016. In 27% of audits, Positive Technologies was unable to penetrate the network perimeter and obtain unauthorized access to LAN resources. This can be explained by the fact that some customers perform regular penetration testing and eliminate the vulnerabilities found. However, we should keep in mind that network infrastructure configuration changes constantly, and that is why penetration testing should be performed on a regular basis. Moreover, it is necessary to continuously monitor services that are available from the Internet. At any time, whether by mistake or lack of competence in information security, an administrator can open a "dangerous" network port on the perimeter and expose the network to threats.



Minimum level of an attacker's qualification required to penetrate network perimeter (percentage of systems)

Less effort was required than in 2015 to penetrate the perimeter. In almost 55% of cases (compared to 46% in 2015), an external attacker with minimum knowledge or skills could penetrate the perimeter and access LAN resources. As in previous years, breaching the network perimeter requires exploiting an average of two vulnerabilities.



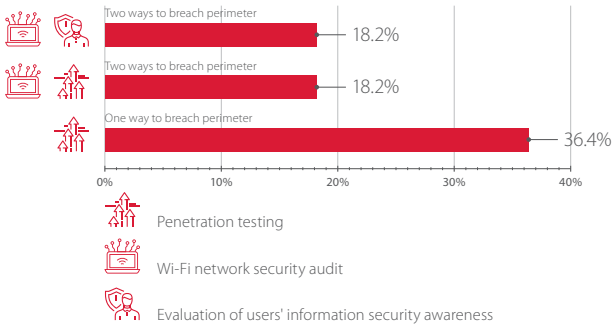
Difficulty of perimeter penetration (percentage of systems)

Examples of penetrating the perimeter and accessing LAN resources

Trivial difficulty of perimeter penetration	JDWP is available on the network perimeter. Any intruder can use a publicly available exploit (github.com/IOActive/jdwp-shellifier) to execute arbitrary commands on the server. By using this vulnerability and excessive privileges of the service, Positive Technologies testers gained full control over the server and obtained access to the LAN (an internal network interface was available on a host).
Low difficulty of perimeter penetration	A web application for managing the client's employee training was identified on a tested host. By registering a new account without confirming identity, testers could access web application functionality and upload a web command-line interpreter (web shell) to the server, which made it possible to execute arbitrary OS commands on the server with the privileges of the web application. As a result, Positive Technologies testers could access the LAN, because an internal network interface was available on a host.
Medium difficulty of perimeter penetration	**Example 1.** By using a known vulnerability in Adminer, it was possible to read local files on a host and find a configuration file with an account for accessing a database. In the database, testers found a table with more than 400 user accounts and hash of their passwords. By using one of these accounts (the account password was derived from its hash), they obtained access to the web application on the attacked resource. The web application's functionality allowed uploading a web command-line interpreter to the server and executing OS commands. The attack led to obtaining access to the LAN (an internal network interface was available on a host). **Example 2.** As part of assessing the information security awareness of employees, a mass mailing was made, encouraging employees to visit a site and enter their user name and password. Some employees entered their credentials in the fake authentication form. Such credentials can be used for unauthorized access to system resources. The minimum needed for performing phishing attacks is to register a domain and create a fake authentication form. Moreover, intruders need to make the phishing site replicate the design of the page that the employee is used to seeing. To do this, an intruder needs to conduct additional reconnaissance, which significantly increases the complexity of the attack.

Penetration testing revealed an average of two attack vectors per system leading to unauthorized access to LAN resources. On one system, five such attack vectors were detected.

Although an attacker needs only one way to penetrate the network perimeter and gain LAN access, in some cases multiple ways were found: standard penetration testing, social engineering, and via wireless networks.

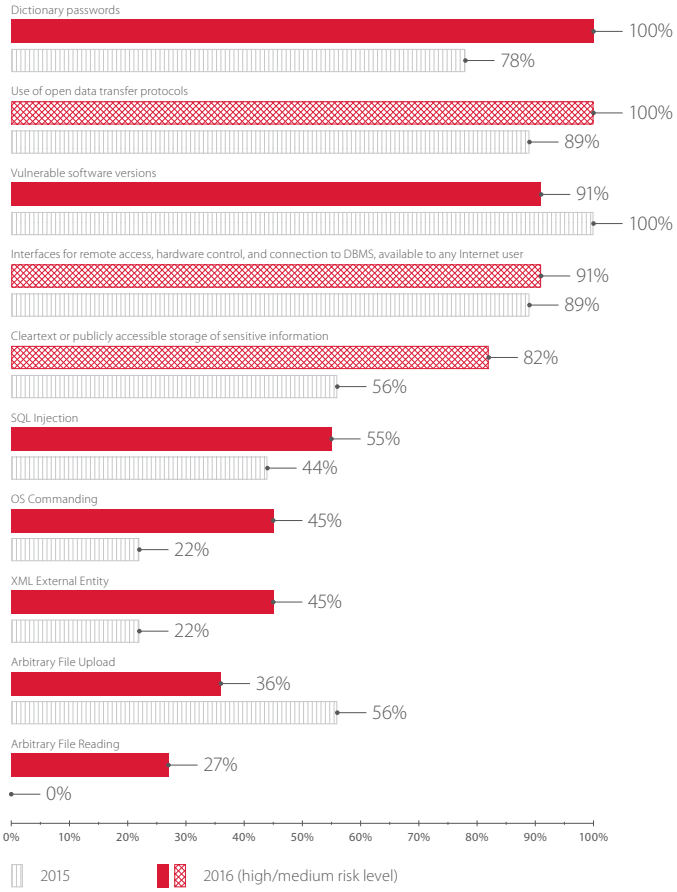


Perimeter penetration (percentage of audits)

In 77% of cases, penetration of the network perimeter was successful due to vulnerabilities in web applications, and in 23% of cases due to easily guessable dictionary passwords.

Interesting fact

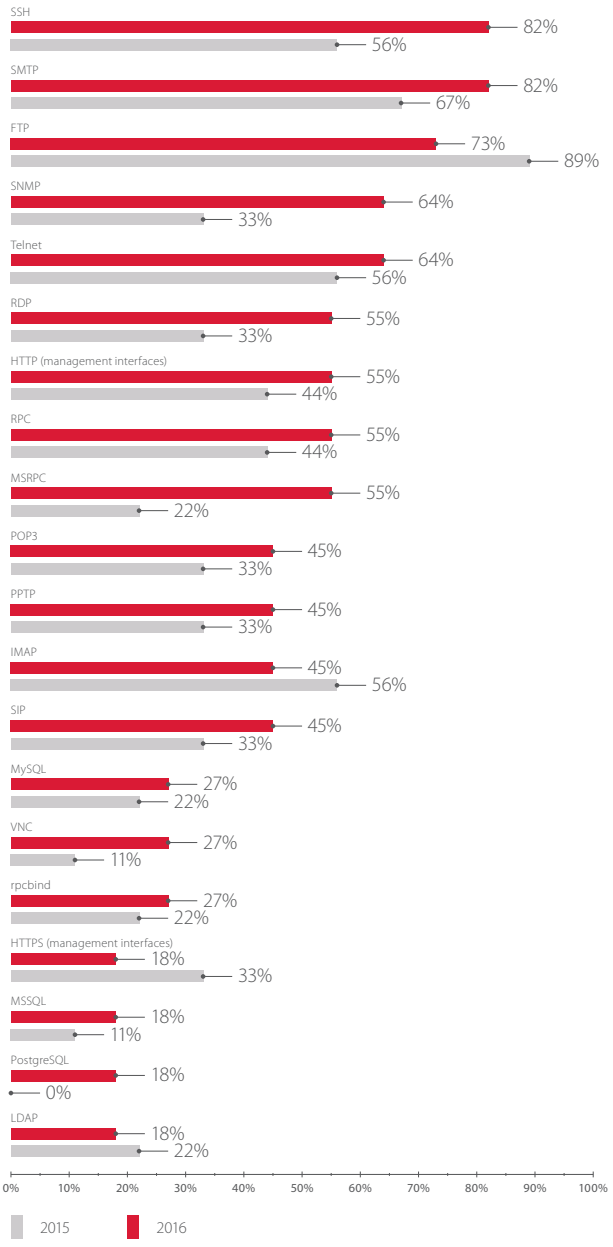
In several cases, **our team detected unauthorized web command-line interpreters** on web application servers, suggesting previous successful attacks. The attackers apparently had been able to conduct attacks on LAN resources for several months, since these web-based interpreters were revealed only during our security audit.



Most common vulnerabilities on the network perimeter (percentage of systems)

Interesting fact

In 2016, one of our tests of a corporate information system revealed not only web command-line interpreters on external-facing resources, but also **five vectors of attack** that allowed a minimally skilled external attacker to breach the network perimeter and gain access to LAN resources.



Protocols used on the network perimeter (percentage of systems)

The top five network perimeter vulnerabilities are very similar to those found last year. Penetration testing revealed dictionary passwords[1] and open data transfer protocols on all systems. Almost all systems had components with out-of-date software. Our experts scanned network perimeter hosts and in 91% of cases discovered remote access, hardware control, and DBMS connection interfaces that any Internet user can access. The number of systems with cleartext storage

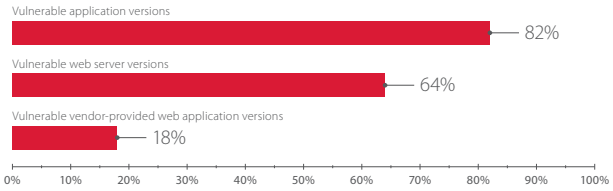
1 Detailed statistics on vulnerabilities associated with use of dictionary passwords, including on the network perimeter, can be found in section 7 of this report.

of sensitive data, or with public access to such data, also increased. Numbers five through ten in the vulnerability list involve mistakes and flaws in web application code. The overall level of web application security is still low, as confirmed in the Positive Technologies report "Security trends & vulnerabilities review. Web applications."[2]

Flaws in corporate systems related to use of open data transfer protocols weigh in at number 2 in our list. FTP, Telnet, and HTTP are widely used to access management interfaces. Due to the lack of data protection, an intruder is able to intercept sensitive information, including the credentials of privileged users.

The problem of availability from external networks of interfaces for remote access, hardware control, and DBMS connection is still relevant and is one of the five most common shortcomings in 2016.

As compared to 2015, use of outdated software versions on network perimeter hosts fell by 9%. This improvement occurred despite an increase in the percentage of systems using outdated application versions.

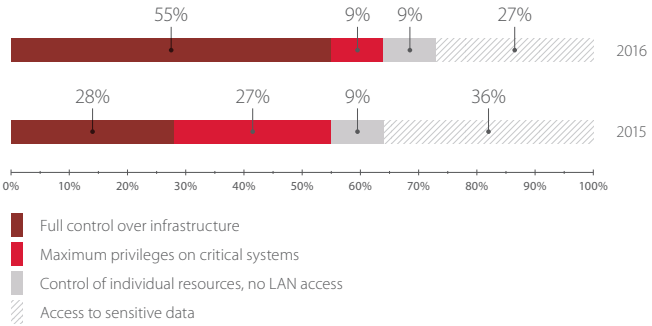


Vulnerable software versions on the network perimeter (percentage of systems)

An interesting tendency is that the number of vulnerabilities with use of excessive application or DBMS privileges fell from 33% in 2015 to 18% in 2016. This is mostly attributable to the fact that newer versions of Microsoft SQL Server do not receive maximum OS privileges by default. Previously, an attacker who bruteforced a Microsoft SQL Server account immediately gained total control over the server unless the administrator manually restricted these privileges. In newer versions, this vulnerability has been tackled by restricting the DBMS account privileges by default. However, even these restrictions sometimes fail to ensure sufficient protection. More detailed examples of privilege elevation with Microsoft SQL Server are given in "Corporate information system penetration testing: attack scenarios."[3]

3.3. Security analysis of intranet resources

After gaining access to the internal network, an external attacker can obtain full control over the whole IT infrastructure or individual critical systems. On more than half of the tested systems, our testers gained control over critical resources (Active Directory, DBMS, or ERP system). 55% of tests resulted in full control over the entire corporate infrastructure, a percentage that almost doubled compared to 2015.

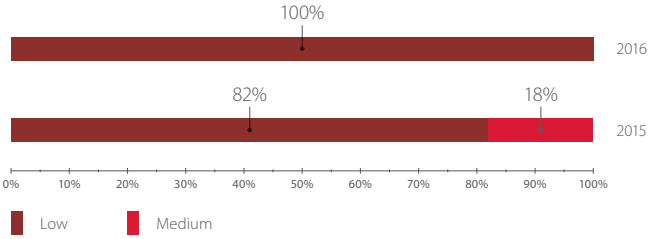


Level of privileges gained by an external attacker (percentage of systems)

2 www.ptsecurity.com/ww-en/analytics/
3 www.ptsecurity.com/upload/corporate/ww-en/analytics/Corp-PenTests-eng.pdf

The insider threat remains real: acting as an employee, for instance, our testers had a 100-percent success rate at gaining full control over the entire infrastructure in 2016 (as compared to 82% in 2015).

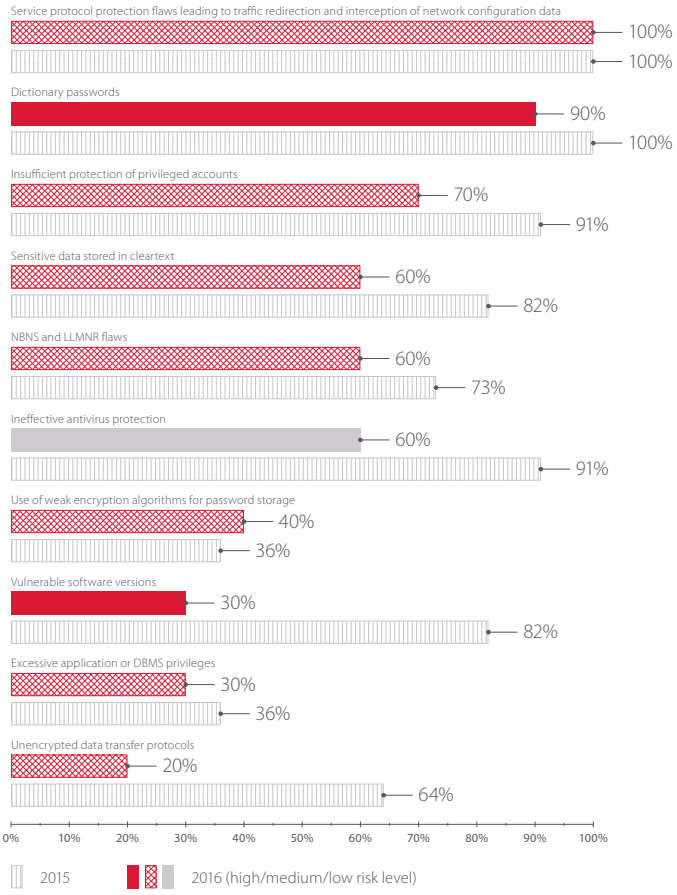
We saw a significant fall in the level of sophistication that an internal attacker would need to access critical resources.



Difficulty of accessing critical resources by an internal attacker (percentage of systems)

To gain maximum privileges on critical systems, in most cases it is enough for a malicious user to bruteforce a local administrator's account on a workstation or LAN server, launch special software, and obtain local administrator accounts for other workstations or servers in cleartext. This attack vector can be subsequently parlayed into domain administrator credentials.

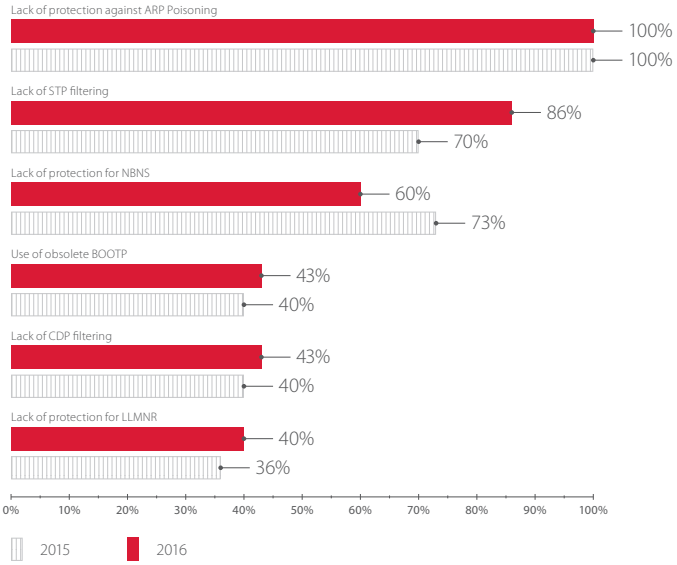
In some cases, just two steps were enough for an insider to get access to critical systems. The first step involved escalating OS privileges to the maximum possible using a published OS vulnerability (CVE-2015-1701) and a publicly available exploit. Then the experts analyzed log files on the server and bruteforced accounts to gain access to a critical system.



Most common intranet vulnerabilities (percentage of systems)

The most common vulnerabilities are security flaws in network layer and data link layer protocols, which may lead to traffic redirection and interception of network configuration data. Every system contained vulnerabilities related to protocol use (ARP, STP, BOOTP, CDP).

Each analysis of LAN traffic revealed a lack of protection against ARP Cache Poisoning, which may be used for traffic sniffing and performing a man-in-the-middle (MITM) attack. If this attack is successful, an intruder can capture confidential information, modify data in transit, and block network connectivity.



Security flaws in service protocols (percentage of systems)

Dictionary passwords fell to second place in the list, having declined by 10% as compared to 2015. But administrators, just like regular users, can be lazy when choosing passwords: all the systems that used dictionary passwords had them also for privileged accounts.

A positive trend in 2016 is a 21-percent reduction in insufficient protection of privileged accounts. Broader use of two-factor authentication for privileged domain accounts and the accounts of key administrators played a role in this. However, we could bypass this authentication in many cases during security analysis. For example, during one intranet penetration test, our testers took advantage of vulnerabilities in the Windows implementation of two-factor authentication with smart cards.

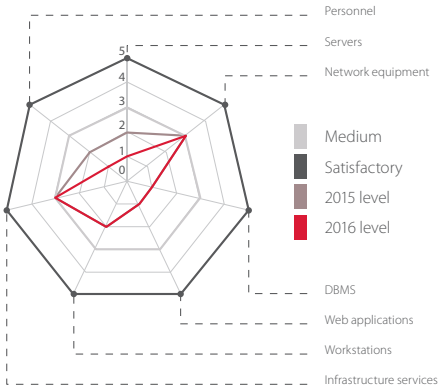
Interesting fact

Two-factor authentication requires that the user should not only know something (for example, a PIN or password), but also have something (most often, a smart card with a certificate installed). When a smart card authentication attribute is set in the domain account configuration, an NT-hash is assigned to the account. The hash value is calculated randomly and invariably during all subsequent connections to the domain's resources. The vulnerability allows an attacker to get the NT-hash assigned to the user by the domain controller and use it when authenticating with the pass-the-hash method. Thus, an attacker no longer needs to have a smart card and know its PIN, and is able to attack domain resources with the privileges of a compromised account for an unlimited period of time.

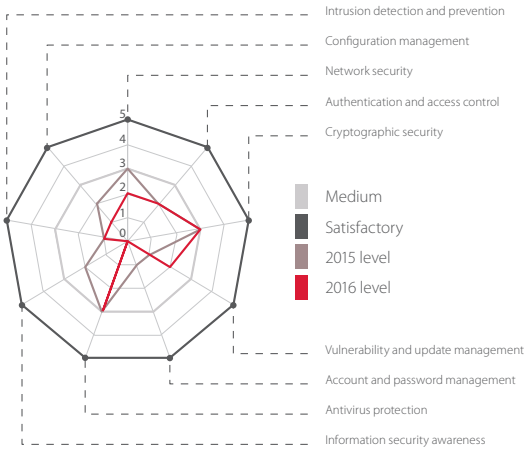
4. SECURITY ASSESSMENT

Attack vectors were classified according to the system components whose vulnerabilities allowed unauthorized access to resources.

Mechanisms were classified according to the security flaws exploited in penetration testing.



System protection: attack vectors



System protection: effectiveness of protection mechanisms

Note

The score 0 on the diagram corresponds to an extremely low level, while 5 corresponds to a satisfactory level of security.

The overall security level decreased compared to 2015 due to changes in awareness of information security and the level of server equipment security from "below average" to "low." The level of security of DBMS and web applications is still low. Effectiveness of protection mechanisms also decreased with regard to four different vectors. At the same time, an increase in the effectiveness of security mechanisms was found only for "vulnerability and update management." The security level of any one component, as well as the effectiveness of protection mechanisms, was no better than "medium."

5. ASSESSMENT OF STAFF INFORMATION SECURITY AWARENESS

As in previous years, security awareness checks were carried out among users as part of penetration testing in 2016. These checks consisted of a series of hacker attacks (agreed upon with the client in advance) and tracking of staff responses. Awareness of employees was tested using company-specific scenarios, consisting of electronic mailings containing an attachment or external URL. Messages claimed to be from either a company employee or an outside individual or company. In some cases, our testers spoke over the phone with responsive employees whose signatures indicated their extension numbers.

Example of user awareness testing

Step 1. Electronic Mass Mailings

Types of emulated attacks:
- Phishing
- Targeted Trojan infection
- Use of software vulnerabilities

Step 2. Gathering of Statistics

Events of interest:
- Users clicking a link, %
- Users opening an attachment, %
- Users entering credentials, %
- Users entering dialog with the intruder, %

Step 3. Phone Communication*

Results:
- Sensitive information (including user credentials)
- Opportunity to plan subsequent attacks

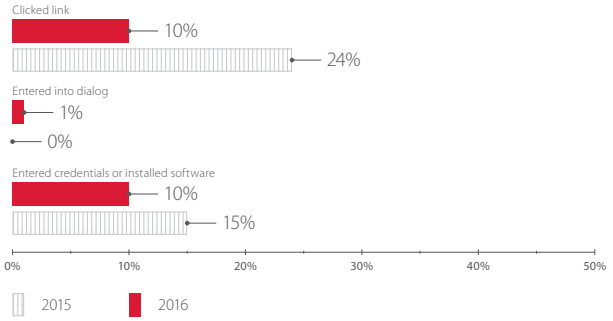
Step 4. Summary of Results

Results:
- Overall assessment of user awareness
- Recommendations for improving the level of user awareness

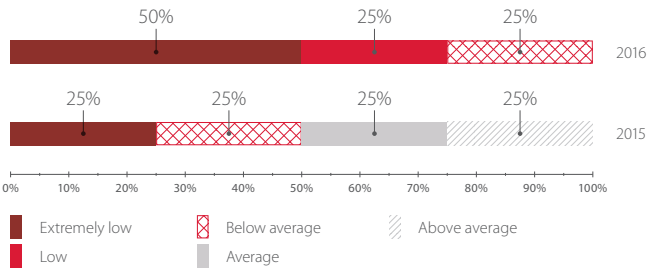
* if pre-approved with customer

Interesting fact

During testing at one company in 2016, employees received phishing messages from Positive Technologies testers and responded, falsely believing that the testers were network administrators at the company. For further testing, the testers selected an employee who had a phone number indicated in his email signature. From a single telephone conversation lasting about four minutes, Positive Technologies specialists were able to obtain information about system and application software in use and regarding the employee's domain account. This information can be used by an attacker to attack the internal network with the privileges of a legitimate user.



Employee awareness testing: overall results

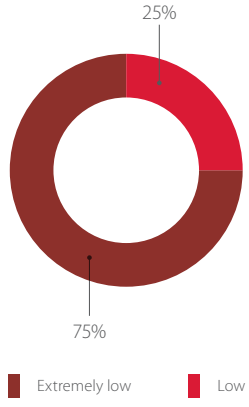


Information security awareness (percentage of customers)

On average, the number of events of interest recorded among users during awareness testing was lower than in the previous year, yet the average level of user awareness in 2016 was lower than in 2015. This is due to the fact that in 2015, most of these events occurred as part of a single testing project, far exceeding the numbers recorded in 2016.

6. SECURITY ANALYSIS OF WIRELESS NETWORKS

As compared to 2015, the overall security level of wireless networks decreased to **extremely low.**



Wireless network security in 2016
(percentage of systems)

On every tested system

the access point does not segregate authenticated users from each other. With access to a guest network, an intruder can attack other users on that network.

On 3 out of 4 systems,

the following vulnerabilities were detected:

1) Vulnerable authentication protocols (MS-CHAPv2, EAP)
2) Dictionary keys for access to wireless networks
3) Lack of wireless network protection mechanisms
4) Unauthorized wireless access points
5) Access to corporate access points from outside of controlled area

On every second system

the following vulnerabilities were detected:

1) Insufficient authentication mechanisms
2) Access to LAN via a wireless network
3) Identical accounts for access to different wireless networks
4) Lack of certificate verification
5) Weak password policy

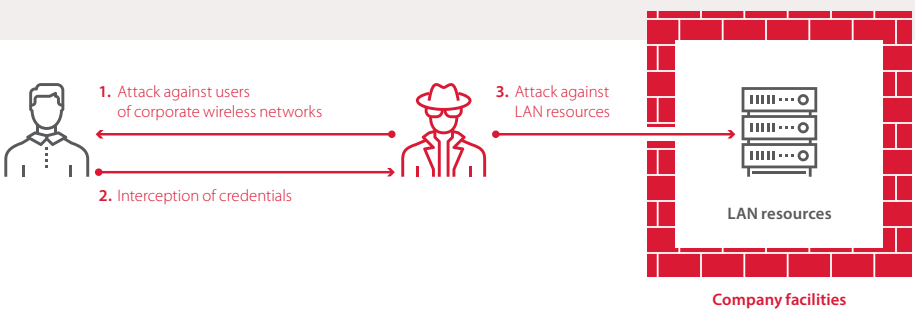
On some systems

the following vulnerabilities were detected:

1) No password needed to access network equipment management interface
2) Use of WPS
3) Use of internal DNS server on guest network

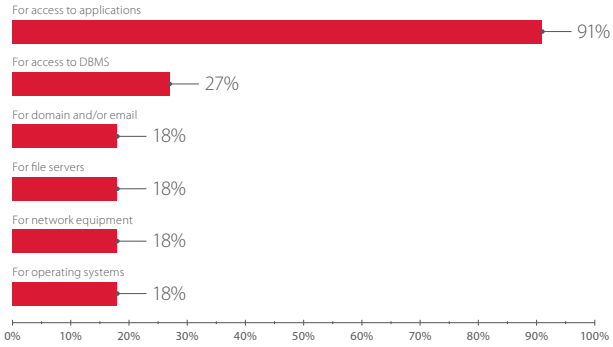
Every second system allowed access to LAN from Wi-Fi. An external intruder, using various vulnerabilities*, can carry out attacks on users of the corporate wireless network and then gain access to critical LAN resources without needing to set foot in company facilities.

* For example, lack of verification of network certificates, use of the vulnerable EAP protocol, or automatic switching of corporate users to an unprotected network.

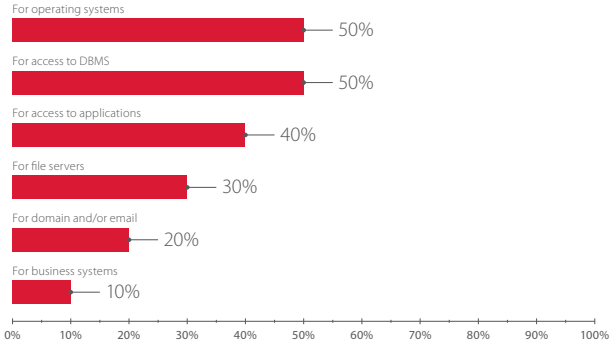


7. INTERESTING FACTS ABOUT DICTIONARY PASSWORDS

Use of dictionary passwords is a major security problem. This vulnerability ranks **first** among the most common vulnerabilities detected on the network perimeter, and **second** on internal networks.

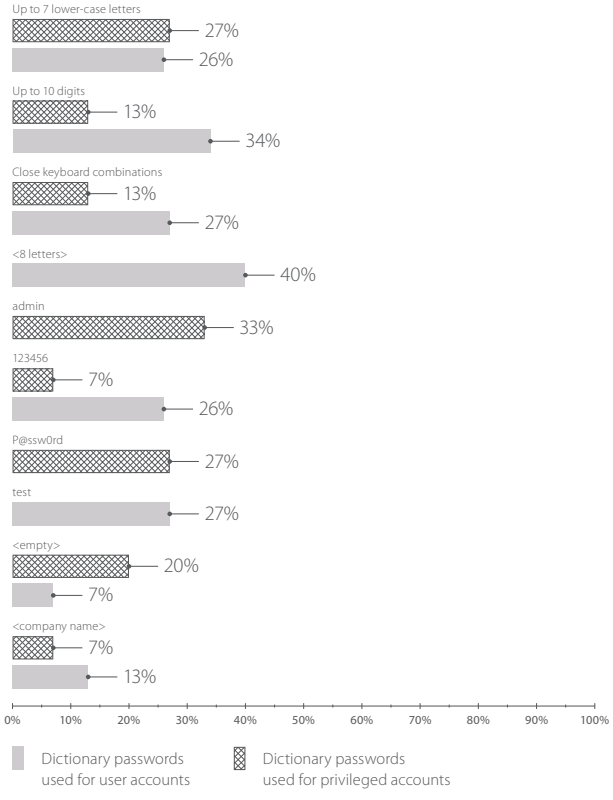


Dictionary passwords on the network perimeter (percentage of systems)



Dictionary passwords on intranet (percentage of systems)

On 33% of corporate systems, a privileged account with the password "admin" was found. This password is the most common administrator password. Second and third place went to "P@ssw0rd" and dictionary passwords of up to seven lowercase letters.



Most popular dictionary passwords in 2016 (percentage of systems)

CONCLUSIONS

As shown by our research, today's corporate information systems have become more vulnerable to attacks by external and internal intruders, and implementing such attacks does not require great skill. Compared to last year, the level of security of wireless networks and user awareness regarding information security have significantly decreased.

The vast majority of attacks on corporate infrastructures involve exploitation of common vulnerabilities and flaws. Companies can dramatically improve their security stance and avoid falling victim to attacks by applying basic information security rules:

1) Implement a strict password policy.
2) Protect privileged accounts.
3) Do not store sensitive information in cleartext or on publicly accessible resources.
4) Minimize the number of open network service interfaces on the network perimeter.
5) Protect or disable unneeded protocols. Make sure that networks are segmented.
6) Minimize the privileges of users and services.
7) Regularly update software and install operating system security updates.
8) Use SIEM systems for attack detection.
9) Use web application firewalls for application protection.
10) Regularly train employees and improve information security awareness. Follow up to verify that such training is having the intended effect.
11) Use antivirus solutions for protection against malware, which is often spread via social engineering.
12) Perform penetration testing in order to identify new attack vectors and test protection methods in a timely manner.

By applying all these measures, companies can ensure effective protection and justify the cost of expensive specialized security solutions.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

© 2017 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.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com