POSITIVE TECHNOLOGIES

VULNERABILITIES IN CORPORATE INFORMATION SYSTEMS

2018

CONTENTS

INTRODUCTION

Corporate IT infrastructure is a complex multicomponent ecosystem designed to automate business processes. Domain infrastructure, email services, web applications, and business systems are all at the core of any corporate information system. Although the size of IT infrastructure depends on the company size and headcount, most companies have common information security flaws in their information systems. For example, WannaCry ransomware affected more than 500,000 computers, many of them owned by governments, large companies, and small businesses. This outbreak confirmed that absolutely any company may suffer from hacker attacks.

This report outlines main trends in security assessment of corporate information systems and provides information about the following:

+ Most common attack vectors that can be used by a hacker to access corporate network applications
+ Most common vulnerabilities on the network perimeter
+ Criticality of actions performed by an attacker having access to the intranet
+ Security flaws that an attacker can exploit to gain maximum privileges in the corporate infrastructure
+ Effectiveness of social engineering attacks
+ Ability to gain intranet access via attacks on wireless networks

The source material for these statistics and analysis comes from security assessments of corporate information systems performed by Positive Technologies in 2017.

1. EXECUTIVE SUMMARY

Security assessment of network perimeter:

+ Security assessment of corporate information systems revealed that in 68 percent of cases, it was possible to penetrate the network perimeter and access the LAN.
+ Common vectors for intranet penetration are bruteforcing accounts—by taking advantage of passwords that consist of dictionary words or simple combinations—and exploiting web application vulnerabilities.
+ Automated scanning of network perimeters revealed that 31 percent of companies were at risk of infection by WannaCry encryption malware.

Security assessment of intranet resources:

+ Penetration testers with insider privileges obtained full control over company infrastructure in all cases tested.
+ Among corporate systems tested from April 14 to December 31, 2017, 60 percent contained vulnerability MS17-010, which is evidence of late installation of critical OS security updates.
+ Insufficient protection against recovery of user accounts from the operating system memory is a major vulnerability that allows gaining full control over a corporate information system.

Evaluation of staff awareness:

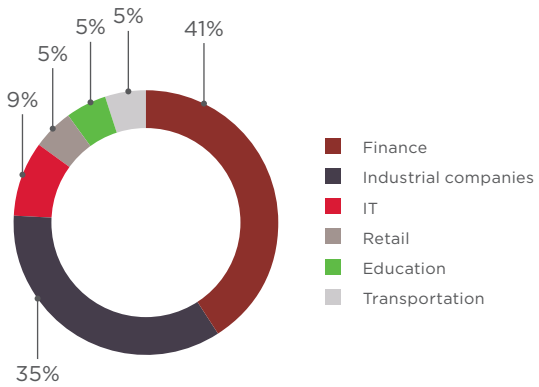
+ In test mailings, 26 percent of employees clicked links to phishing websites, of which almost half entered their credentials in a fake authentication form.
+ One out of every six employees exposes corporate infrastructure to the risk of virus attack.

Security assessment of wireless networks:

+ In 75 percent of cases, attacks on wireless networks resulted in access to the corporate intranet and sensitive information (such as domain user accounts).

2. RESEARCH DATA

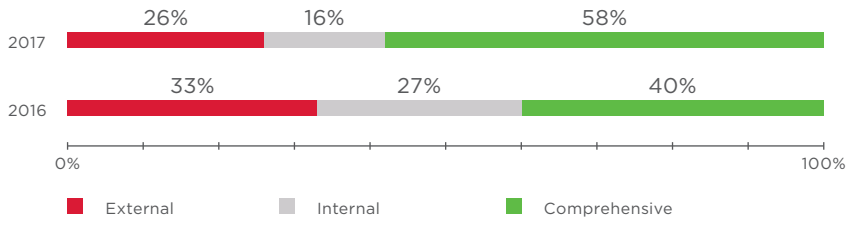
The statistics for 2017 draw upon security audits of 22 corporate systems belonging to companies in various industries. These particular audits were chosen so as to provide a maximally informative picture. Projects involving a limited number of hosts are not included, since they are not representative of the overall state of corporate information system security. As in 2016, most penetration testing was performed on behalf of financial and industrial companies. Successful attacks on corporate systems in finance and industry tend to generate the greatest profit for attackers. A successful attack against bank infrastructure frequently leads to direct theft of funds. Penetration of the intranet at an industrial company can lead both to leakage of sensitive information (which can be sold to competitors) and to disruption of operations.



Tested systems, by industry

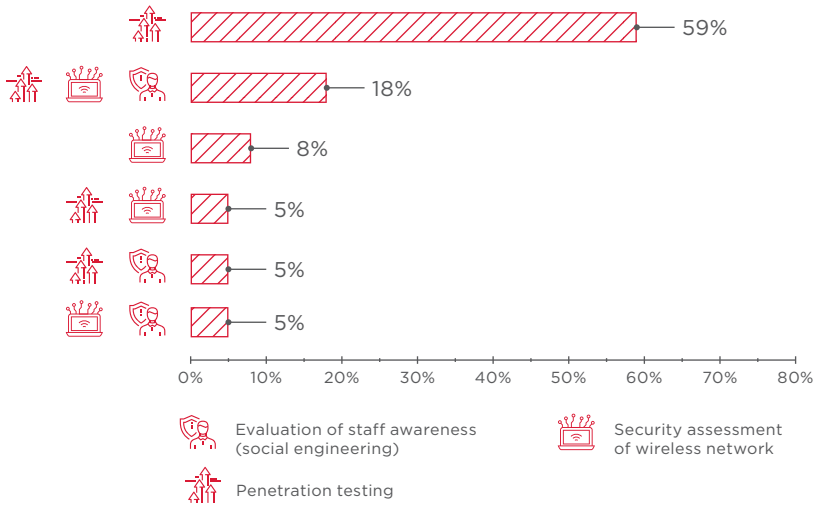
Security assessment of corporate networks included external, internal, and comprehensive (external plus internal) penetration testing. Penetration testing is an effective method for detecting vulnerabilities in corporate infrastructure and obtaining an objective, independent evaluation of the state of security. Testers simulate the actions that a real attacker would attempt, from both the Internet and the company's intranet. This approach recreates the conditions that attackers face during a real hack and provides the information needed to promptly remediate flaws.

Clients are increasingly interested in comprehensive testing. Besides protecting their network perimeter from external attackers, clients realize the need to minimize the risk of intranet compromise by internal attackers.



Types of penetration testing (percentage of tested systems)

A significant portion of clients also requested assessment of Wi-Fi security and staff awareness (social engineering) in addition to penetration testing.



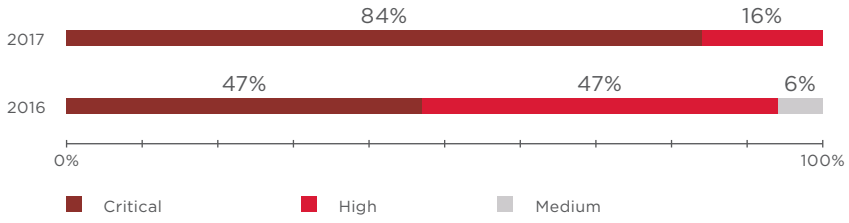
Types of services performed (percentage of tested systems)

Network perimeter security data from external penetration testing in 2017 is compared both with results from 2016 and statistics from automated scanning during the WannaCry outbreak. In the second quarter of 2017, Positive Technologies offered free-of-charge scanning of the external perimeter for detecting vulnerable services. Scanning was requested by 26 companies in different industries. External penetration testing and automated scanning are considered and compared more closely later in this report.

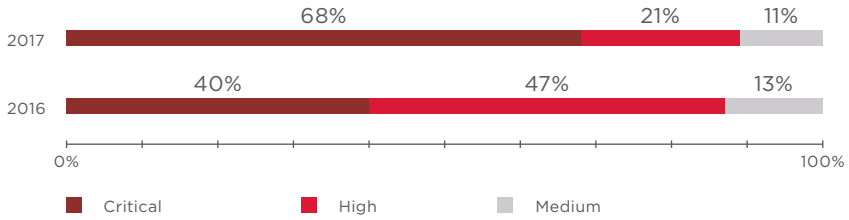
3. STATISTICS FOR 2017

3.1. Security assessment results

Almost every security assessment performed by our specialists reveals multiple vulnerabilities and security flaws, which allow an attacker to perform a full compromise of the entire corporate infrastructure, obtain access to sensitive information, or perform Denial of Service attacks. Vulnerabilities are placed in one of three categories: configuration flaw, missing security update, or flaw in web application code. Each detected vulnerability is ranked by severity level according to CVSS v3.0 metrics.

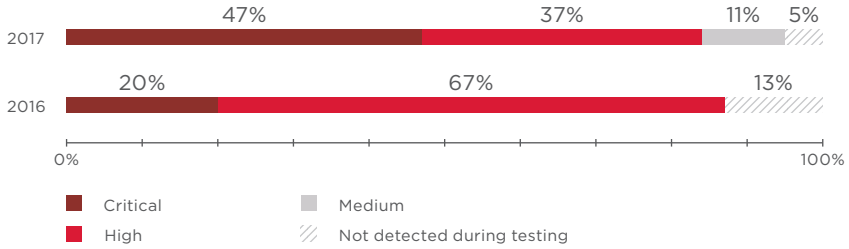


Maximum severity of detected vulnerabilities (percentage of tested systems)

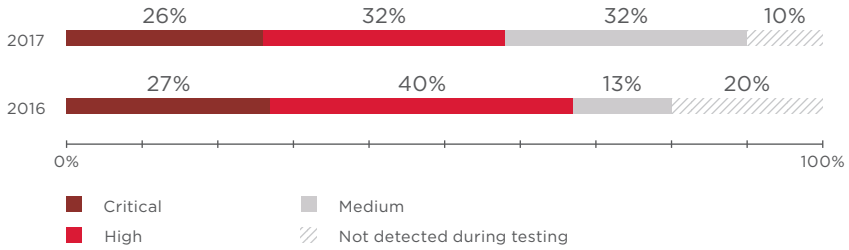


Maximum severity of vulnerabilities caused by configuration flaws (percentage of tested systems)

18 years
is the age of the oldest vulnerability CVE-1999-0532 detected during automated analysis of the network perimeter



Maximum severity of vulnerabilities caused by uninstalled security updates
(percentage of tested systems)



Maximum severity of vulnerabilities caused by flaws in web application code
(percentage of tested systems)

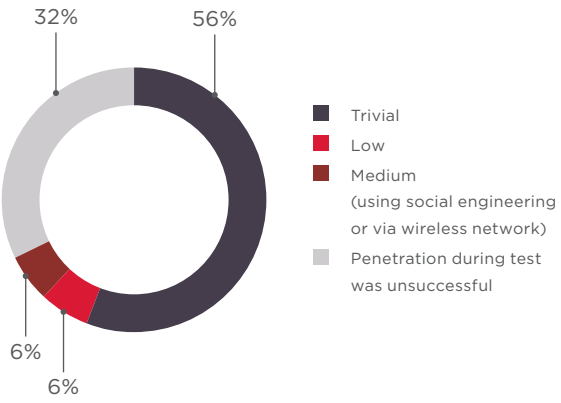
Compared to 2016, the share of corporate systems with critical vulnerabilities (CVSS score ≥ 9.0) almost doubled. The main cause is the publication of critical vulnerability MS17-010, which affects the SMB service on Windows systems. After exploits had been made available to the public, our specialists exploited this vulnerability in numerous internal penetration tests to obtain total control over LAN hosts and continue an attack up to obtaining maximum privileges on the domain.

Some systems were not found to contain any flaws in web application code or flaws caused by uninstalled security updates. However, black-box testing cannot detect all possible vulnerabilities. The main aim of penetration testing is to objectively assess how well a corporate system is protected from attacks.

3.2. Security assessment of network perimeter

Results of external penetration testing

Statistics for 2017 show that the security level of the network perimeter is unchanged from 2016. However, penetrating the network perimeter became less complicated. In 2016, the difficulty of accessing LAN resources was "trivial" in only 27 percent of tests, but the equivalent figure doubled to 56 percent in 2017.



Difficulty of network perimeter penetration (percentage of tested systems)

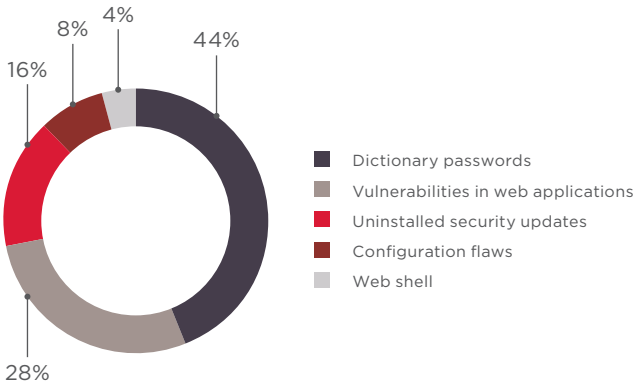
10
is the maximum number of vectors for intranet penetration detected on a single corporate information system in 2017

The reason is that access to LAN resources requires two basic steps: for example, bruteforcing an account with a dictionary password to log in to a web application, and exploiting vulnerabilities in order to perform OS commanding on the target host.

Security assessment of corporate information systems detects, on average, two vectors for intranet penetration at each company tested. The maximum number of vectors detected at a company was 10.

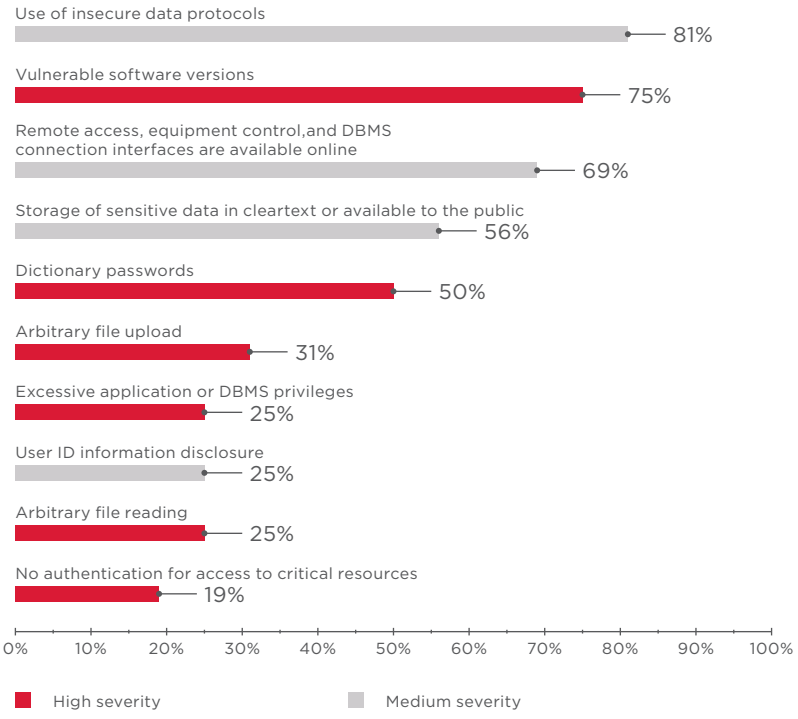
All successful vectors for intranet penetration can be divided into the following categories:

+ 44 percent of successful attack vectors are based on bruteforcing credentials for access to web applications, database management systems, and other services accessible on the network perimeter. With credentials in hand, the attacker can now execute OS commands on the target host.
+ 28 percent of attack vectors are based on exploiting web application vulnerabilities. Several external tests revealed vulnerabilities that allow remote execution of OS commands with the privileges of the web application in a single step, without even logging in.
+ In 16 percent of cases, an attacker could access intranet resources by exploiting vulnerabilities in obsolete software versions (such as CMS platforms).
+ In other cases, an attacker can use configuration flaws to extract credentials stored in cleartext, such as on web application pages, in order to access systems on the network perimeter. In some tests, our experts also found a web shell that had been already uploaded to the servers of tested companies, indicating previous successful external hacks by unknown attackers.



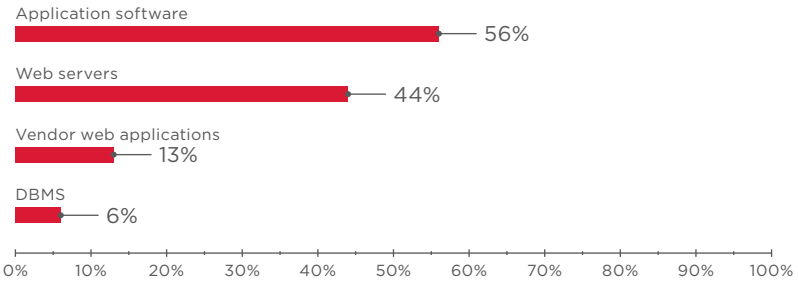
Attack vectors for penetrating the network perimeter

The top five common vulnerabilities on the network perimeter are the same as in 2016, though their relative percentages shifted. In general, the average number of vulnerabilities detected in external penetration testing is falling. For example, every system tested in 2016 had vulnerabilities caused by the use of dictionary credentials. In 2017, this figure fell by half, mostly thanks to clients who had acted on recommendations from previous testing to remediate vulnerabilities identified, address configuration flaws, and improve enforcement of password policies. The external penetration testing repeated at these companies 12 to 18 months later reflects these companies' progress, improving the picture of vulnerabilities in 2017.

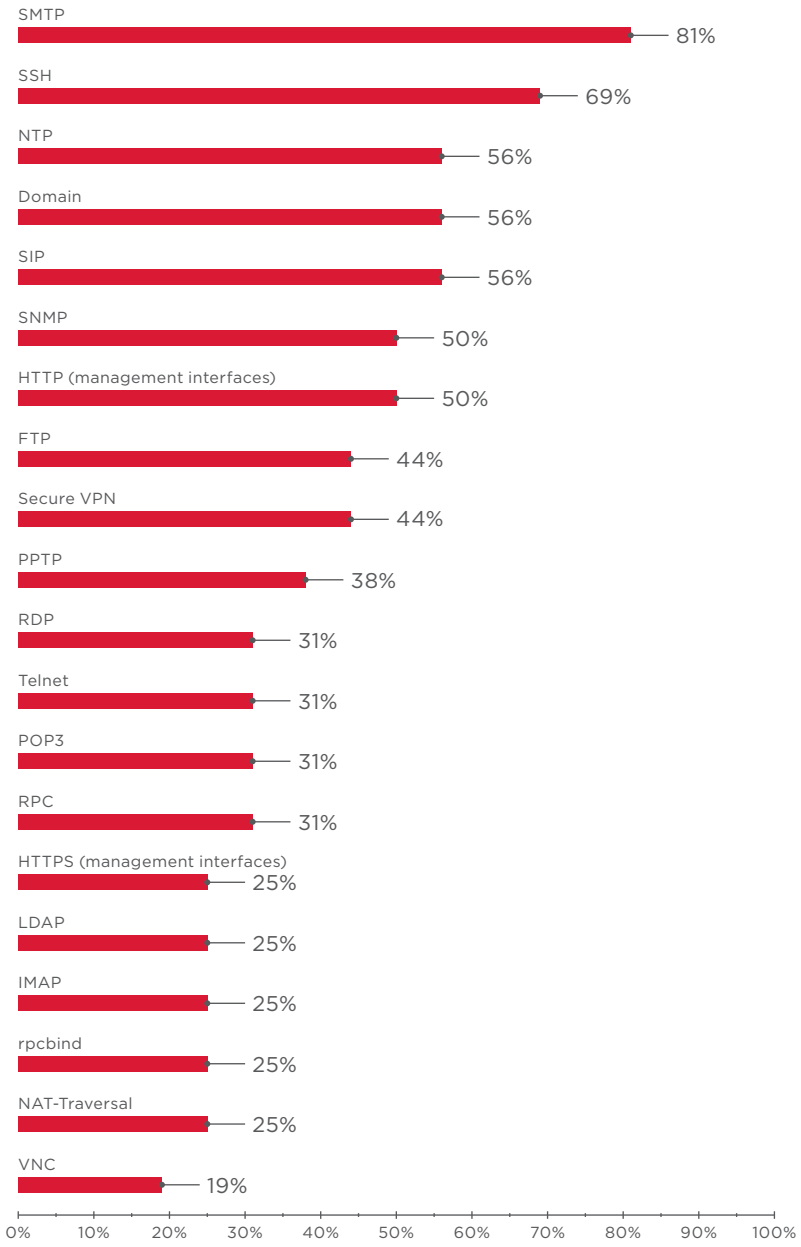


Most common vulnerabilities on the network perimeter (percentage of tested systems)

As in 2016, most vulnerabilities detected on the network perimeter were found in application software and on web servers.



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



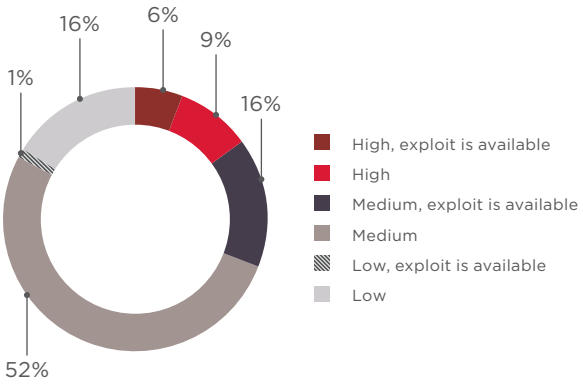
Protocols used on the network perimeter (percentage of tested systems)

Security assessment of the network perimeter

As mentioned before, Positive Technologies made a special offer to companies in Q2 2017: external perimeter scanning, free of charge, for detecting vulnerable services. The main aim was to prevent the spread of damage by WannaCry malware. A total of 26 companies in different industries—IT, telecom, finance, oil and gas, and retail—requested an automated scan of their network perimeter.

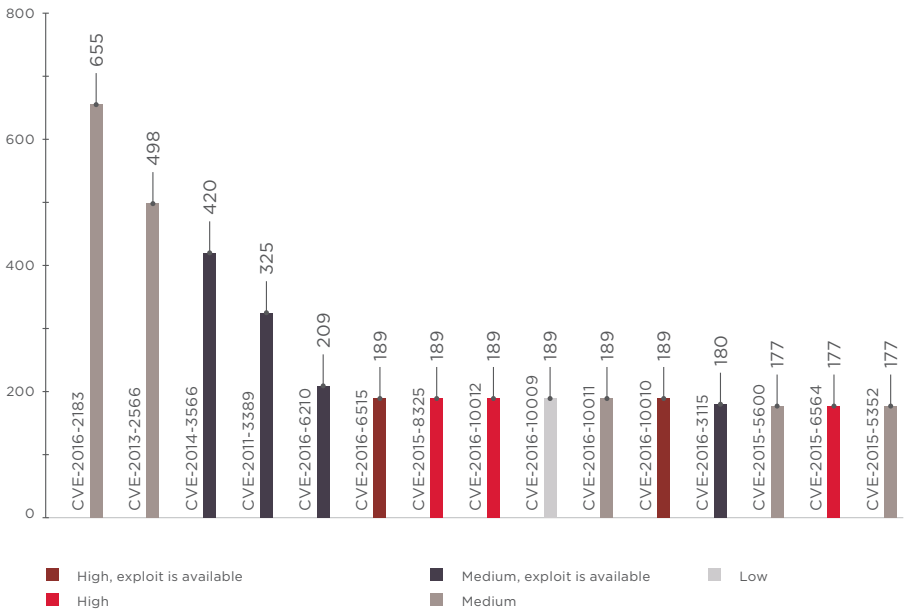
The first task for the companies was to define the borders of their corporate systems. But even this was not easy for everyone: 23 percent of the companies either could not define their network borders or defined them incorrectly. Even in the absence of testing, the inability to define the network perimeter is clear evidence of poor protection from external attacks.

Network perimeters were scanned by the MaxPatrol compliance and vulnerability management system in combination with additional software. Scanning revealed numerous vulnerabilities: 15 percent were of high severity according to CVSS v2.0, with some of them having publicly available exploits.



Severity of vulnerabilities (percentage of all vulnerabilities)

Many of the vulnerabilities detected by automated scanning of the network perimeter are common across systems. The most critical of these vulnerabilities is CVE-2016-6515 in OpenSSH: password lengths for password authentication are not limited, which allows remote attackers to perform Denial of Service attacks. A public exploit[1] for the vulnerability has been published. An attacker can also bruteforce credentials to connect via SSH and obtain user privileges on UNIX systems; the CVE-2016-10010 vulnerability in OpenSSH in this case allows using another exploit[2] for local privilege escalation on a compromised host and developing an attack on LAN resources.

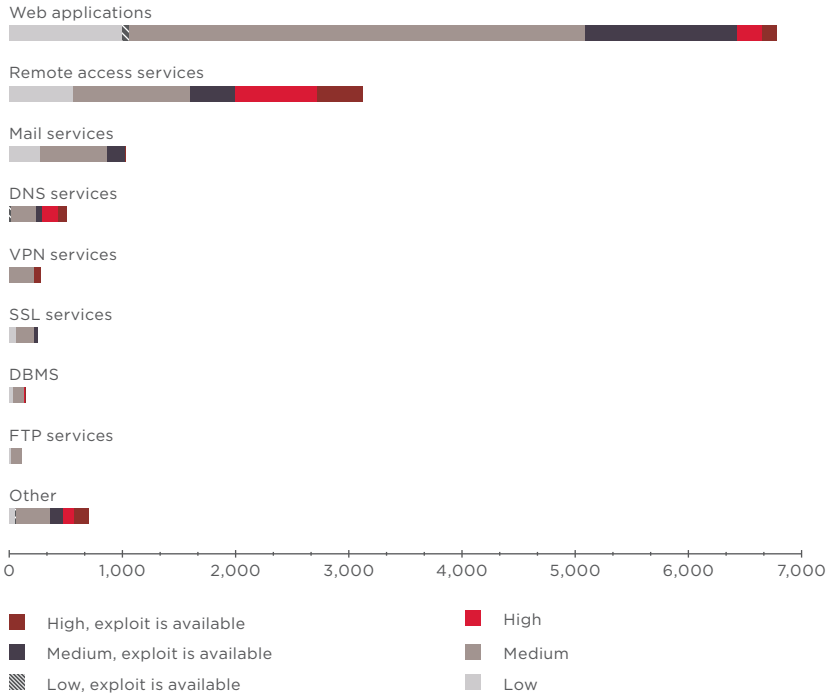


Most common vulnerabilities on the network perimeter, by severity level (automated assessment)

Most vulnerabilities revealed by the assessment of accessible services were in web applications and remote access services (SSH). These results of automated assessment match the statistics of external penetration testing: vulnerabilities and configuration flaws in web applications were generally the point for "jumping off" to gain access to LAN resources.

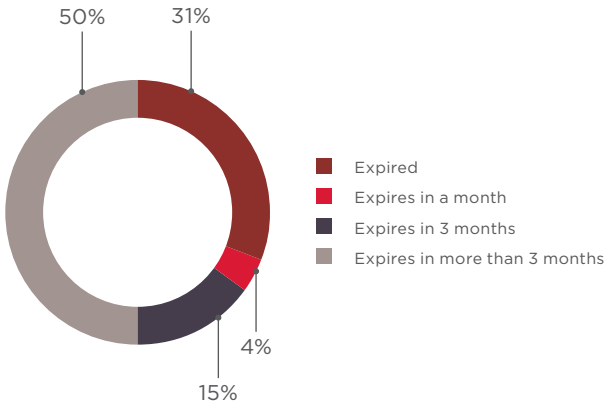
1 exploit-db.com/exploits/40888/

2 exploit-db.com/exploits/40962/

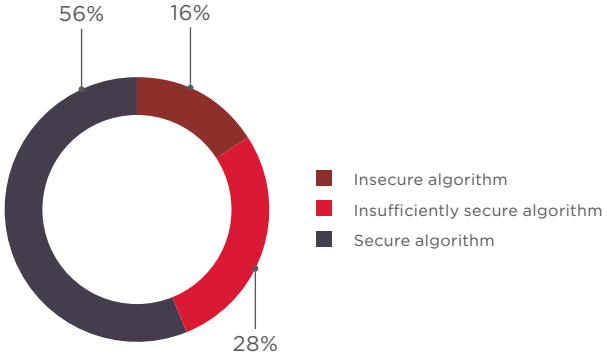


Number of vulnerabilities depending on services in use, by severity level

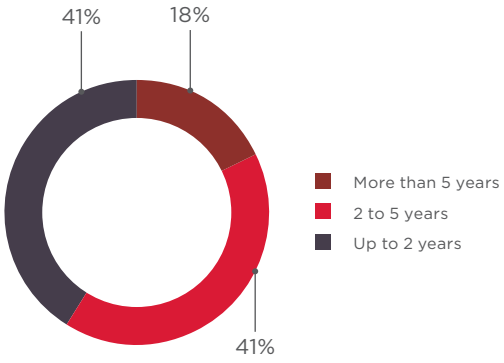
Automated assessment of accessible web applications provided separate statistics for the state of SSL certificates. At the moment of scanning, more than a quarter of the certificates had expired, 16 percent used insecure cryptographic algorithms (such as SHA-1), and one in every six certificates had a validity period of more than five years.



Validity status of SSL certificates



Encryption algorithms in SSL certificates



Validity of SSL certificates

Expired SSL certificates may trigger significant reputational losses and lost business for companies: as soon as users see a warning that a website is using an invalid certificate, they may decide not to visit it.

Insecure encryption algorithms make SSL certificates useless, because they enable an attacker to intercept network traffic and decrypt data. An attacker can also alter an SSL certificate and create a phishing website for infecting visitors with malware and stealing their credentials. Yet visitors would think their computers became infected after visiting the official company website.

A validity period of more than five years places SSL certificates at risk for having their encryption key cracked.

Automated scanning of network perimeter resources revealed that 8 out of 26 companies had external hosts with open TCP port 445 running SMB—meaning that the infrastructure of almost one third of companies was vulnerable to WannaCry.

31%
of companies could be infected by WannaCry

3.3. Analysis of intranet resources

If an attack against network perimeter resources is successful, an external attacker can access the internal network and continue the attack up to gaining total control of the company's IT infrastructure.

As in 2016, penetration testing performed with the privileges of internal users (such as ordinary company employees who are given access to the user segment of the network) showed that total control of the infrastructure can be obtained on all tested systems. In a mere 7 percent of tests, was a "medium" level of sophistication needed for an insider to access critical recourses. In all other cases, even a minimally skilled attacker could compromise the entire corporate system.

A typical vector for intranet attack was to gain maximum privileges on a LAN host and run software to obtain the credentials of other users who had previously connected to that host. By performing this two-step sequence on numerous hosts in succession, the attacker can eventually find a host that has the domain administrator account and obtain the password in cleartext.

Gaining maximum privileges on intranet hosts became significantly easier for attackers in 2017 when information about vulnerability MS17-010 was published. On March 14, 2017, Microsoft released an update to fix the vulnerability. A month later, on April 14, the Shadow Brokers hacking group released EternalBlue,[3] an exploit for the vulnerability. From mid-April to the end of 2017, our experts successfully used this exploit in 60 percent of internal penetration tests, which confirms that critical OS security updates were not installed on most corporate systems in due time.

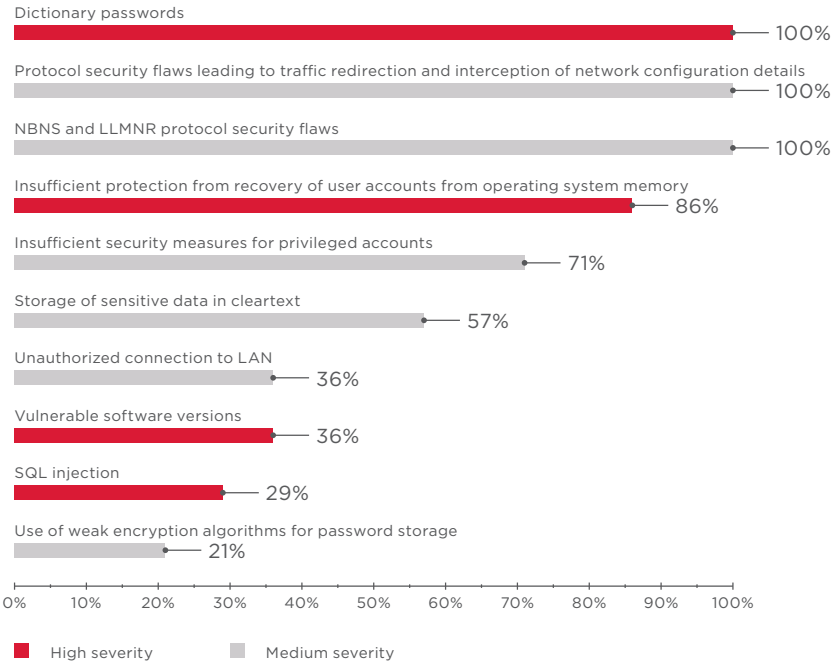
60%
of corporate systems tested from April 14 to December 31, 2017 contained the MS17-010 vulnerability

By the end of 2017, more and more corporate systems had been updated in response to vulnerability MS17-010. But in some cases, another published critical vulnerability (MS17-018) was exploited on Windows hosts for local privilege escalation. This vulnerability also has an exploit, which is unavailable to the public.

3 vulners.com/seebug/SSV:92952

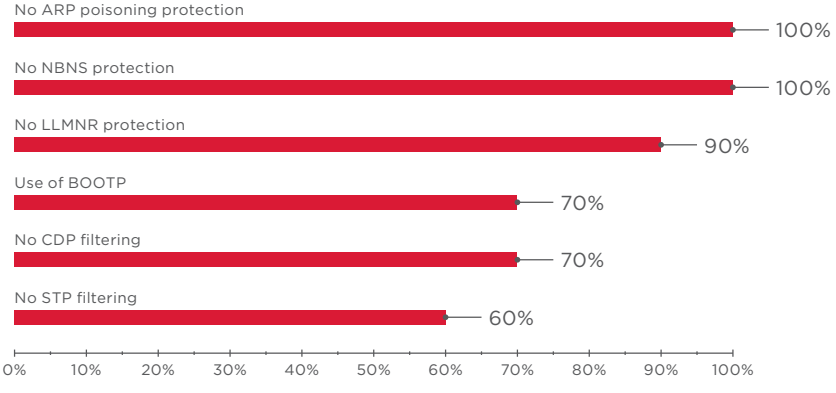
Compared to 2016, the statistics for the most common intranet vulnerabilities remain almost the same. The only exception is a new type of vulnerability, which is referred to here as "Weak protection against account recovery from OS memory." On Windows hosts, passwords (or their hash sums) can be recovered in cleartext from system memory by special software, if the attacker has local administrator privileges. Previously, this vulnerability was considered a flaw in antivirus software, since antivirus software should prevent running any software that extracts credentials. But recently, such malware has been written in PowerShell to bypass antivirus protection. Now to prevent extraction of credentials from OS memory, a comprehensive approach is required, including prohibiting storage of cached data, clearing the credentials of logged-out users from the memory of the lsass.exe process more quickly, and disabling wdigest. Recent versions of Windows 10 with Remote Credential Guard also allow isolating and protecting the lsass.exe system process from unauthorized access. Therefore, in 2017 we have broken out credential extraction into a separate metric for a more accurate picture of the state of security.

On the 14 percent of corporate systems where protection against account recovery from OS memory was adequate, other attack vectors were used to obtain total control of corporate infrastructure.

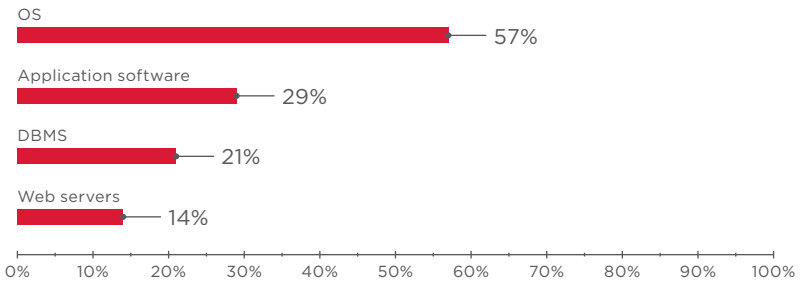


Most common intranet vulnerabilities (percentage of tested systems)

Statistics on security flaws in service protocols are taken from the tests that included analysis of LAN traffic (71% of clients). Other clients opted out of such analysis, because of the risk that it might cause interruptions in network operation.



Security flaws in service protocols (percentage of tested systems)



Vulnerable software versions found on intranet (percentage of tested systems)

Internal testing revealed that main flaws in corporate information systems are the failure to install critical security updates in a timely manner and weak protection against account recovery from OS memory.

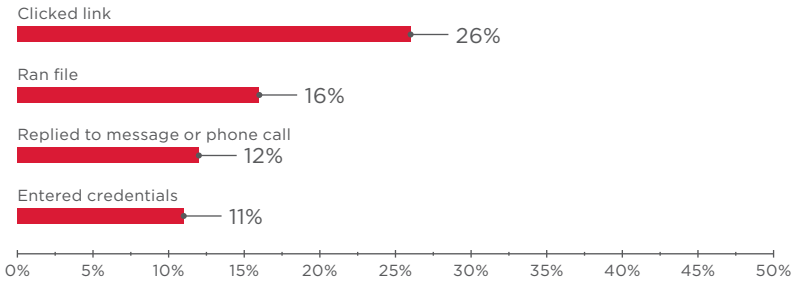
4. ASSESSMENT OF STAFF INFORMATION SECURITY AWARENESS

Security awareness checks were carried out among employees as extra part of penetration testing of corporate information systems. Testing is approved in advance by the client and involves social engineering attacks that imitate what real attackers would do. The responses of employees are then tracked and categorized.

Testing included two methods: by email and by phone. The following four potential responses were tracked:

+ Clicking a link to an attacker's website
+ Entering a password in a specially crafted authentication form
+ Running an attached file
+ Communicating with an attacker by phone or by email

The results demonstrated that 26 percent of employees click links to phishing websites, with almost half of them entering their data in a fake authentication form. One out of every six employees exposed the corporate infrastructure to the risk of virus attack by running an attached file. In addition, 12 percent of employees were willing to enter into dialog with an attacker and disclose information, which can be used in attacks on the corporate information system.



Risky responses (percentage of employees)

More than 1,300 emails were sent in security awareness tests during 2017. Half of them contained a link to a phishing website and the other half had an attachment: a file with a script that sent the file opening time and the employee's email address to our testers. A real attacker could add a set of exploits targeting various vulnerabilities, including CVE-2013-3906, CVE-2014-1761, and CVE-2017-0199. Such an attack can result in control of the user's workstation, malware propagation, Denial of Service, and other negative consequences.

A typical example of a social engineering attack:

1) An attacker deploys exploits for various software versions on a website.
2) Potential victims receive an email message that links to this website.
3) An employee clicks the link in the email. As soon as the web page loads, vulnerabilities are exploited.

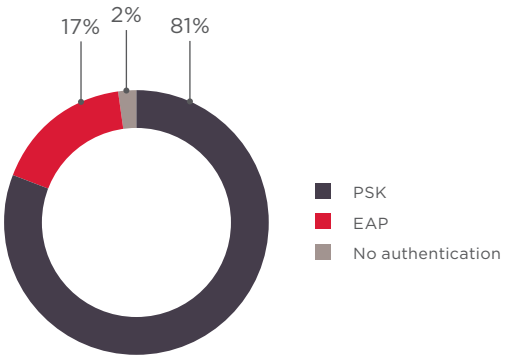
These attacks can lead to infection of the user's workstation with malware. Moreover, if a user has an outdated browser version, Remote Code Execution can be implemented (for example, CVE-2016-0189). As soon as the attacker has access to an intranet host, the attack can be continued to gain maximum privileges on the corporate infrastructure. For more details on attack scenarios involving social engineering, see our report "Social engineering: how the human factor puts your company at risk."

5. SECURITY ASSESSMENT OF WIRELESS NETWORKS

40%
of companies have a dictionary password for wireless network authentication

Attacks on wireless (Wi-Fi) networks are yet another way for an external attacker to gain access to intranet resources. Even if attempts to penetrate the network perimeter (such as attacks against web applications) are unsuccessful, an attacker can still make use of wireless network vulnerabilities. An attack against a wireless network requires inexpensive equipment and access to a location within signal range of the wireless network. An attacker even does not need to be on company property: our tests revealed that 75 percent of wireless networks are accessible from outside controlled areas. In many cases, a parking lot next to an office building would be close enough to perform a wireless network attack.

Almost all wireless networks tested in 2017 used the WPA2 protocol with various authentication methods, the most common of which was PSK (pre-shared key).



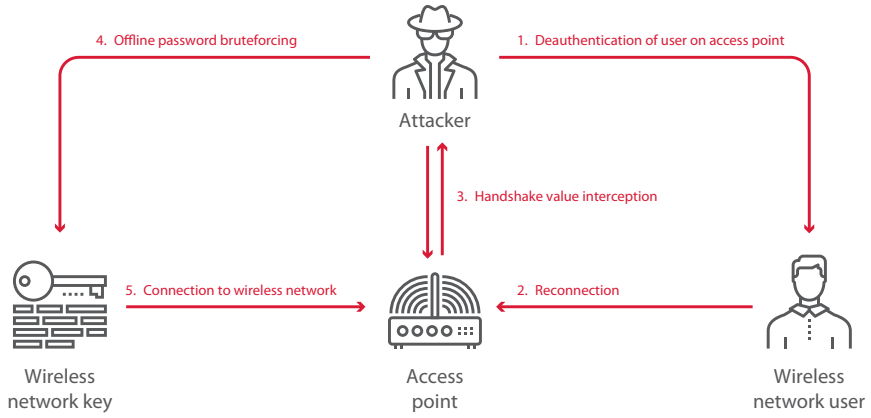
Wireless network authentication methods

Wireless network attack scenarios depend on the authentication method in use. The following two scenarios for gaining intranet access were the most common in 2017:

+ Interception of handshake between an access point and a legitimate user (works with PSK authentication method only)
+ Spoofing of access points to attack wireless network users (works with all authentication methods)

The first scenario involves bruteforcing a password for the intercepted handshake value. The success of this method depends on the complexity of the password in use. However, note that the password can be bruteforced outside the access point coverage area. Our experts are limited by testing timeframes and sometimes do not have enough time to bruteforce passwords for intercepted handshake values. However, more patient attackers might have more success.

After bruteforcing the password and connecting to an access point, the testers found that 75 percent of tested wireless networks do not isolate users from each other. Thus, a hacker can attack users' devices, for example, by exploiting the MS17-010 vulnerability on personal and corporate laptops.

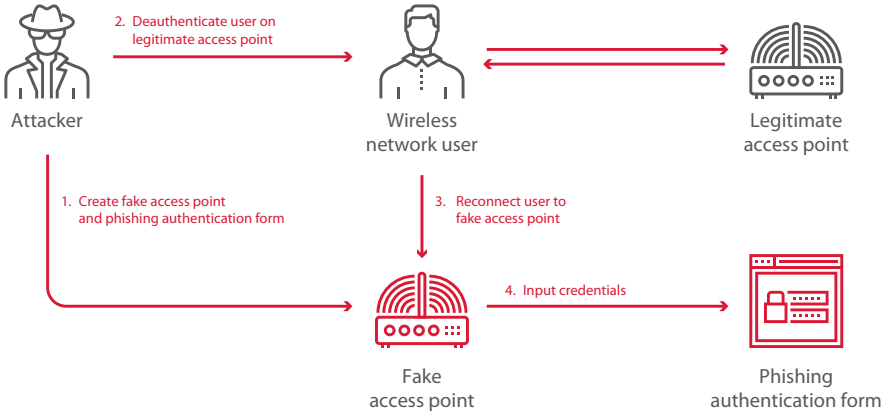


Interception of handshake between an access point and a legitimate client

If bruteforcing of an access point password is unsuccessful, the second scenario (access point spoofing) can be tried out.

Firstly, an attacker can use a fake access point in combination with a phishing authentication form to obtain credentials and intercept sensitive information transmitted over unencrypted data transfer protocols (such as HTTP or FTP).

One of tests performed by Positive Technologies in 2017 involved assessment of a wireless network in Moscow, Russia. Testers used a fake access point with the extended service set identifier (ESSID) MT_FREE, which is used for access to the wireless network available in public transport and very popular among city residents. A fake authentication form was created, complete with the logo and design of the client. After a user connected to the fake access point, any attempt to visit a website was redirected to the fake authentication form. In this manner, testers obtained the domain credentials of employees and used them to continue the test attack.



Access point spoofing

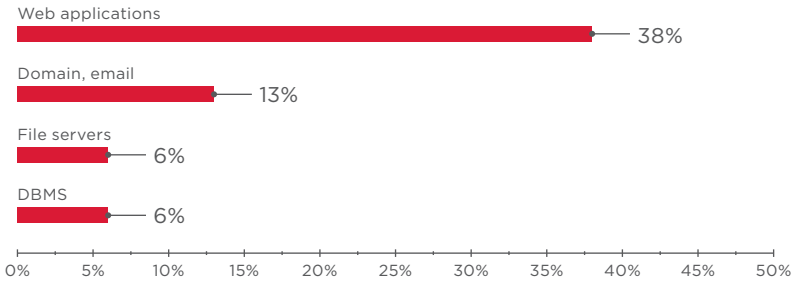
At only 1 out of 8 tested companies did employees not enter their passwords in a fake authentication form

Secondly, a fake access point can help an attacker to intercept credentials stored on a user's device. An attacker creates an access point with the same ESSID and settings as a legitimate access point. If a user has enabled automatic connections to known networks, the user's device will try to connect to a fake access point if the signal is currently stronger than that of the legitimate one. As a result, the attacker can obtain the hash sums of employees' passwords and use them to continue the attack on corporate infrastructure.

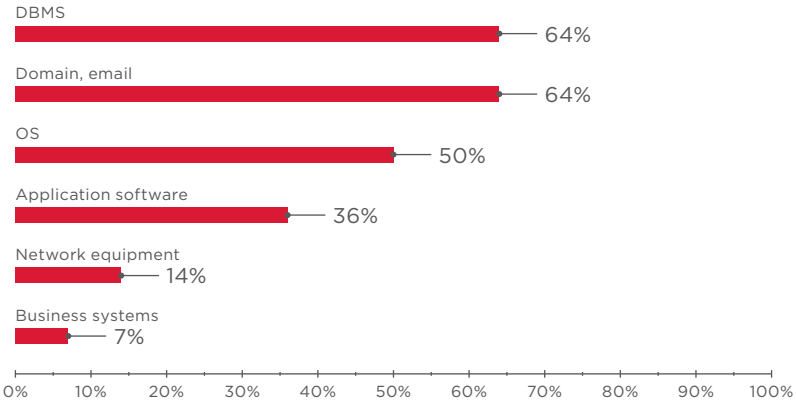
In 75 percent of cases, attacks on wireless networks result in access to intranet resources and sensitive information (such as domain user accounts). This method of intranet penetration is an effective alternative to classic attacks against network perimeter hosts.

6. INTERESTING FACTS ABOUT DICTIONARY PASSWORDS

Based on penetration testing results, we have created a graph of the services on which dictionary passwords are most common. These statistics are primarily intended to remind system administrators of the necessity to use complex passwords and timely change standard accounts as soon as a new service is installed and in use.



Dictionary passwords for services on the network perimeter (percentage of tested systems)

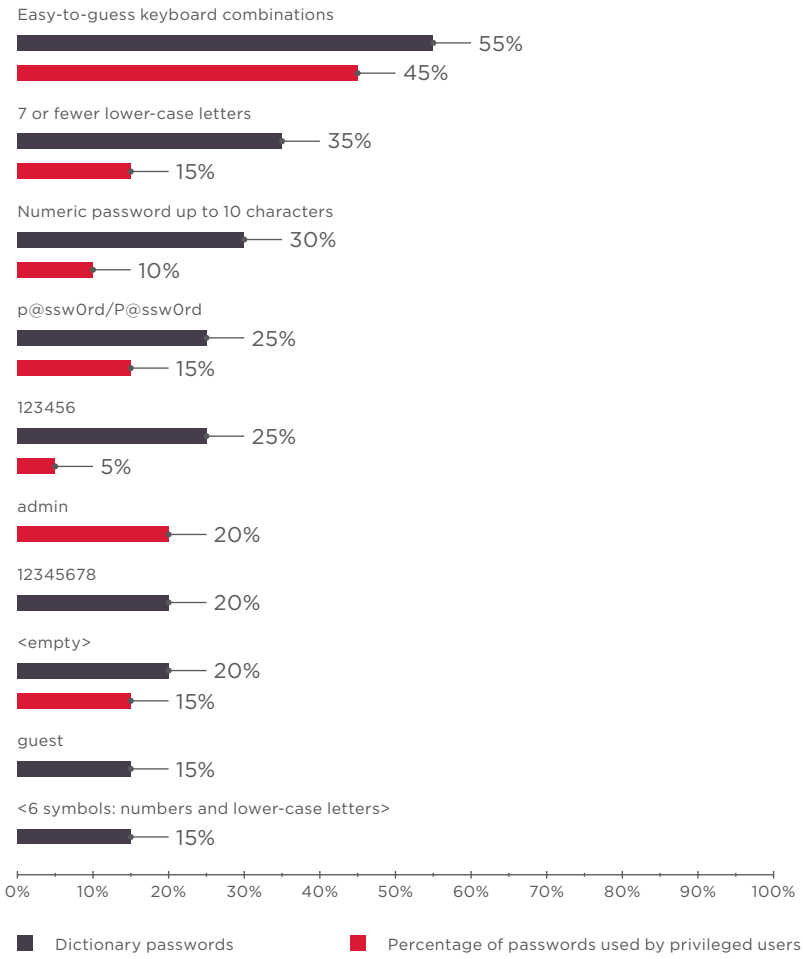


Dictionary passwords found on internal networks (percentage of tested systems)

Results for 2017 demonstrated that common users and administrators frequently choose passwords that are combinations of keys close on the keyboard, assuming that a long and meaningless password (such as zaq12wsxcde3 or poiuytrewq) is sufficiently strong to protect them from unauthorized access. However, this belief is erroneous: although such a password may seem to be gibberish, all such key combinations have long been added to password-cracking dictionaries. Hackers can bruteforce these passwords in a matter of minutes.

Qwerty, Zaq1xsw2

and other close key combinations are the most common passwords even among privileged users



Most common dictionary passwords (percentage of tested systems)

CONCLUSION

Corporate information systems are still vulnerable to attacks by external and internal malicious users. The results of external penetration testing prove that companies are starting to pay attention to the security of their network perimeters. Unfortunately, protection of corporate systems from internal attackers is rather poor, as our testers found. In 2017, penetration testers acting as external attackers with a variety of different methods, including social engineering and wireless network attacks, successfully penetrated the network perimeter in 68 percent of cases. An internal attacker was able to obtain control of LAN resources in 100 percent of cases, despite all the software and organizational measures in place to prevent such attempts.

Our core recommendations for ensuring an acceptable level of security on corporate information systems remain the same as in previous years:

+ Prevent use of dictionary and other easy-to-guess passwords; develop and enforce strict password policies.
+ Ensure additional protection of privileged accounts (such as domain administrator accounts). Two-factor authentication is a good practice.
+ Protect infrastructure against attacks aimed at recovering credentials from operating system memory. For this purpose, install Windows 8.1 or later and add all privileged domain users to the Protected Users group on all privileged user workstations and on all hosts to which privileged accounts connect. Recent versions of Windows 10 with Remote Credential Guard also allow isolating and protecting the lsass.exe system process from unauthorized access.

- Check that no sensitive information that could be useful for an attacker is stored in cleartext (for example, on web application pages). Examples of such information include credentials for access to different applications and corporate address books listing employees' email addresses and domain identifiers.
- Restrict the number of services on the network perimeter. Verify that any interfaces available for connection should really be accessible to all Internet users.
- Install OS security updates and the latest versions of applications in a timely manner.
- Assess the security of wireless networks. Scrutinize the authentication methods in use and enable isolation of access point users.
- Regularly train employees on information security awareness and verify employee knowledge on an ongoing basis.
- Use SIEM systems for timely detection of attacks. Prompt detection of attacks is critical for limiting the damage from digital attacks.
- Install a web application firewall (WAF) to protect web applications.
- Perform regular penetration testing for timely detection of vectors that could be used in attacks and assessing the actual effectiveness of applied security measures.

While this list is not exhaustive, failure to implement even just one of these recommendations could lead to a full compromise of corporate systems, and all expensive protection tools and systems would be in vain. A comprehensive approach to information security is the best starting point for protecting any corporate information system from attackers.

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.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com