NETWORK PERIMETER LIFE IN PICTURES

Vladimir Lapshin

When discussing information security, we usually divide threats into external and internal ones. External threats mean cyber-attacks on the network perimeter. Hacker attacks are often seen in movies, TV series, and books, with hackers trying to access some network on the other side of the globe, and it can become difficult to distinguish real stories from fiction.

Practice shows that network perimeter security was and still remains an important issue. Many companies suffer from network intrusions as the perimeter can be accessed by both good and bad actors.

Some companies try to audit their network security themselves, while others hire special agencies. Hackers also check network security of companies, and then companies have to investigate how their intranet was intruded. Our specialists perform audits of the network security and investigate unauthorized network access.

Mass media have published statistics regarding this issue, and our own findings are not optimistic. Both companies with advanced IT security, and companies with limited resources are being hacked. Based on our pentesting experience, 99% of network perimeters can be overcome. We also assume that 1% of companies have some perfect protection system, which is unhackable.

Everybody who knows something about information technologies or cyber security has his idea of hacker attacks. However, it is difficult to determine what should be done to prevent successful attacks on the network perimeter. In this article, we will give recommendations on what can be done and what should be done.

This article is based on research conducted for companies with advanced information security practices related to network perimeter protection, i.e. for companies where the following is implemented:

+ Asset inventory
+ Threat and asset ranking
+ Vulnerability and software updating management

The asset inventory means that information about systems of the network perimeter is available, this information complies with the real configuration, and the purpose of these systems is justified.

Analysis of the research results confirmed that corporate networks had skeletons in their closets, as half of the incidents related to undocumented systems. Nobody knew about those systems, nobody knew the purpose of those systems, and nobody knew how and why those systems were implemented in the network perimeter.

Ranking means threat assessment with respect to the system elements. It allows testers to rank vulnerabilities depending on their severity and vulnerable elements, and is useful when evaluating large network perimeters.

Vulnerability and software updating management means a procedure to be followed when eliminating vulnerabilities. It also includes documentation specifying acceptable risks and the responsibilities of the divisions and work groups involved.

Companies not compliant with the above were not included in the research, as the security level of such companies was low and discovered vulnerabilities were not fixed. Based on our assessment, 40% of such systems will be vulnerable, and 30% of services will pose a threat.

OUR PARTICIPANTS

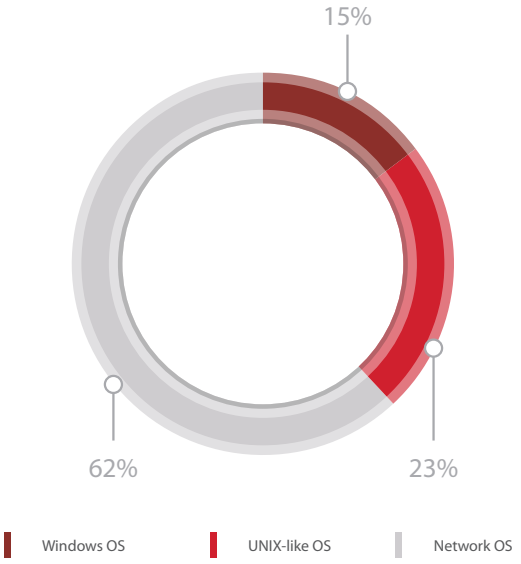
Network security was assessed in 10 organizations (one of them is Positive Technologies and the rest will remain anonymous). The address space included in the research included 130,000 unique IPs. New scanning methods developed by Positive Technologies were used in the research. The given range was scanned on a regular basis at least once a week to obtain the dynamics of change, but that imposed significant timing constraints on scanning.

The research occurred over a two-year period from 2014 through 2015.

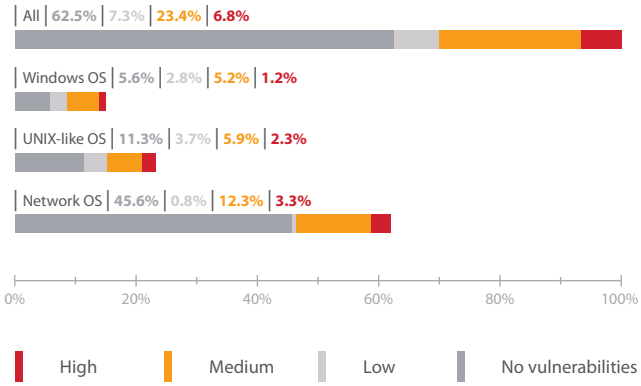
YOUR VULNERABLE MAJESTY…

The specified IP range was scanned regularly during the research. About 10,000 IPs (7.7% of the selected range) were available permanently and the rest were not in use or access to them was restricted by firewalls, and the research uncovered around 15,000 vulnerabilities.

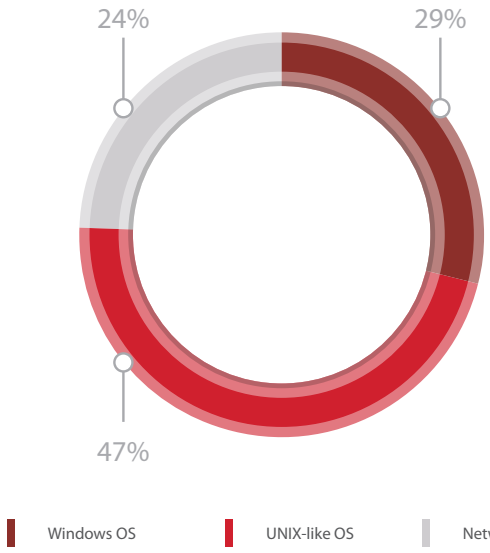
Operating systems detected during the research are into the following groups:

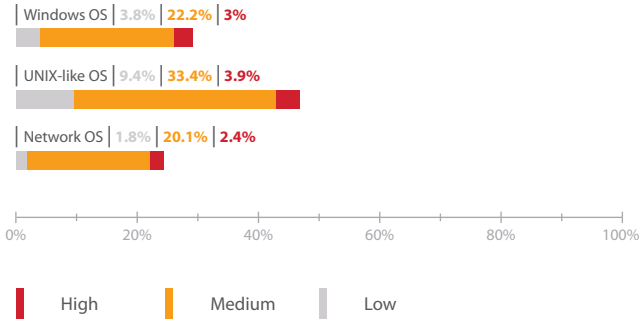


37% of the systems were vulnerable. 7% of them contained vulnerabilities with High severity ratings (based on CVSS scores), 23% contained vulnerabilities with Medium severity ratings. If we include the results of banner checks, the results are worse.



Discovered vulnerabilities with respect to operating systems are shown in the diagram below.





The key results are:

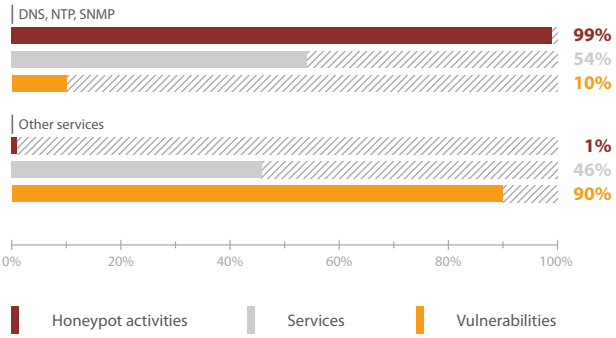
+ The most widespread network operating systems contained the least number of vulnerabilities, around 25% of the total number.
+ UNIX-like systems contained the largest number of vulnerabilities, i.e. more than 45% of the total number.
+ Windows operating systems contained around 30% of the discovered vulnerabilities.

Correlation between the number of discovered vulnerabilities and operating systems shows that software-updating approaches depend on the OS type. This should be taken into consideration when improving efficiency of the cyber security management.

HACKERS' PETS

In the course of the research, we tried to identify services most popular among hackers and tried to correlate vulnerabilities with cyber-attack contexts. For this purpose, we used PT MultiScanner with Honeypot functions and we deployed it in the Internet in our address space along with actual systems.

As a rule, these systems should have no activities as they have no actual services and are not parts of any information system. However, within the first month of our experiment we detected multiple activities on them. Most of the activity related to usage of DNS, NTP, and SNMP services. We analyzed the sniffed traffic and saw explicit attempts to use our services for DDoS attacks. These attempts formed 99% of all registered events. Such results were predictable as DDoS attacks are profitable, attack methods are simple and available, the number of vulnerable services is more than 50% of the total number, and they contain around 10% of all vulnerabilities.



The rest of the services made up only 1% of the activities in the research.

We divided these services into 7 classes:

+ Critical services
+ Infrastructure services
+ Control interfaces
+ Viruses and backdoors
+ WEB services
+ DBMS
+ SIP

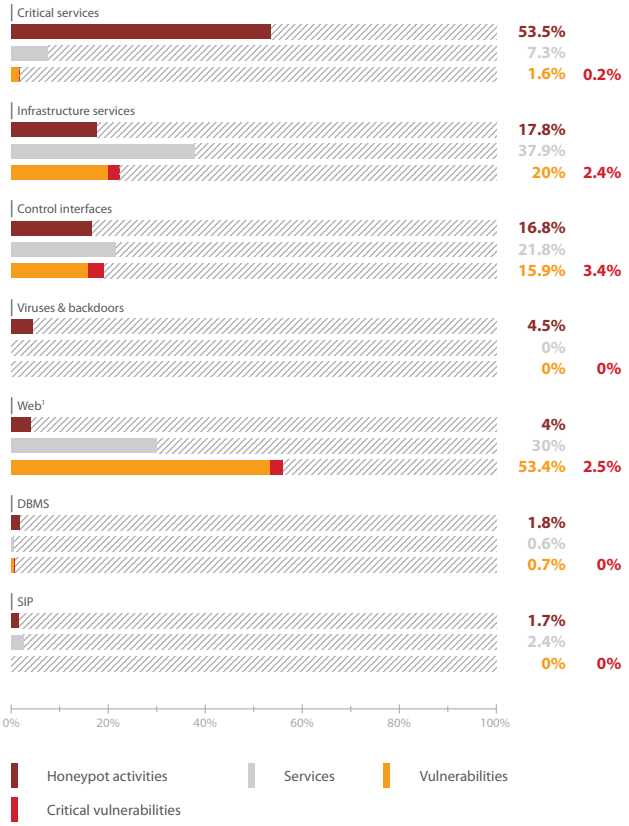
Services are considered critical if they pose vital cyber risks when deployed on the network perimeter, e.g. services providing access to the file system, RPC services, directory services, printers, service interfaces of virtualization systems, etc.

Infrastructure services include VPN services, email services, proxies, customized services, network services, BGP routers.

Control interfaces include Telnet, SSH, RDP, VNC, etc.

Other classes are self-explanatory.

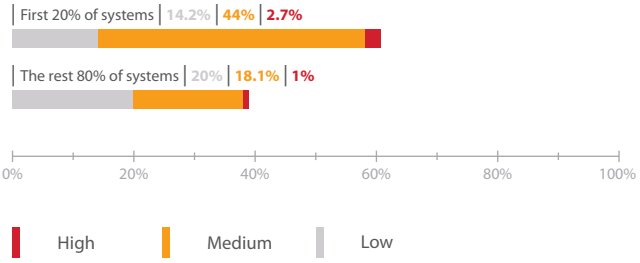
Analysis of the information from detected services, vulnerabilities and network activities shows that network infrastructures are very popular among hackers.



STATISTICS VS DYNAMICS. IN SEARCH OF TRUTH

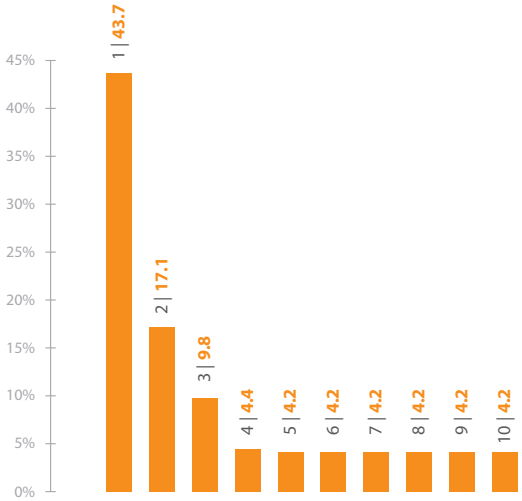
It is important to check the Pareto principle with respect to vulnerabilities, i.e. 20% of most vulnerable systems contain 80% of all vulnerabilities.

We analyzed scans of vulnerable systems for a random date and sorted them in descending order with respect to the number of discovered vulnerabilities:



The first 20% of systems were the most vulnerable ones; they contained around 60% of all vulnerabilities. These systems contained the most part of vulnerabilities with High and Medium severity ratings, two thirds of vulnerabilities with High severity ratings, and around the same number of vulnerabilities with Medium severity ratings.

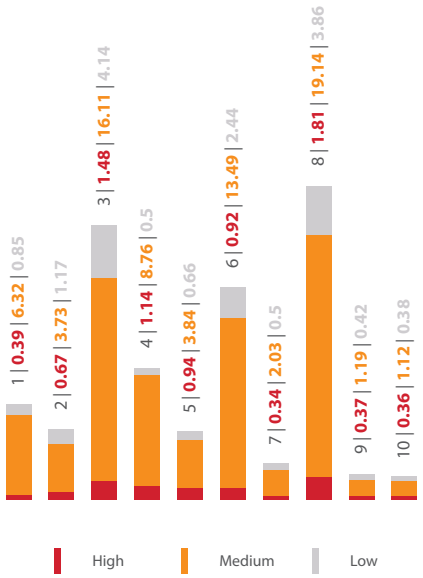
The Pareto principle did not hold true in this case. We divided these systems into 10 equal groups, calculated vulnerabilities for each group and plotted the following diagram.



The diagram above demonstrates that the first 30% of systems contain the majority of vulnerabilities. The rest of vulnerabilities are distributed uniformly among the rest of the systems.

These results give static presentation of a system for a random date. However, it is unclear if this is sufficient for appropriate cyber security assessment of the network perimeter.

To determine changes occurring in the network perimeter we divided the research period into 10 equal intervals. For each interval, we analyzed the number of new services and vulnerabilities. The results show that the perimeter was changing continuously.

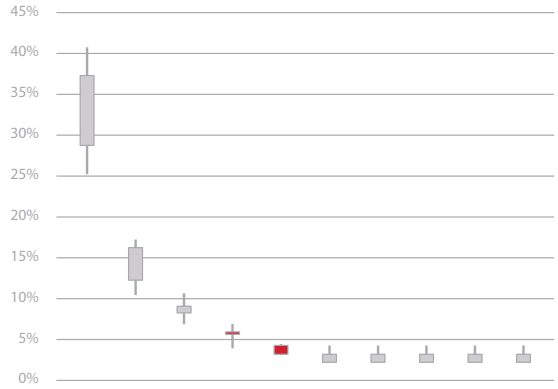


[1] A small number of attacks on web services is due to absence of web sites on Honeypots, the server just established connections and returned no content. We register much more malicious activities on actual web sites protected with the PT AF.

Thus, static distribution of vulnerabilities cannot be used.

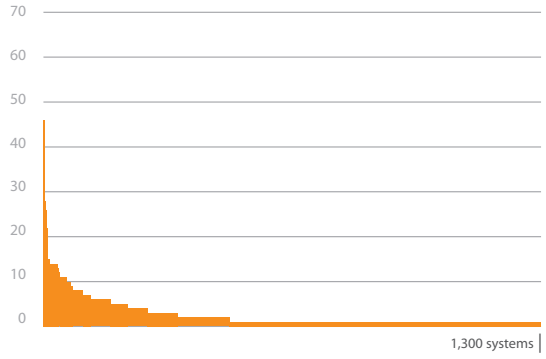
The best format to demonstrate changes with respect to time came from the financial sector in the form of Japanese candlesticks. Candlesticks are composed of the body representing the initial and final amounts of vulnerabilities for a given interval, and wicks showing the minimum and maximum amount of vulnerabilities for this interval. The fewer number of values the better. A gray candlestick means a decrease of vulnerabilities, a red one means an increase in vulnerabilities.

These results confirm our assumption that 30% of the most vulnerable systems contain the largest amount of vulnerabilities.

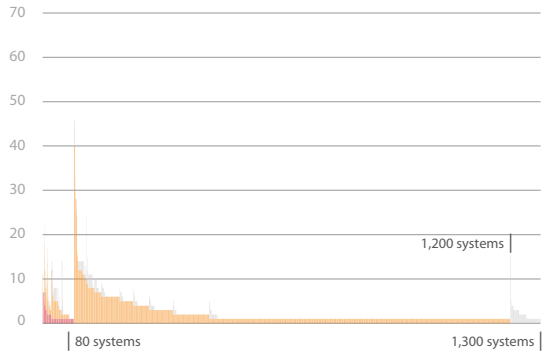


THE DOORS ARE OPEN, LET'S WALK THROUGH?

The first interval included around 1,300 vulnerable systems. Distribution of vulnerabilities in these systems is shown in the chart below.



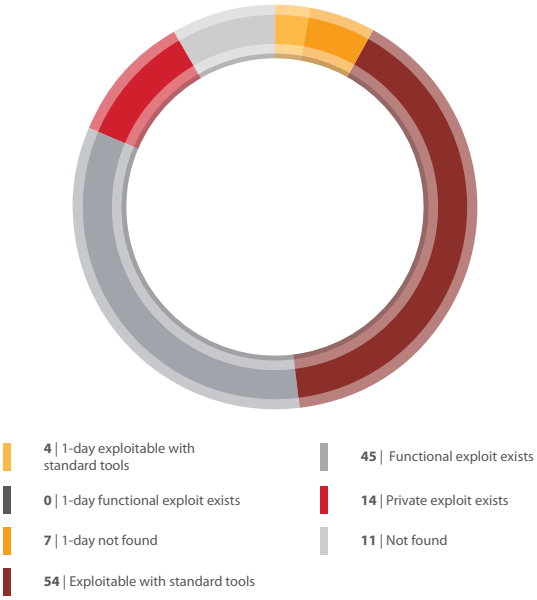
To determine the most vulnerable systems, we differentiated vulnerabilities based on their CVSS scores and sorted them with respect to their severity ratings marked with red, orange and gray colors.



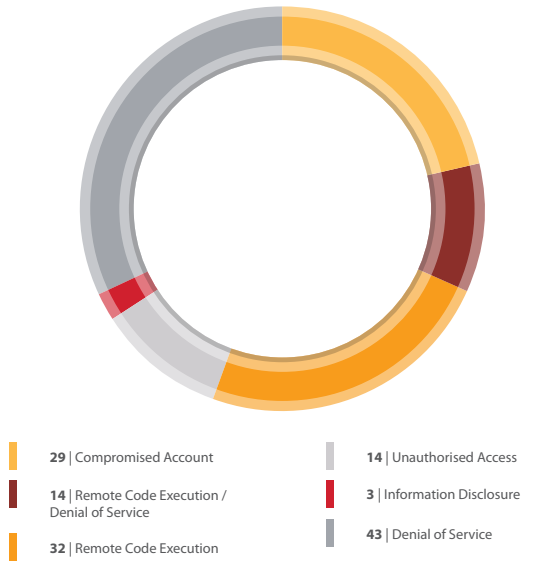
Eighty systems out of 1,300 vulnerable systems contained vulnerabilities with High severity ratings. One fourth of these systems contained more than one vulnerability with High severity rating. We considered this segment most risky, thus correlated it with the information about vulnerability exploitation from the PT knowledge base.

After correlation, we had the following:

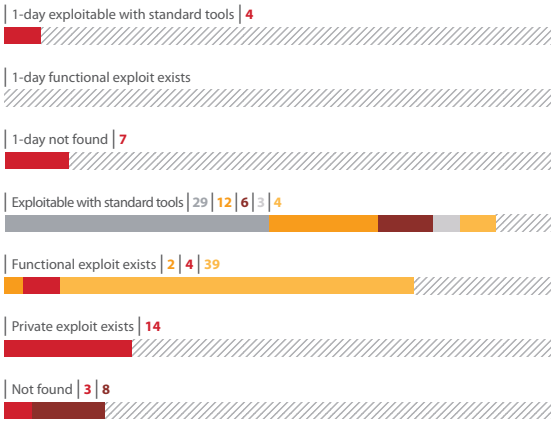
1. Availability of exploits:



2. Vulnerability impact type:



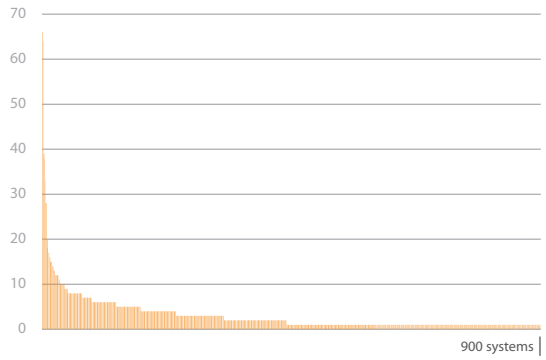
Severity of vulnerabilities at the beginning of the research was high. Exploits were available publicly for more than half of the vulnerabilities. One fourth of vulnerabilities allowed remote code execution (RCE). Thirty-six exploits were found for 46 RCE vulnerabilities. Six of them could be exploited using publicly available ready-to-use tools, and sixteen of them could be exploited using standard pentesting tools.



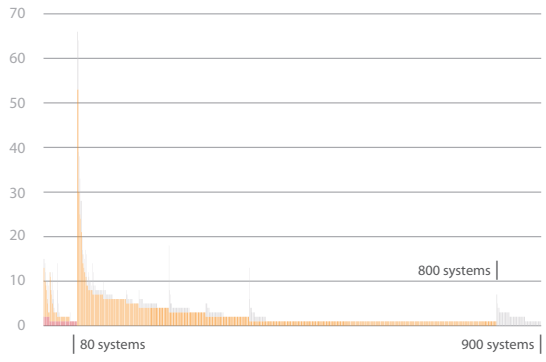
Access complexity of such vulnerabilities is low, i.e. an attacker would need only basic knowledge and Metasploit software to successfully exploit the vulnerability.

There was an interval where 1,700 systems were vulnerable, 120 out of them contained vulnerabilities with high severity ratings.

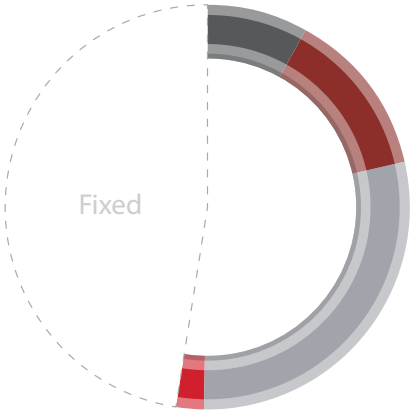
Cyber security enhancements reduced the number of vulnerable systems to 900 systems by the end of the research.



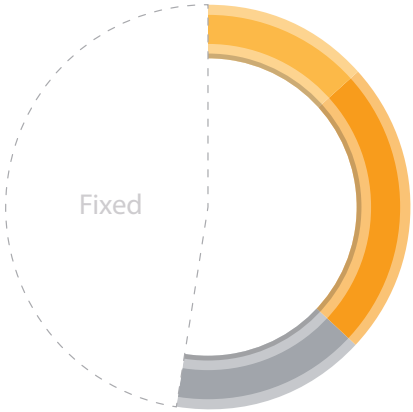
Systems containing more than two vulnerabilities with high severity rating were patched, i.e. only new vulnerabilities were present.

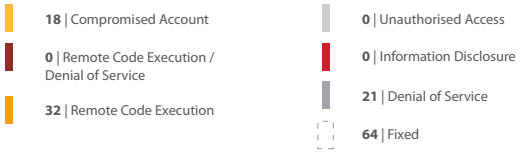


Exploit availability for these vulnerabilities is shown below.



Vulnerability impact type:



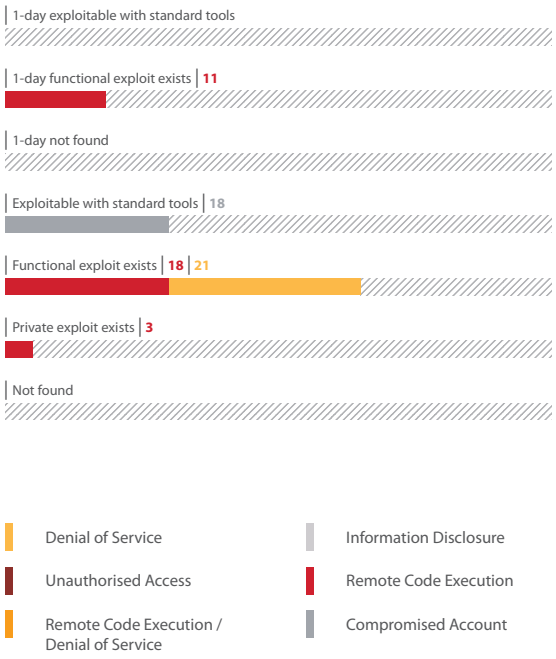


A comparison of the results shows that there are still 32 RCE vulnerabilities with ready-to-use exploits. Twenty-nine vulnerabilities of the above have high severity rating, as exploits for them are available publicly.

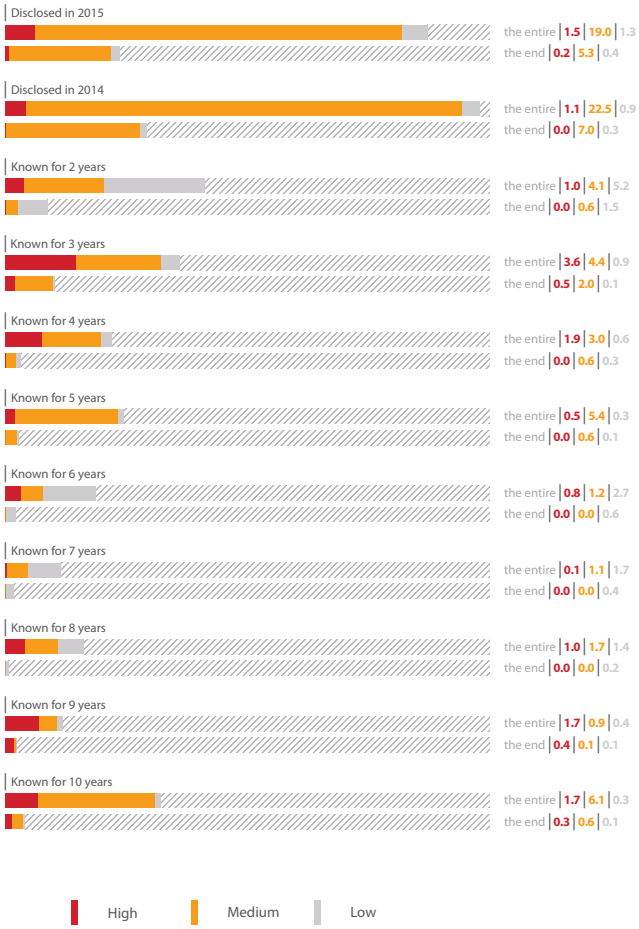
STRIKING A BALANCE

This section describes other factors increasing the risk of vulnerability exploitation and presents correlation of these factors with the above results.

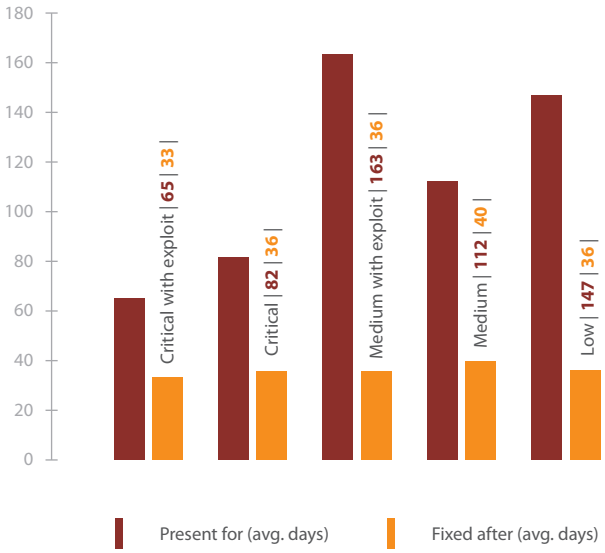
According to a Verizon report issued in 2015 (*www.verizonenterprise.com/DBIR/2015/*) 99% of successful attacks were conducted using vulnerabilities that were over a year old. Based on our research the number of such vulnerabilities discovered



in network perimeters was significant, and while half of the vulnerabilities were disclosed during the research, the remainder had been known for more than two years. The diagram below displays vulnerabilities for the entire research period (in the top columns) and vulnerabilities at the end of the research (in the bottom columns).



The longer vulnerabilities are known the greater the probability of their exploitation. According to Verizon, if an exploit exists then there is a 50% probability that it will be exploited in the first month and a 100% probability that it will be exploited in the first 12 months. Thus, the duration of the vulnerability presence in the network perimeter is crucial. In our research, this factor was considered separately for systems, which had no updates, and for systems, that received regular updates.



The red bars show an average period for which vulnerabilities were present in the network perimeter. Critical vulnerabilities were present for 60 to 80 days. Vulnerabilities, discovered more than 12 months ago and patched were present in 5% of the systems. This value is not large, but cyber security of the system is as strong as only its weakest link.

The green bars show the average period after which vulnerabilities were patched/fixed. This value was around 30 to 40 days for all severity ratings. We consider this value acceptable, as systems in the network perimeter should stay available and all updates should be tested properly before implementation.

GOING FORWARD

Internal analysis of the system does not reflect actual cyber security of the network perimeter. Thus, it is impossible to create an effective cyber security system, as the previously discussed measures will not be relevant to current conditions.

Implementation of cyber security management may take a lot of time and effort, but it should enhance cyber security of the company as well. Collecting information about the network perimeter may discover new methods of cyber risks management. To create an effective cyber security system, we should know what to protect and what to prevent.

The first steps in this direction require minimum investment, e.g. through open source utilities. For help in setting up and upgrading your tools, you may contact specialists from Positive Technologies.