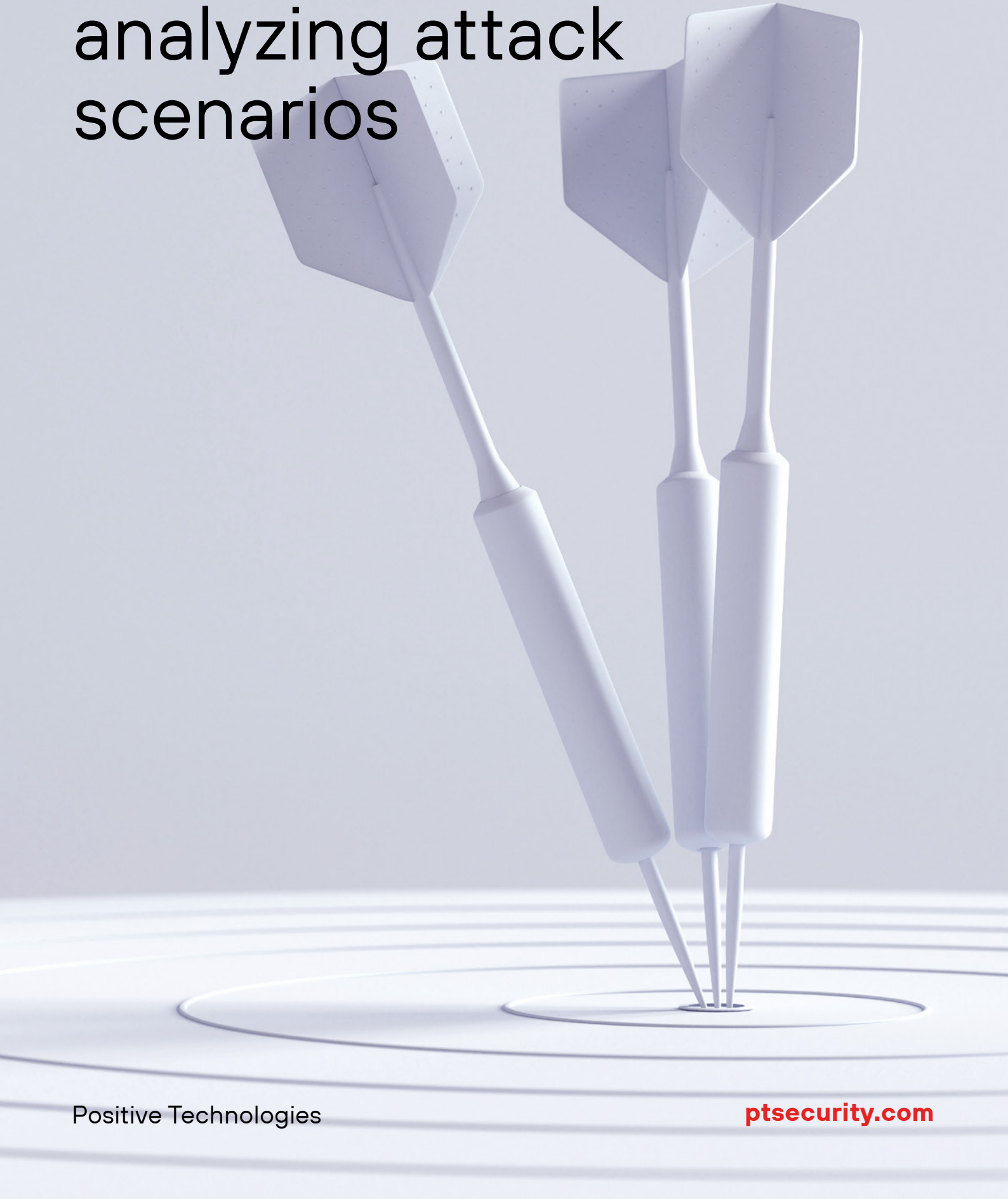
Business in the crosshairs: analyzing attack scenarios



Positive Technologies

ptsecurity.com

An attacker may not know your infrastructure, yet have a plan to move through it before penetrating your network

When speaking about IT infrastructure security, we mean the security of the information systems that make up that infrastructure. But when it comes to corporate security, we primarily have in mind the security of the business: its uninterrupted operation, resistance to external factors, maintaining and growing its reputation and customer base. In these uncertain times, organizations face not only economics-related risk factors. Another potential cause of downtime and failure to achieve strategic goals comes from cyberattacks. For any company, it is possible to draw up a list of unacceptable events which, if they occurred, would have a catastrophic effect on operations. Such events, and how to prevent them, are the topic of this article.

Because companies' business processes are intertwined, the same information systems can be involved in multiple processes. One employee can use several IT systems and perform unrelated tasks. The desire for uninterrupted business operation means that employees need access to all systems and services from anywhere. This, in turn, leads to a more complex infrastructure, making it harder to control resources and access to them. For a successful attack, an intruder does not need to study the company's network in detail: it is enough to gain access to one key system, then expand the attack to several target systems, where the unacceptable event directly occurs.

An **unacceptable event** is one that occurs as a result of cybercriminal activity, making it impossible to achieve operational and strategic goals or leading to long-term disruption of core operations.

A **target system** is an information system whose compromise could lead directly to an unacceptable event for the business.

A **key system** is an information system that an intruder needs to compromise in order to develop an attack on a target system, or a system whose compromise would greatly simplify the scenario for attacking target systems.

For instance, maximum privileges in the domain can allow a cybercriminal to gain access not only to the chief accountant's computer (and hence to 1C, the client bank and important accounting documents), but also to the CEO's and the ICS operator's.

Our study is based on data obtained during information systems security assessment from the perspective of external and internal attackers in H2 2020–H1 2021. In one in three projects, before work got underway, the client specified the systems for which certain attack capabilities needed to be checked. In some cases, our experts simulated APT attack scenarios, applied social engineering techniques, and evaluated countermeasures by information security services in response to pentest actions with a view to eliciting which unacceptable events attackers can actualize and the company's response capability to emerging incidents.

We outline the most common attack penetration and development techniques against the target system, and discuss bottlenecks in the infrastructure that need to be factored in when building the protection system. You will learn what measures to take to prevent the occurrence of impactful events on business.

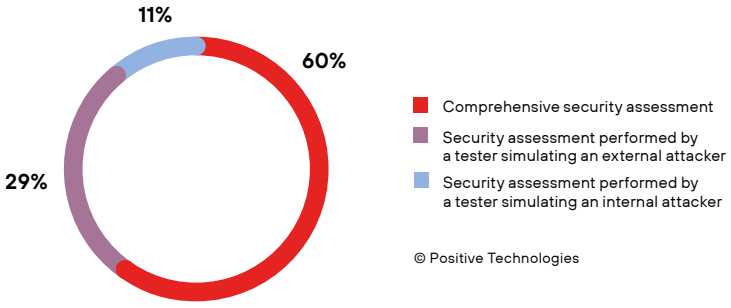


Figure 1. Security assessment format (share of projects)

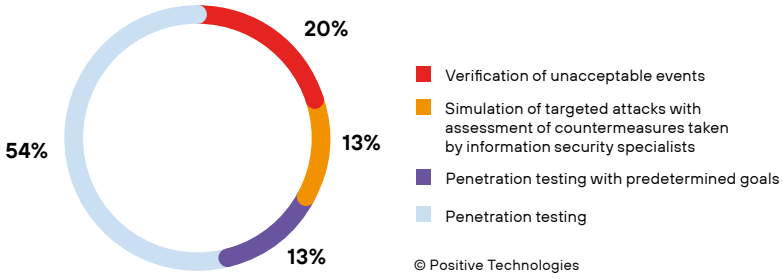


Figure 2. Types of work (share of projects)

1 The study encompassed 45 projects; in each case, the client consented to the results being analyzed and published in anonymized form.

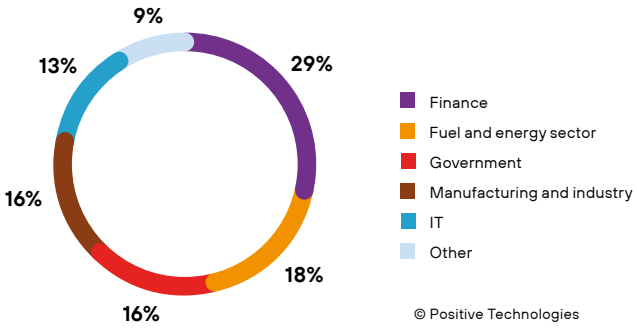


Figure 3. Distribution of companies by industry

Most often, companies are asked to evaluate the feasibility of the following categories of unacceptable events[2]:

- Disruption of production processes
- Disruption of service delivery processes
- Compromise of the digital identity of top management
- Theft of funds
- Theft of sensitive information
- Fraud against users

71%

of unacceptable events can be actualized by attackers within one month[3]

93%

is the share of companies where an external attacker is able to breach the network perimeter and gain access to local network resources

87%

of unacceptable events can be actualized at industrial companies

In 100%

of companies, an internal attacker can gain full control over the infrastructure

At every bank

actions disrupting business processes and impacting quality of service can be carried out

In 100%

of companies, maximum domain privileges allow access to other key systems

2 Unacceptable events were described individually for each company with values of unacceptable damage. For the purposes of the study, we grouped such events into the categories listed.

3 Estimated on the basis of projects for verification of unacceptable events.

How attackers achieve their aims

In verification projects, companies, on average, identified six unacceptable events to be actualized. According to our clients, the greatest danger for them comes from events related to disruption of production and service delivery processes and theft of funds and sensitive information. In 71 percent of the identified events, it was possible to confirm the feasibility[4]. Note that to carry out an attack leading to an unacceptable event, the cybercriminal would need no more than a month. On some systems, attacks can unfold even in a matter of days. For instance, at one company, just two days after the corporate network was penetrated, Positive Technologies demonstrated how it was feasible to steal the personal data of millions of users. Although financial institutions are considered among the most protected, during verification of unacceptable events, actions disrupting business processes and impacting quality of service could be performed at every bank. For example, access was gained to the ATM management system, potentially leading to theft of funds.

4 Unacceptable events are verified according to predefined criteria. The task is carried out in the real infrastructure of the company, and is terminated one step before the onset of an unacceptable event without harming business processes.

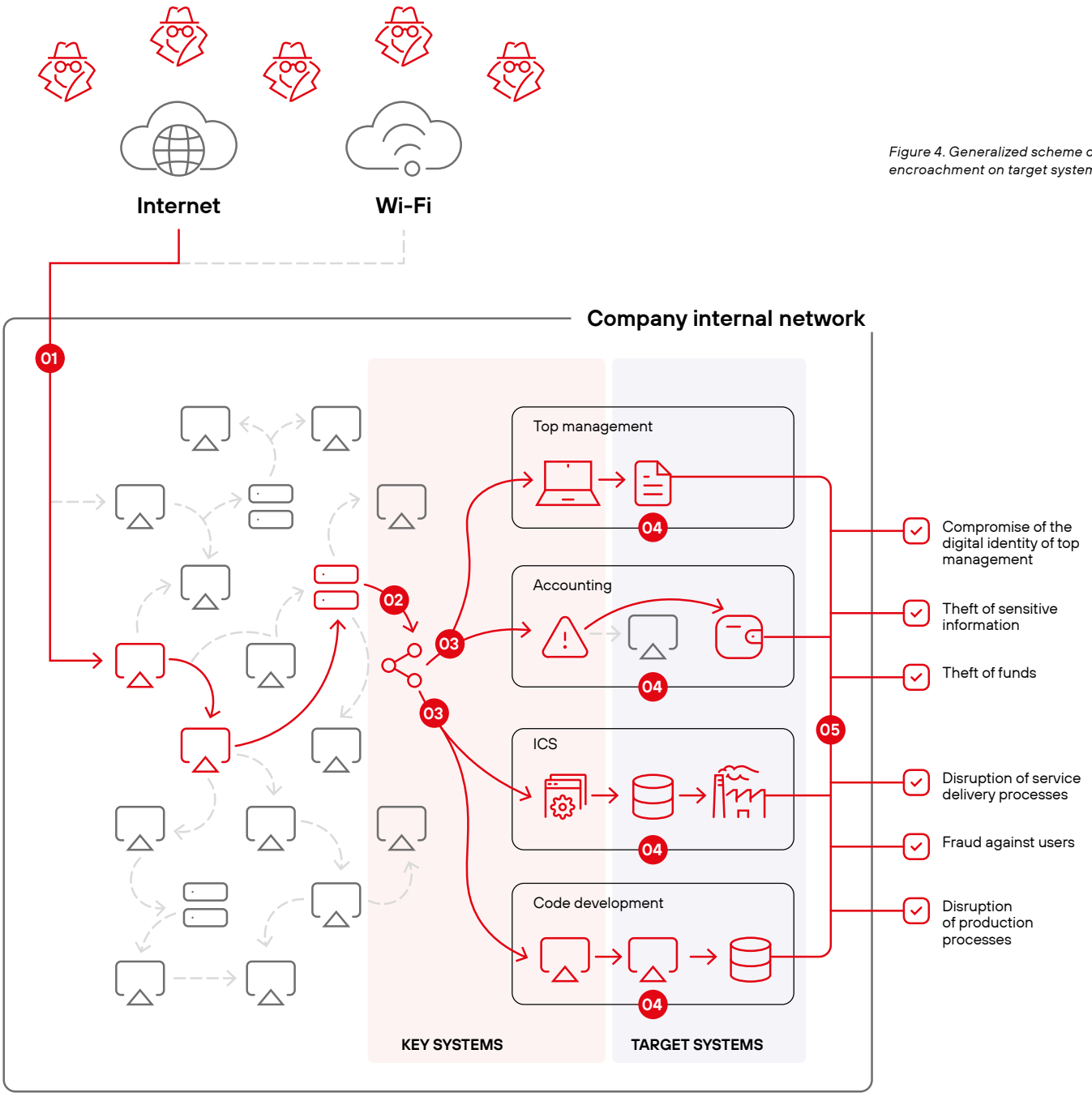


Figure 4. Generalized scheme of encroachment on target systems

Key systems whose compromise allows attackers to develop an attack and trigger an unacceptable event on a target system

Target systems whose compromise can lead directly to an unacceptable event

01 Breaching the network perimeter

02 Obtaining maximum privileges on domain infrastructure

03 Obtaining access to key network segments, including key computers and servers

04 Developing the attack on target systems

05 Actuating unacceptable events

→ Attack vector

→ Potential attack vector

Step 1 — Overcoming the network perimeter

The attacker's path from an external network to the target systems begins by breaching the network perimeter. On average, it takes **two days to penetrate a company's internal network**.

During security assessment from the perspective of an external attacker, carried out in H2 2020–H1 2021, Positive Technologies **succeeded in breaching the network perimeter in 93 percent of projects** even without social engineering. This figure has remained consistently high for many years, which confirms that cybercriminals are capable of picking the lock of almost any corporate infrastructure. During this work, Positive Technologies rarely employs social engineering, only in the case of simulating targeted attacks. However, according to our cyberthreat statistics, attacks using social engineering in reality rank first among corporate network penetration methods, accounting for 57 percent of all attacks on companies.

As for attacks that compromise systems at the network perimeter, the main method of penetrating the corporate infrastructure is credential compromise. This is primarily because employees like to set simple passwords, including for system administration accounts.

The use of outdated software versions and insecure protocols allows cybercriminals to exploit known vulnerabilities to breach the network perimeter. We have already shared the automated security assessment, which highlighted vulnerabilities found in the services of Internet-facing companies.

Based on the results of the security assessment from the perspective of an external attacker, exploitation of known vulnerabilities in software (60% of projects) and in the code of web applications (43%) was what enabled our experts to penetrate the corporate network. Among the vulnerabilities exploited were:

- Remote code execution (CVE-2020-0688) on an Internet-facing Microsoft Exchange server
- Directory traversal (CVE-2020-3452) and Information disclosure (CVE-2020-3259) in the web interface of Cisco Adaptive Security Device Manager (ASDM)[5]
- Remote code execution (CVE-2020-1147) in Microsoft SharePoint
- Remote execution of OS commands (CVE-2019-19781) in Citrix NetScaler[6]
- Remote code execution (CVE-2015-8562) in CMS Joomla

Several methods of penetrating a local network from the Internet could be used simultaneously in one project. The average number of local network penetration vectors per project is 3; the maximum is 19.

5 Vulnerabilities discovered by Positive Technologies, https://www.ptsecurity.com/ww-en/about/news/cisco-fixes-vulnerabilities-in-asa-firewall-found-by-positive-technologies/

6 Vulnerabilities discovered by Positive Technologies, https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies/

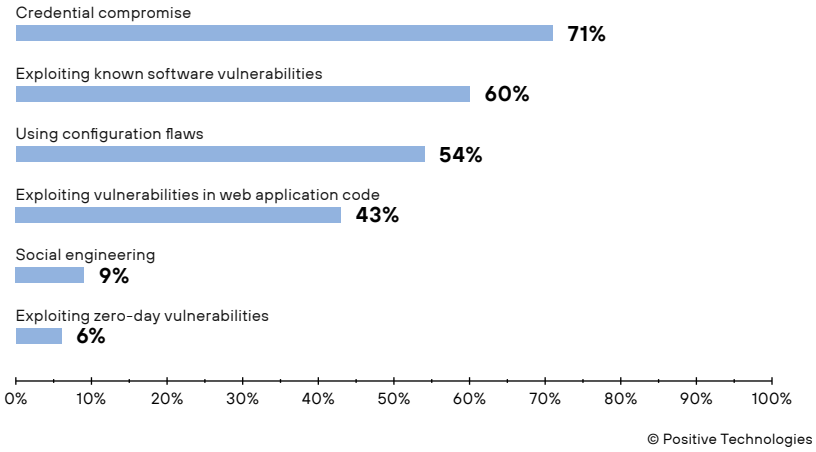


Figure 5. Local network penetration methods (share of companies)

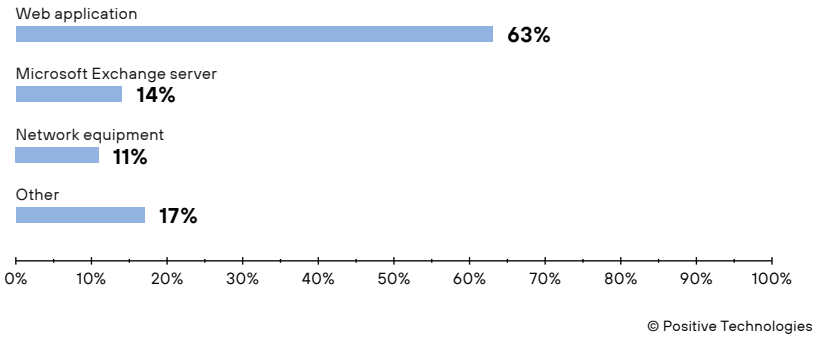


Figure 6. Corporate network penetration points (share of companies)

Step 2 Getting maximum privileges

In **100 percent** of companies, an internal attacker can gain **full control over the infrastructure**, while in 81 percent of companies there exists a simple way to gain domain administrator privileges, which even a low-skilled attacker can manage. Note that this trend continues year on year: in 2019 it was also possible to gain full control over the infrastructure in all companies. Domain administrator privileges are not always required to actualize an unacceptable event, but having them greatly simplifies attack development. Our study shows that maximum domain privileges can be used to gain access to other key systems in 100 percent of cases.

An attacker with credentials and domain administrator privileges could obtain many other credentials to move laterally in the corporate network and gain access to computers and servers. Most companies lack network segmentation by business process, which allows several attack vectors to be developed to the point of multiple unacceptable events occurring simultaneously. If a company has built trust relationships between domains or reuses administrator credentials, an attacker can gain control over other corporate domains and further develop an attack from there. The **maximum number of controlled domains** within one company, obtained during security assessment from the perspective of an internal attacker, is **10**.

We have already talked about attack development scenarios within the corporate infrastructure, including recommendations on how to identify an attacker at different stages of movement through the network, so we will not go into details here.

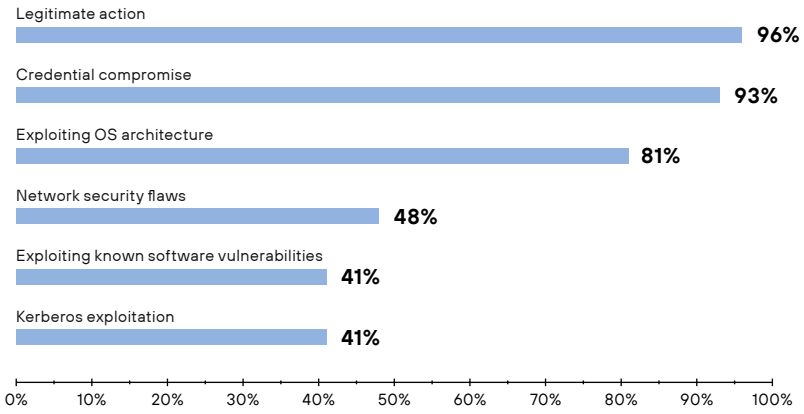


Figure 7. Successful attacks inside the network (share of companies)

In most internal network attacks, cybercriminals prefer to make use of architectural features of the operating system and authentication protocols, and to perform other legitimate actions that do not differ from the usual activity of users or administrators so as to remain under the radar.

In 40 percent of companies, our experts exploited software vulnerabilities[7] that, in most cases, could be used to escalate privileges in the system, for example:

- a critical vulnerability in the Netlogon protocol (CVE-2020-1472) that allows privilege escalation to the level of domain administrator, listed as one of the most exploited vulnerabilities of 2020, according to the US Cybersecurity and Infrastructure Security Agency (CISA);
- the PrintNightmare vulnerability in Windows Print Spooler (CVE-2021-34527), which makes it possible to execute arbitrary code remotely, view, modify, or delete data, and create new accounts with user rights.

7 Since penetration testing and simulation of targeted cyberattacks are carried out using the black-box method, software vulnerabilities may not be exploited in attacks if a simpler or more covert compromise option exists, yet be present in all systems examined.

Step 3 — Gaining access to key systems

Before reaching the target system, an attacker has to perform several steps in sequence. In some companies, the required level of access is provided by domain administrator privileges (in which case the domain controller is the key system on the path to actualizing an unacceptable event); in others, the attack chain is longer and more key systems need to be compromised.

The task of gaining access to isolated network segments, key computers, and servers is often facilitated by administrative, virtualization, protection, or monitoring tools. These systems are also important for attackers because through them they can act stealthily under the guise of legitimate users without creating additional suspicious connections, as well as execute commands with high privileges. The main problem is that such systems:

- Store information about the infrastructure (devices, IP addresses, active services, software used).
- Allow remote control of devices (including remote code execution on agents).
- Have a distributed architecture (web interface, databases, server, agents).
- Have preinstalled accounts and use specific ports for connection.
- Can contain vulnerabilities if not updated regularly.

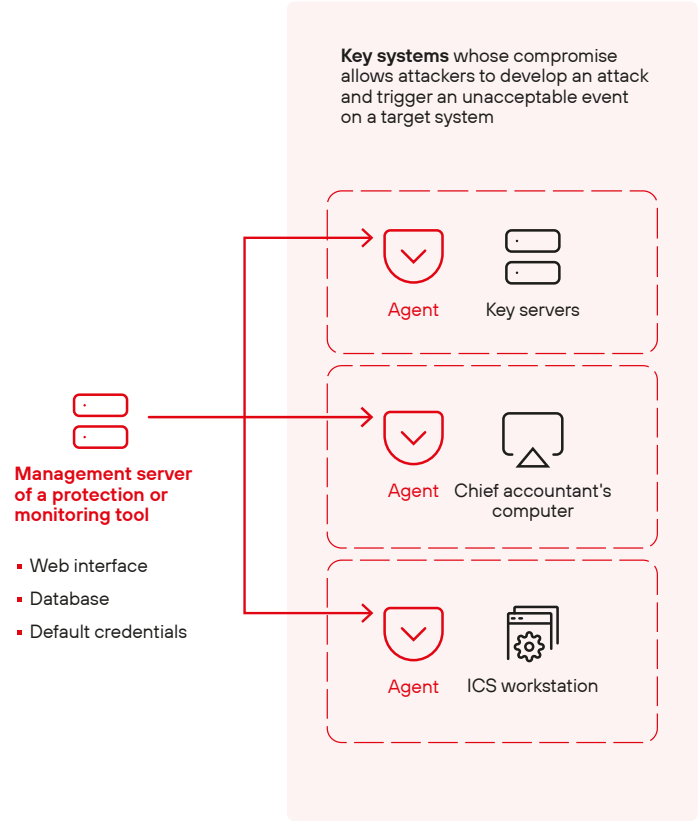


Figure 8. An example of gaining access to key systems through protection and monitoring tools

Steps 4 and 5 — Developing an attack on target systems and actualizing unacceptable events

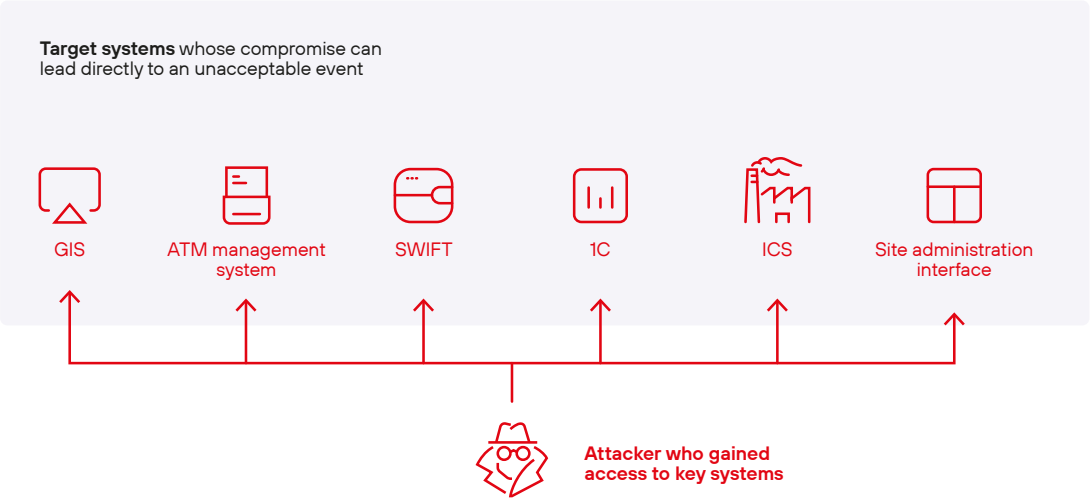


Figure 9. Developing an attack on target systems

Once an intruder has penetrated the industrial network and, say, gained access to the ICS operator's computer, only one step remains before reaching the target system where an unacceptable event can be actualized, such as process disruption or equipment failure. Examples of target systems, depending on the company's field of activity, can be an ICS, a geographical information system, an ATM control system, SWIFT, 1C, an administration site interface, a code development and versioning environment, and so on. **In the industrial and energy sectors, 87 percent of unacceptable events were confirmed as part of verification projects**. The ability to complete this last step and bring the attack to fruition is partly down to employee failure to comply with information security policies. On the computers of 9 out of 10 engineers is a plaintext document listing the systems they use, with a brief description, IP addresses, and login credentials.

In the banking sector, key systems include employee workstations for handling payment systems and ATMs. During verification of unacceptable events at such organizations, our experts were able to gain access to the bank's target systems with privileges for performing banking operations in two out of three companies; at the same time, it was possible to **perform actions disrupting banking processes and impacting quality of service in every bank**. All in all, as part of the verification process within the contracted period, Positive Technologies actualized 62 percent of unacceptable events in banks.

When it comes to an arbitrary commercial organization, in order to steal funds, an attacker needs to get to the company's invoices and bills. In this case, the computers of finance employees can be classified as key systems. If a cybercriminal is interested in the company's databases and business applications, their actions will be aimed at gaining access to—and developing attacks against—the servers.

Due to the interlacing of business processes, the steps performed by an attacker aimed at seemingly different target systems actually occur in parallel. Gaining access to one key system automatically grants access to several target systems. Thus, an attacker who obtains maximum privileges in the domain infrastructure can gain access to the computers of accountants and top executives, or any other corporate systems. During verification at one of the companies, it proved possible to gain access to the 1C: Enterprise system from software developers' computers.

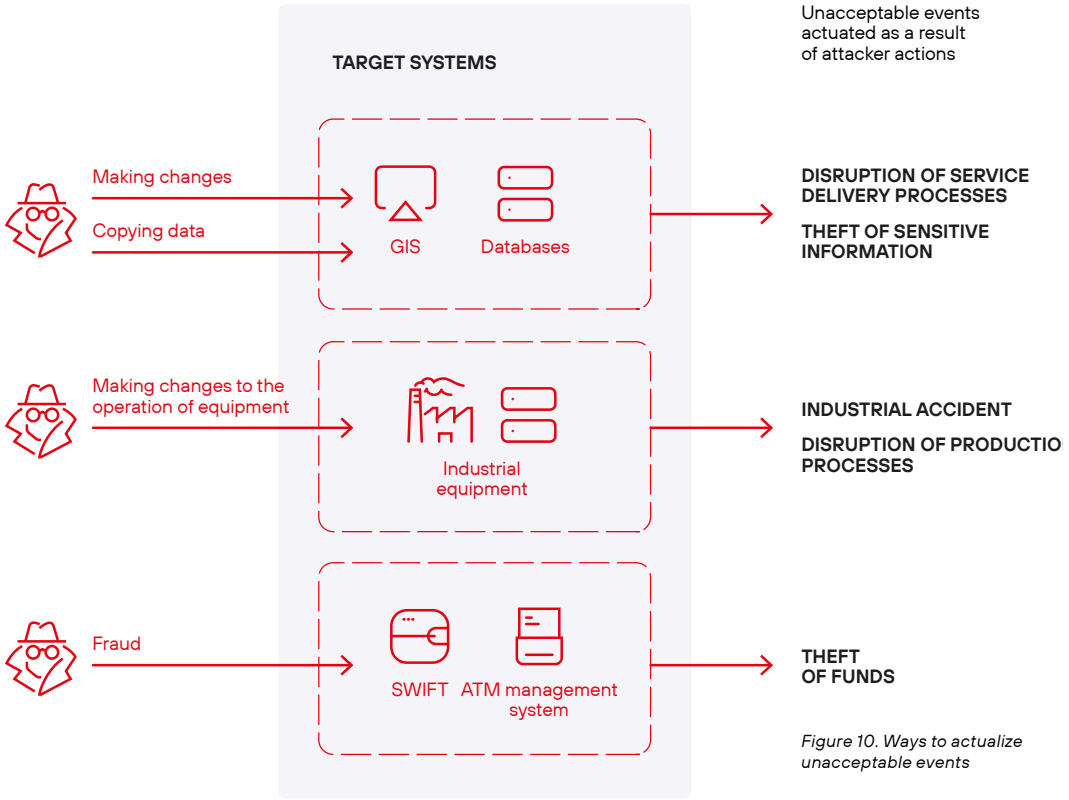


Figure 10. Ways to actualize unacceptable events

How to detect and stop an attack in time

Building an effective corporate protection system requires an understanding of what unacceptable events exist. By tracing the business process path from unacceptable events to target and key systems, we can pin down the relationships and determine the sequence of protection measures to be applied. To make it more difficult for an attacker to move through the corporate network to the target systems, we propose a series of interchangeable and mutually reinforcing measures. The choice of solutions should be based on the company's capabilities and infrastructure.

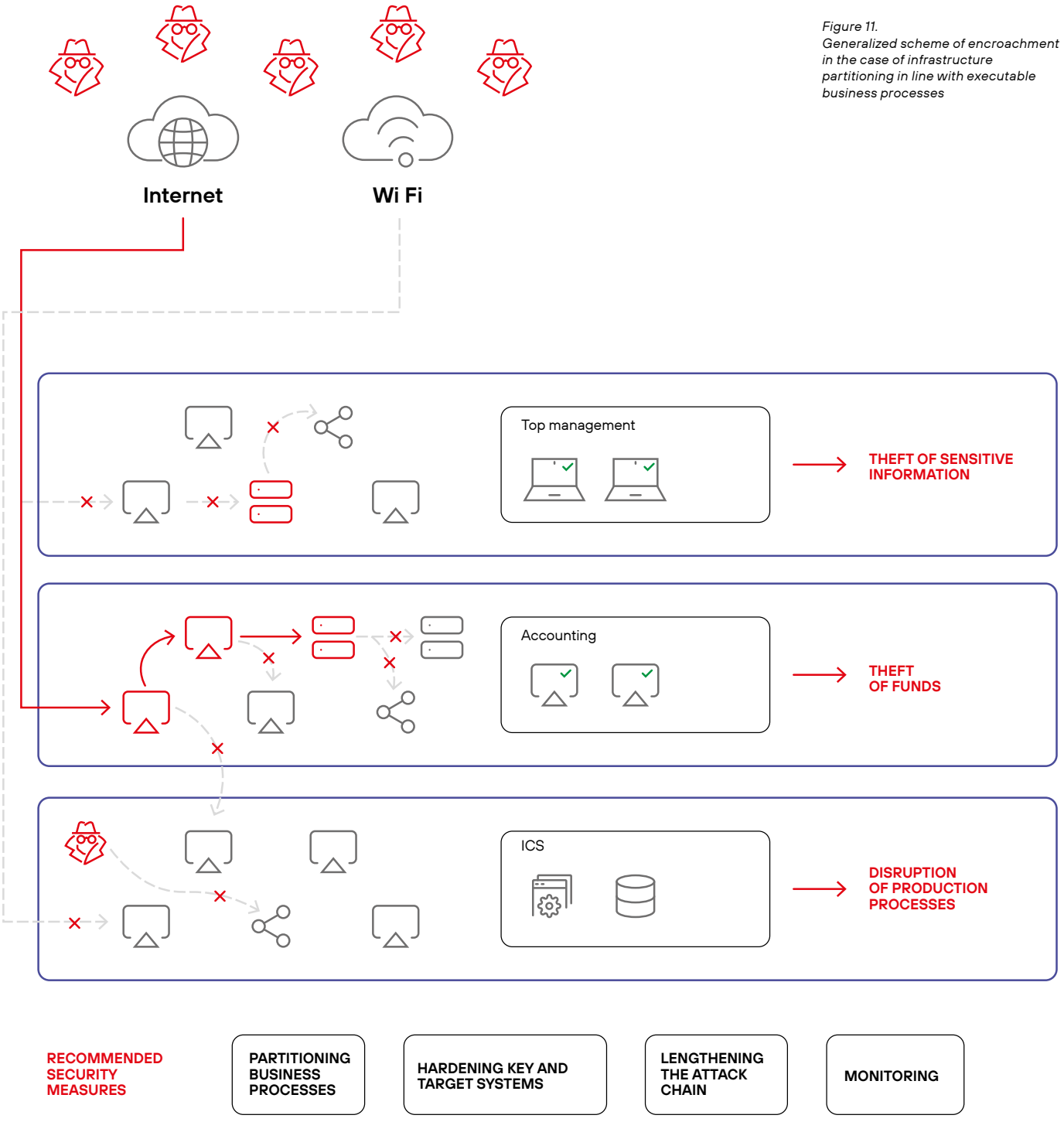


Figure 11.
Generalized scheme of encroachment in the case of infrastructure partitioning in line with executable business processes

1. Partitioning business processes

Building business processes is a complex, resource-intensive task, as is changing ones already implemented. But, as our research shows, when the same key system is involved in multiple business processes at once, it is much easier for an attacker to succeed, because they only need to compromise one system to get to several target ones. We recommend paying special attention to infrastructure components engaged in several business processes at the same time, and checking whether any can be used to actualize events that are unacceptable for the company. Partitioning the most company-critical processes from others can be an effective tool for protecting against the actualization of unacceptable events on a par with other security measures.

2. Configuration security control

To rule out a cyberattack-related unacceptable event, it must be made as hard as possible for an intruder to encroach on the target. The more complex the attack chain leading to the target system, the lower the chances of successful compromise and the higher the chances of cybercriminal error. We recommend paying special attention to the protection of penetration points into the infrastructure from external networks, minimizing their number, and ensuring a high level of security for key and target systems.

Hardening is the process of increasing security through reducing the attack surface and eliminating potential attack vectors (including vulnerabilities, insecure configurations, and weak passwords).

3. Enhanced monitoring

An important protection tool is the monitoring of information security events not only on endpoints, but in network traffic too. Keep in mind that an intruder will seek to simplify the attack vector, look for quick ways to achieve the goal, and adapt their actions to business processes to stay hidden, which means they will attack key systems. Enhanced hardening and advanced monitoring of information security events at penetration points and in key and target systems are effective ways to protect against unacceptable events. Advanced monitoring increases the likelihood of detecting cybercriminal activity even in systems that, for whatever reason, lack enhanced protection measures or the latest updates. It is especially important to enable advanced monitoring of information security events in key systems engaged in multiple critical business processes simultaneously.

4. Lengthening the attack chain

Whether the information security service has time to respond in the event of detecting an attack depends on how far the intruder has to "travel." The shorter the chain, the fewer options the defenders have. To stop an attack in time, before an unacceptable event occurs, it is vital to eliminate the shortest paths from the penetration points to the target system. The attack chain is lengthened by correctly segmenting the networks, adding key systems on the attacker's path, and distancing penetration points from the target system by at least several attack steps.

Each organization's infrastructure is unique. In some companies, a single attack can lead to multiple unacceptable events; elsewhere, an attacker will have to work hard to achieve the objective. By choosing the appropriate balance of proposed measures, organizations can detect and stop attacks in a timely and cost-effective manner, thereby preventing unacceptable events.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays