Practical guide with the underestimated but effective cybersecurity tips

Strengthen your cybersecurity to the necessary level on your own with these simple tips.

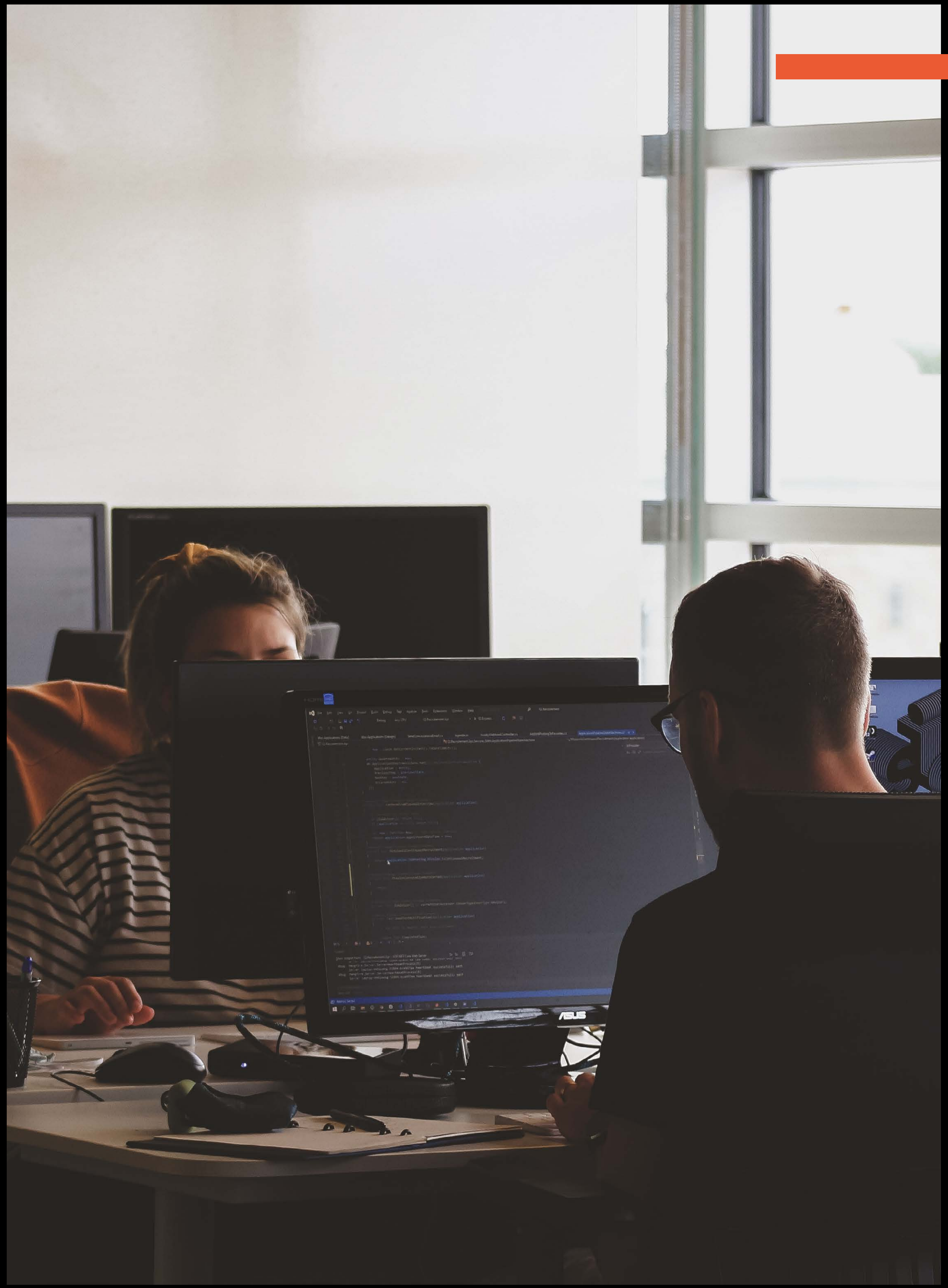
We collected the best basic practices proved by our IT security experts.

**Cybersecurity tips.
Nothing redundant.**

aimpro.soft

YOUR DIGITAL TRANSFORMATION PARTNER

Contents



Today, there are 28.5 billion networked devices in 2022.

Each of them is threatened.

As CTO, you have a voice in decision-making regarding the evolution of the business, you are responsible for the tech advancements of the business as well as the resilience of the software part to threats. Cybersecurity takes a significant portion of your responsibility tasks, more than 80% of your precious time.

At the moment, cybersecurity is one of the most important threats to companies due to COVID-19 and remote circumstances. 78% of security and IT leaders say remote workers are harder to secure. And your organization is under hacker attack every 39 seconds. There are many solutions on the market that are proven and reliable.

Could protection come at a cost?

Understanding your challenges, we have prepared a guide with best practices from Aimprosoft so that you can improve your security with simple and inexpensive methods without extra spending.

Contents

Challenges faced by CTOs in the way of implementing cybersecurity

83% of companies consider not if a data breach will happen but when. *IBM Report

$7 trillion is a predicted amount of a cybercrime world cost in 2022. *Cybersecurity Ventures

15% of growth in costs associated with cybercrimes is expected over the next five years. *Cybersecurity Ventures

The permanent security challenges in any organization are:

- Constantly evolving security threats and attack methods
- Growing opportunities for attacks as data volumes, remote working increase, and digital transactions
- Increased use of cloud computing and IoT entails emerging extra security needs
- Sophisticated and well-funded adversaries
- State-sponsored state-sponsored cyber operations an attacks automation using AI and machine learning Technologies
- Resource limitations (budget, staffing)
- Low cybersecurity awareness among business users

We're Aimprosoft

We've been keeping the clients' valuable data out of foe hands with our DevOps data security strategy.

Get a free consultation

The security challenges, as mentioned above, are usually exposed to certain technical nodes. For each case, we suggest certain actions that will positively affect cybersecurity. We have done them ourselves and recommend them as simple practices you can easily implement in your organization.

Vulnerability 1: External network attacks

$4.24 million
was the average cost of a data breach in 2021.

IBM Security report

It is crucial to assess critically how your company connects to the Internet, how it filters traffic from the Internet to your business, and how it does the same for traffic going the other way.

Boundary firewall

A digital security system commonly used to monitor all incoming and outgoing traffic in your network identify and block unwanted traffic server resource-consumers can accommodate all points of contact. You must have firewalls in place between your office network and the internet at the perimeter of a network.

Packet-filtering firewalls – filter traffic by packets with only header information to determine their safety. They come in two categories: stateful and stateless.

Next-generation firewalls (NGFW) – determine a dangerous connection based on the contents of a packet and the program designated to receive it.

Proxy firewalls – act as intermediaries between the internal user server and the internet, filtering messages at the application layer to protect the network resources.

Network address translation (NAT) firewalls – placed at the router level can stop malicious activity before the data is sent to your private or public IP addresses.

Stateful multilayer inspection (SMLI) firewalls – use holistic data inspection to detect threats and make more manageable the full state of network traffic streams.

Contents

IDS/IPS systems

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents, logging information, and detecting and blocking threats defined individually, according to configured policy.

Open-source IDS/IPS tools

A combo of Snort + Suricata is the most frequent choice of cybersecurity implementors. Snort combines the advantages of the signature-based method with the ability to detect anomalies in real-time. Suricata is designed for multi-threading and allows using methods other than signature-based attack detection, and enables GPUs for calculations in IDS mode and more advanced IPS. There are about 65,000 events that are manually set up and take a long time to get right.

Alternatives: Bro (renamed Zeek), Linux IDS, Sweet Security.

Ready-to-use products

Information systems security products are ready-made events that already contain settings for monitoring, detecting, and responding to malicious activity. These security software platforms, which allow organizations to monitor, visualize, analyze and protect unstructured data, are available by subscription.

Examples: Varonis, SolarWinds Access Rights Manager, Netwrix Auditor, ManageEngine ADAudit Plus, STEALTHbits, Lepide Auditor.

Vulnerability 2: Internal network attacks

30 percent
of data breaches involve internal actors.

Verizon

Networks are complex and diverse, as are the types and severity of threats and attacks against them:
- network compromising by outside users;
- possibility of malicious traffic reaching.

Contents

Broadcast domain split

Subnetting a network allows for avoiding a huge broadcast domain. In modern IPv4 networks, broadcast traffic is necessary. Say you have a network with 65,000 connected devices, so every quantum of time, something broadcast will be sent. By dividing such a network into 256 networks with 254 hosts each, you will get 256 separate broadcast domains and a relatively small (254) number of broadcast traffic sources necessary for normal performance.

Dividing a network into subnets

Segmenting a network into subnets can provide a certain level of security. There are few chances to guarantee traffic control on the local network. As a result, there is a control for MAC addresses on switches, and end devices can be configured in various ways. The best time to perform this centrally is when traffic switches between networks. The router is set up with centralized filtering, so a firewall may also be set up there.

Disabling AutoRun

By disabling software that launches a memory stick automatically, «auto-run» or «auto-play,» you protect network devices from malware. It can be done on Windows through Settings, macOS through System Preferences, and Linux through the settings app for your distribution. Selecting the alternative where users are asked to decide what will happen when they insert a memory stick is appropriate.

Vulnerability 3: Lack of timely software updates

671% is a peak of brute-force attacks fixed in 2021.

Abnormal Security

An organization's risk or exposure to data breaches or cyberattacks can be significantly decreased by having a well-thought-out, workable plan for distributing and applying updates to the software.

Contents

Security and OS update

By installing critical or dangerous security updates for operating systems and firmware, you raise the odds of addressing security vulnerabilities within a program or product in time.

Account security

A distinct username and password are required to access any user or administrator account. No devices should be accessible without a login and password, so make sure they are. Also, accounts can't be shared by users.

Brute-force attack protection

Attempts to discover a password by systematically trying every possible combination of letters, numbers, and symbols averaged 26% of all organizations per week. Password-based authentication, multi-factor authentication, and device unlocking credentials are simple but quite effective secure configuration methods against brute-force attacks anyone can afford.

Vulnerability 4: Bad end-user management

82% of breaches involve human error

Verizon Data Breach Incident Report 2022

The weakest link in cybersecurity must be people. Therefore, businesses should train staff members about the different cybersecurity threats they could encounter to avoid being duped into revealing information that is not intended for distribution.

VPN (Virtual Private Network)

By installing critical or dangerous security updates for operating systems and firmware, you raise the odds of addressing security vulnerabilities within a program or product in time.

Contents

Vulnerability 5: Data loss

236.1 million ransomware attacks worldwide were fixed during the first half of 2022.

Statista

Data loss causes expensive production and productivity loss, which could result in missed deadlines, disgruntled clients or consumers, and lower business margins. It is crucial to have ready-to-use plans to restore lost data or rely on data backups, and disaster recovery systems to maintain ongoing operations.

Backups and contingencies

3 out of 4 cases of data loss are caused by human error, as reported by the IT Policy Compliance Group. The backup practice of copying files or databases to a secondary location (local, cloud, or hybrid) for preservation in case of equipment failure or catastrophe helps maximize uptime and lower costs. Backing up data is pivotal to a successful disaster recovery plan. A cybersecurity contingency plan is a documented course of action that provides instructions, recommendations, and considerations for an organization concerning IT services and data recovery in case of a security breach, disaster, or system disruption.

Vulnerability 6: Limited resources to cope with breaches

$4.35 million is the average cost of a breach, including notification, forensics, legal fees, and fines.

IBM

Due to the ongoing evolution of the threat landscape, businesses of all sizes are exposed to cyber risk. As your company's network grows, fraudsters try to take advantage of gaps in your security measures. Data breaches and cyberattacks are costly and becoming more frequent. A cyberattack can force you out of business in addition to being an inconvenience.

Contents

Cyber liability insurance

Organizations should carry cyber liability insurance to provide some financial means of remedying attacks or breaches if/when they occur, given the rising reliance on technology and data in daily operations and the evolving nature of cyber threats.

A company could need to retain technology forensic specialists to ascertain the type of cyberattack, depending on the severity of the cyberattack, which incurs additional costs. Depending on the consequences, these costs can quickly escalate to hundreds of thousands or even millions of dollars. Determine what types of attacks or breaches you need to cover in order to specify them in your cyber liability insurance policy. Pay attention to the level of specific coverage costs, and that there are types of events that are not covered, as well as conditions that will result in policy withdrawal.

Vulnerability 7: Social engineering

98% of the time, social engineering is used in cyberattacks.

Purplesec

Some of the most effective cyberattacks don't target hardware or software—they target people. Social engineering is a way of obtaining confidential information through psychological influence on a person to benefit through access to passwords and secure systems.

Main types of social engineering:

Pretexting – an attacker works under the pre-compiled scenario by using real requests with the name of the company's employees.

Phishing – an intruder uses a fraud technique aimed at obtaining authorization data of various systems.

Trojan horse – a technique based on users' emotions, making them interact with a disguised malicious program that collects or modifies information by an attacker.

Reverse social engineering – a person-to-person attacker-victim attack to compel the latter into divulging sensitive information.

Contents

Security awareness training

It is imperative that every employee of the organization understands the risks associated with releasing both personally identifiable information and business secrets, as well as how to stop data leaking. Prepare instructions on confidential information and information that can be disclosed to whom and when. Simulating social engineering also attempts to train employees to resist temptation.

Increase spam filtering via email gateways

Cybercriminals frequently use email to conduct social engineering scams. Thus the company must adopt the proper email gateways to mark these scams as spam in your employees' inboxes. Implementing a solid email gateway can avoid up to 99.9% of all spam, which accounts for 45% of all emails, and is primarily socially engineered to compromise computer systems and networks and steal data.

Implement policies for key procedures

As social engineering is designed to deceive humans, antivirus programs, network firewalls, etc., cannot prevent social engineering success. Therefore, implementing appropriate policies when performing work tasks can help reduce the success rate of cyber criminals.

SSL Certification

Data encryption with an SSL certificate from the authorities effectively minimizes the consequences of hackers gaining access to your organization's communications systems. This type of digital certificate provides website authentication and encrypted communication.

Contents

About Aimprosoft

Aimprosoft can ensure the proper cyber security level for our clients against online threats being approved by Cyber Essentials, a UK Government-backed minimum standard scheme that protects against the most common cyber attacks.

Aimprosoft is a software development company that offers a wide range of services for a successful digital transformation. More than 17 years of market presence helped us obtain profound knowledge of product creation and become strong advocates of a customer-centric approach with a deep understanding of our clients' needs. The arsenal of our software engineers encompasses 50 technologies that help them enhance the capabilities of our customers' businesses, increase their revenue, and modernize outdated processes. Apart from a diverse stack of technologies, we also use the capabilities of Liferay, Alfresco, and Hybris platforms that have become our key tools for building enterprise-grade software solutions. Over time, we gained considerable expertise in application development for a wide range of industries, such as Education, e-Commerce, Healthcare, IoT, Real Estate, Retail, Telecom, and many others.

We develop software with care.
Contact us to outsource your development tasks.

67 Halytska Str. Ivano-Frankivsk,
Ukraine, 76019

US+14088444477
UK+4402081444696
UA+38068 675 5774

aimprosoft.com
info@aimprosoft.com