O2 Czech Republic a.s.

Prague, Czech Republic

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT

REPORT ON CONTROLS AT SERVICE ORGANIZATION RELEVANT TO DESCRIPTION OF O2 CZECH REPUBLIC A.S. SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS TO MEET THE CRITERIA FOR THE SECURITY, AVAILABILITY, CONFIDENTIALITY, PROCESSING INTEGRITY AND PRIVACY.

THROUGHOUT THE PERIOD
2023-01-06 THROUGH 2023-30-11

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Scope	O2 Czech Republic a.s. (service in the scope see below)
Period of Examination	June 1, 2023, to November 30, 2023
Applicable Trust Principle(s)	Security, Availability, Confidentiality, Processing Integrity and Privacy
Location (s)	Prague, Czech Republic
Subservice Providers	O2 IT services s.r.o.
Opinion Result	Unqualified

O2 Czech Republic a.s. services in the scope of the report:

- Virtual Data Centre (VDC)
- Private Cloud
- Virtual Data Centre - SQLaaS
- MBR backup
- VDC backup
- Veeam Cloud connect
- NGFW Advanced
- NGFW Premium
- O2 AntiDDoS Standard
- O2 Antispam
- Security expert Center - SIEM (SIEM service)
- Security expert Center - LM (Log management)
- Security expert Center

I. Independent Service Auditor's Report

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To: Board of Directors of O2 Czech Republic a.s.

Scope

We have examined O2 Czech Republic a.s. ("O2 Czech Republic," or the "service organization") accompanying description of its system entitled "Description of O2 Czech Republic a.s. Service Organization's System" throughout the period June 1, 2023 to November 30, 2023 , (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 3®) (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period June 1, 2023 to November 30, 2023 to meet the criteria for security, availability, processing integrity, and confidentiality set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria)*.

Service Organization's Responsibilities

O2 Czech Republic has provided the accompanying assertion titled, "Management of O2 Czech Republic's Assertion," (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. O2 Czech Republic is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls that are suitably designed; and operating effectively to meet the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period June 1, 2023 to November 30, 2023, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

O2 Czech Republic uses O2 IT services, a subservice organization, to provide infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at O2 Czech Republic, to achieve O2 CZ's service commitments and system requirements based on the

applicable trust services criteria. The description presents O2 CZ´s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of O2 CZ´s controls. Our examination included the services provided by the subservice organizations, and we have evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve O2 CZ´s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve O2 CZ's service commitments and system requirements based on the applicable trust services criteria

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within O2 CZ´s in-scope services were effective throughout the period June 1, 2023 to November 30, 2023, to provide reasonable assurance that O2 CZ´s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BDO Audit s.r.o.

31.01.2024

Management of O2 Czech Republic a.s. Service Organization's Assertion

MANAGEMENT OF O2 CZECH REPUBLIC A.S. SERVICE ORGANIZATION'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within O2 Czech Republic Service Organization's (O2 CZ's) in-scope services throughout all of the period: June 1, 2023 to November 30, 2023, to provide reasonable assurance that O2 CZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, Processing integrity and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 (update 2022) Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout tall of the period: June 1, 2023, to November 30, 2023, to provide reasonable assurance that O2 CZ´s service commitments and system requirements were achieved based on the applicable trust services criteria. O2 CZ´s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls stated in the description operated effectively throughout all of the period: June 1, 2023, to November 30, 2023, to provide reasonable assurance that O2 CZ´s service commitments and system requirements were achieved based on the applicable trust services criteria.

MICHAL KREJČÍK
9. 2. 2024

RADEK SIKTAŘ
9. 2. 2024

JAN HRUŠKA
9. 2. 2024

II. Attachment A
Description of the boundaries of the O2 CZ system

II. ATTACHMENT A

DESCRIPTION OF THE BOUNDARIES OF THE O2 CZECH REPUBLIC A.S. SYSTEM

O2 Cloud brings new possibilities to build a modern global IT infrastructure. O2 Cloud enables improved customer service, increased process speed, reduced operational complexity (installation and operating costs, asset management and control) and enhanced security.

O2 Security services include Next Generation Firewall, AntiDDoS and Antispam to protect customers communicating over the internet, by e-mail and corporate IT.

O2 Security Expert Centre offers complete protection of the customer's ICT environment based on log management tools, SIEM and an expert security team.

This report has been prepared to provide information on internal controls of O2 that may be relevant to customers seeking security, availability, processing integrity, confidentiality, and privacy.

The scope covered in the report includes the following services:

Cloud services (O2 Cloud)
- Virtual data center (VDC)
- Private cloud
- Virtual data center – SQLaaS
- MBR Backup
- VDC Backup
- Veeam Cloud Connect

Security services (O2 Security)
- NGFW Advanced
- NGFW Premium
- O2 AntiDDoS Standard
- O2 Antispam

Security Expert Centre services (O2 SEC)
- Security expert Centre - SIEM (SIEM service)
- Security expert Centre - LM (Log management)
- Security expert Centre

The scope of locations covered in this report includes facilities located in the Czech Republic:
- Praha, Za Brumlovkou 266/2, 140 00 (Headquarters)
- Praha, V lomech 2339/1, 149 00 (Data Centre Chodov)
- Praha, K Zahrádkám 2065/2, 155 00 (Data Centre Stodůlky)

COMPANY PROFILE

O2, the leading telecommunications operator on the Czech market, continues its mission to deploy technologies that improve people's everyday lives. O2 provides voice, internet and data services to customers ranging from households and small and medium-sized businesses to large corporations and governmental organizations. Right now, O2 is building a fifth-generation mobile network (5G), launched as the first one into commercial operation. The O2 mobile network also includes virtual operators offering their services such as BLESKmobil, Tesco Mobile and MOBIL OD ČEZ. At the same time, O2 is the largest provider of internet for households and businesses, offered to 99% of addresses.

With its O2 TV service, O2 is the country's largest operator of TV over the internet. Having purchased a number of sports licenses, O2 is able to offer its customers the most appealing sports content on the Czech market. O2 is one of the key players in the field of hosting and cloud services, as well as managed services and ICT. As trends in the telecommunications industry change significantly, O2 also focuses on the development and offering of non-traditional telecommunications services. These include, in particular, financial services such as hardware insurance or mobile travel insurance.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The goal of O2 Czech Republic is to deliver top-quality telecommunications services. O2 defines its strategy and goals in compliance with its mission to deliver benefits to customers and generate relevant business profit.

Service commitments:

O2 Czech Republic effectively communicates its service obligations to its users through contracts, service level agreements and published policies. The service commitments involve a wide range of aspects related to the services provided by the organization.

Examples of service commitments:

As an example of a service commitment, we can mention the high level of service availability. This means that customers can rely on being able to access their telecommunications services at any time with minimum failures.

System requirements:

System requirements play a key role in the O2 business. The system requirements have been defined to provide efficient services, to comply with all legal requirements and to meet company's targets. The system requirements follow the Cyber Security Act (ZoKB) implemented through system policies, procedures, contracts and regulations.

Examples of system requirements:

O2 Czech Republic must ensure adequate system availability and ability to withstand overloading so that customers can enjoy the full potential of all services This includes implementing redundant infrastructure and non-stop monitoring.

Communication of commitments and requirements:

Transparency is a key responsibility of the management of O2 Czech Republic. By publishing the key service commitments and system requirements O2 allows its users to get a full picture of the O2 goals to evaluate the efficiency of the implemented controls.

Service credibility:

Specific service commitments and requirements for the O2 Czech Republic system have an impact on how customers see the reliability and quality of the services. A high level of service availability plays a key role in seeing O2 Czech Republic as a trustworthy service provider.

O2 Czech Republic pays great attention to providing a top service availability. To achieve this goal, the company implements a robust infrastructure and focuses on preventing system failures. For example, in addition to redundant systems, O2 Czech Republic performs periodical inspections and maintenance of the equipment and infrastructure to minimize the risk of failure.

O2 focuses on rapid detection and resolution of any problems that could affect the availability of services. O2 Czech Republic is equipped with sophisticated monitoring tools and systems that enable rapid reaction to any potential incidents to minimize long downtime or restricted access to some services.

At the same time, O2 Czech Republic keeps innovating and upgrading its systems and technologies to improve the features and performance for its customers. O2 regularly communicates with users and informs them of all planned maintenance windows or other activities potentially affecting the availability of the services.

O2 Czech Republic takes care to deliver its customers excellent service availability. By implementing a robust infrastructure, service monitoring, rapid reaction to all potential problems and continuing system innovation, O2 provides the customers a non-stop reliable access to all services.

ORGANISATIONAL STRUCTURE

The company is headed by the Board of Directors. The Chief Executive Officer (CEO) reports to the Board. The executive line of the organizational structure reporting directly to the Chief Executive Officer includes the following divisions and units: Commercial Division, Technology Division, Finance Division, Legal and Regulatory Affairs Division, Human Resources Division, Security unit, Public Administration Unit, Wholesale Services Division, Corporate Communications Unit and General Secretariat Department. The Company's top management consists of the Company's Board of Directors, the Chief Technology Officer (CTO) and the Chief Commercial Officer (CCO). The Company also has an Executive Committee as an advisory body to the Chief Executive Officer. The members of the Executive Committee are Directors of the Commercial Division, the Technology Division, the Finance Division, the Legal and Regulatory Affairs Division, the Human Resources Division and the Corporate Communication Department.

POLICIES AND PROCEDURES

The Company's activities are governed by general legal regulations, the Articles of Association and O2 internal management documents regulating all internal management systems and organization.
The management documents set out in detail the principles, rules and procedures for internal managing activities, taking into account their specific importance, location, technology, goals and other relevant parameters. Based on the company's strategy, policy and objectives, the management documents incorporate in detail all mandatory elements of external legislation into the company's conditions.
The rules for the administration and management of the corporate management document system are defined in a separate document.

CONTROL ENVIRONMENT

The Company has set up an internal control system described in management documents, approved by the Company's Board of Directors. An important role in this system is played by a unit called O2 Internal Audit, functionally reporting to the Supervisory Board. Internal Audit provides the Company's bodies with an independent and professional assessment of the internal control and management system, the condition and development of the examined area against current best practice. In addition, Internal Audit fulfils internal audit functions for O2 daughter organizations. Depending on the findings of the audits, adequate corrective measures are taken by relevant managers. The O2 Internal Audit monitors how the findings are dealt with and reports the results to the Company's bodies. The principles of internal auditing, including principles of independence and objectivity, are described in the IA O2 Statute.

The basic principles applied in the Company's accounting procedures include control based on the "four eyes control" and the separation of the process of creating and administering business partner data from the process of payment and settlement of booked liabilities. At the same time, the list of people authorized to create, edit or approve accounting records in the SAP system is limited and periodically monitored. For individual accounting documents, one can always identify a concrete user who created or cancelled the document. The correctness of accounting and financial statements is continuously reviewed within the Finance Division. Selected areas of accounting and compliance of internal processes with the applicable legislation and internal guidelines and procedures are verified by internal audit. In the event of inconsistency, corrective measures are immediately proposed and promptly implemented. The efficiency of the internal control system, the process of developing individual and consolidated financial statements, and the process of external audit are monitored by the Supervisory Board.

The Finance division includes a department called "Revenue Assurance" whose goal is to reveal potential revenue losses due to data leakage This end-to-end process covers all billing activities from the initiation of CDR to the issuing of customer invoice (bill).

The control environment also includes the application, compliance and checks of compliance with the requirements of ISO standards for management systems,

implemented within the integrated management system. With regard to the scope of this report, the following standards are particularly relevant:

- ISO 20000-1 Information technology – Service management,
- ISO 27001 Information technology – Security techniques – Information security management systems supplemented by requirements of ISO 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services and ISO 27018 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,
- ISO 22301 Security and resilience – Business continuity management systems.

The compliance with the above standards is reviewed through internal audits and periodical certification and inspection audits conducted by a renowned certification body.

INFORMATION AND COMMUNICATION

Effective communication increases people's engagement and improves understanding of the needs and expectations of external and internal customers, contributing to the effective functioning of the company.

There are five rules of communication with customers at O2 (1. I say everything that is important, 2. I tell the truth, 3. I follow up on the customer's request, 4. I represent O2, 5. I am polite), and these communication rules should be used company-wide, including in internal communication.

In O2, the basic information channel for all employees is the intranet, as well as email communication or SMS. In addition to the electronic channels, information is also provided in person during meetings, meetings with the top management or off-site meetings.
The internal communications include, but are not limited to, communication of O2 policies and procedures, corporate events, new initiatives, and awareness on information and cyber security. Also, an annual process exists to set objectives among all executives and is rolled down to employees. These objectives are filtered down to team members through the annual and midyear review process.

External communication is carried out by relevant functions and roles within the company, e.g.:

- customer communication: sales consultants, call center operators, account managers, service managers, service desk etc.,
- public and media communication: Corporate Communication unit,
- communication with suppliers: Purchasing, Logistics, Vendor Management, CTO Strategy Office,
- crisis management communication: Crisis Team.

A range of channels are used for external communication, from face-to-face meetings, phone calls to electronic tools such as email, chat, social networks and the company website, www.o2.cz.

MONITORING

Operational and safety monitoring

O2 maintains reasonable and appropriate technical and organizational measures, internal controls and information security procedures to protect its information assets as well as all customer data from accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction.
O2 uses a number of automated monitoring systems for operational and security monitoring to ensure top-class performance and service availability. Monitoring is used at the level of user applications, user stations, servers and technological stations, security devices and network elements. Selected points of connection of the O2 network with public data networks and interfaces between selected security zones are monitored by IDS. Traffic between public or third-party networks and the O2 network is controlled by firewalls. The configuration of the firewalls is based on the principle of "everything which is not allowed is forbidden".
Operational and security monitoring is followed by relevant incident management processes, including security incident management.
The requirements for operational monitoring of information system elements respect all legislative requirements (especially GDPR) and separate management documentation.
As a provider of cloud services, O2 provides customers with logging options depending on the type of service and offers the possibility of monitoring the operation (traffic) of these cloud services.

Internal audit
In the Our Business Principles document (see below), O2 defined the commitment to apply appropriate control mechanisms to assess and manage risks for O2, its employees and its image. Therefore, the Company has established an internal audit function to assure the Company's bodies and management of the efficiency of all internal governance and risk management processes, as well as to comply with the recommendations of good corporate governance practices. Internal audit is an independent and objective activity based on the philosophy of adding value by improving internal company operations. Internal audit helps O2 achieve its objectives by using a systematic methodological approach to evaluate and improve the efficiency of the risk management system, management and control processes, and corporate governance. Internal audit activities follow the rules of the International Professional Practices Framework (IPPF): a) Key principles b) Code of Ethics c) Standards d) Definition of internal audit. Furthermore, audit activities are carried out in accordance with the relevant legal regulations and internal management documents governing the performance of internal audit. Internal Audit provides independent and objective assurance as to whether the company ensures: compliance with the requirements of legal regulations and other mandatory requirements, reliability of information, efficiency of risk management processes and prudent management and protection of company assets.
O2 internal audit plays the role of the third line of defense in the IPPF's three-line model. In this model, the first line of defense includes operational management, the second line various functions of risk and compliance control incorporated by O2 management, while the third line includes independent assurance.

CODE OF CONDUCT AND ETHICS

The Company adheres to the recommendations of the Czech Corporate Governance Code 2018, the general rules of which are based on the applicable legislation of the Czech Republic. The recommendations are also inspired by comparable national codes of

corporate governance (in particular, the German and Austrian codes) and international standards of corporate governance (in particular, the G20 / OECD Principles of Corporate Governance of 2015). Support for the performance of corporate governance and management, including the fulfilment of the requirements of the Czech Corporate Governance Code 2018, is the responsibility of Company Secretary, organizationally a member of the Legal and Regulatory Affairs Division.
The Compliance Code is part of the internal culture of O2 Czech Republic a.s. representing its approach to the compliance with legal regulations raising the ethical and responsible business standards. Measures derived from the aforementioned rules called the „compliance program" and the focus on abiding by the rules fall among the priorities of the O2 management. The prime goal of the measures is to set up an internal mechanism for O2 to prevent any illegal activities and, if any such activity occurs, to be identified and responded to accordingly.
O2 has a comprehensive and interconnected system of internal regulations and procedures in place, to ensure company compliance with laws and regulations. The starting point and central point are "Our Business Principles" (hereinafter referred to as the "Business Principles") representing the source of values and principles to define our internal regulations. Numerous internal regulations explicitly refer to our business principles, boosts the awareness and the importance of the principles. All areas described in Our Business Principles form a traditional part of the country's legal order. Furthermore, O2 describes in its internal regulations how its employees and members of bodies are supposed to act in specific situations in line with O2 internal processes.

This system is seen as measures within the meaning of §8 Art. 2 of Act no. 418/2011 Coll.

Our Business Principles are both an internal regulation approved by the Board of Directors and a document published on the O2 website (section "Responsible Approach"). The original version of the Business Principles is in Czech. The English version of the O2 website and Our Business Principles are available, too.
The Compliance Officer is responsible for the content and updating of the training. The objective of the training is to explain to all employees the content and meaning of Our Business Principles and the basic principles and rules arising from the key internal regulations to be followed by all employees in order to eliminate the risk of unlawful conduct. The elementary version of the training is mandatory for all O2 employees.

The Employment Rules govern the basic obligations of all O2 employees arising from their employment relationship. The Employment Rules are derived from Our Business Principles. The Policy of Accepting and Providing Gifts and Hospitality and the Conflict-of-Interest Policy constitute an integral part hereof.

The Signature Rules are another key internal regulation dealing with internal procedures of O2 employees when acting on behalf of O2 externally.

In order to achieve the objectives, set out in the Compliance Code and to ensure prevention, O2 has implemented an internal whistleblowing system as an essential element to report a complaint about potentially unlawful conduct directly affecting O2. A whistleblower who meets the conditions for filing a report under the Whistleblower Protection Act is guaranteed adequate protection.

RISK ASSESSMENT PROCESS

Risk management is one of the basic managerial tools of the Company's effective management system, whose aim is to support the fulfilment of the Company's vision and strategy. The risk management system is developed as an integral tool of the Company's internal control. Risks are identified on the basis of regular assessments by competent managers, suggestions from Risk Management and other Company units. Risks are evaluated from the perspective of potential financial impact and likelihood of occurrence. Members of the Board of Directors are kept up to date about all major risks to the Company and the way they are managed.

The management of operational risks in the area of information security and business continuity is governed by an appropriate methodology. The methodology runs on-premises on O2 servers. In accordance with the legislative requirements for cyber security, relevant threats and vulnerabilities are taken into account in the assessment of operational risks. People responsible for the implementation of business plans and sustainable development of the company must consider the following three areas:

- potential damage to the business, caused by security failures;
- real likelihood of relevant vulnerabilities due to prevailing threats vs. security measures in place;
- importance of asset vulnerabilities to possible threats.

O2 carries out risk assessments for all company systems and situations arising from the context of the organization.

HR MANAGEMENT

O2's business success and prosperity depend, but not only, on long-term relationships with customers, seeing O2 as a stable, strong and reliable partner keeping all customer data confidential. In order not to undermine the trust of our customers, to meet their expectations, not to compromise our image and risk of being excluded from public projects, we carefully select our employees for specific positions both in terms of qualification and integrity.

The selection of employees is based on clear criteria in terms of security suitability, trustworthiness, reliability and clean criminal record, The criteria are reviewed for each employee both before and during his or her employment, in accordance with the procedure laid down in our Security Regulations. The criteria for selecting employees are set by the Human Resources Division and all security aspects consulted with the Security unit.

Depending on the type of sensitive information, all employees supposed to get in touch with sensitive information during the performance of their jobs must sign all relevant non-disclosure statements.

O2 employees must attend an obligatory training course covering various topics incl. Our Business Principles, Information protection and GDPR. The training must be periodically repeated. Security training is obligatory for all O2 employees and all external (third-party) individuals and organizations working on the O2 premises.

Each employee is subject to a periodical Performance & Talent Review. The review includes meeting of individual targets, conduct and approach, which also includes adherence to corporate culture, communication, and team cooperation as well as an active, logical and effective approach to solving problems The outcome of the review also includes the identification of needs for further education and individual development.

KEY RESPONSIBILITIES

In O2, responsibilities are set out primarily in the Organizational Rules, which summarize the essential information about the company, determine the system of internal management and organization, define the responsibilities and accountabilities of all company bodies, units and individual employees, determine the reporting lines of the units and responsibilities towards the company bodies including the system of internal management documentation.

As to the services described in this SOC3 report, the following O2 units are of crucial importance:
Product management teams provide and coordinate the development of products and services including launch; manage the lifecycle of products and services.
The network teams take care of the operation of O2 security services, including the operation of the inevitable infrastructure, other teams are dedicated to providing O2 SEC services to O2 customers, including the operation of the inevitable infrastructure.
The Security unit defines and enforces the company's strategy and security policy, manages and defines security measures, promotes the implementation of the measures and controls how these are followed in all areas of physical, information and cyber security.

Suppliers used by O2, namely CETIN (a sister organization) and O2 IT Services (a daughter organization), have significant responsibilities, too.

CETIN owns the data centers used by O2 to operate its cloud services. CETIN thus provides O2 with services for the operation of non-IT infrastructure, is responsible for the availability as well as the physical protection of the data centers and access to the data centers. The data centers are certified for TIER/RATE III.
O2 IT Services operates the hardware and the virtualization platform used for the O2 Cloud services and ensures the performance of the Service Desk.

SYSTEM COMPONENTS USED TO PROVIDE THE SERVICE

Infrastructure

Cloud and backup services

The provision of cloud and backup services is the role of O2 ITS, an organization responsible for the operational part of services such as O2 VDC, O2 Private Cloud, O2 Backup VDC and O2 Backup. The services are operated at CETIN data centers in two locations, Praha Chodov (DC CH) and Praha Stodůlky (DC JZM) with the 24x7x365 monitoring.
The server infrastructure is built on a farm of servers from the world's leading vendors combined with the state-of-the-art virtualization technologies at the High Availability

level. All the servers including the infrastructure are connected redundantly to minimize the downtime due to technology failures. Guaranteed service availability is 99.9%.

O2 Next Generation Firewall
NGFW is designed with the concept of concentrating top-class HW security elements and centralized security in one place. It's because this solution is better in terms of costs, performance and durability than the concept of spread security. Using centralized security, one can achieve the same or higher level of security at lower acquisition and operating costs.

Centralized services over the communication infrastructure dramatically reduce the likelihood of intrusion from the external environment into customer's internal IT environment and create conditions for the customer and the provider to better coordinate their steps in the effort to fight against potential hackers.
NGFW is a geographically redundant security infrastructure developed by backing up production elements in two identical branches located in two different locations, thus achieving great service reliability and availability. NGFW is located at hosting centers meeting strict security requirements with strict parameters, designed and operated at the Tier III level (under the Uptime Institute classification).

The environment meets the following requirements of computing and communications security:

- redundant data connectivity is connected to two independent directions terminated on separate technology in different buildings/facilities,
- communication infrastructure used for the provision of services is technically and geographically redundant,
- communication infrastructure is located in a safe environment of a hosting center or equivalent environment,
- access to the management system of elements and services (local and remote) is controlled in an environment separated from customer environment and,
- infrastructure is controlled by skilled professionals with adequate certifications.

Safety requirements are guaranteed and adhered to throughout the entire term of contract. The O2 CZ ISP network consists of two independent locations providing peering connectivity.

O2 AntiDDoS
The O2 CZ ISP network consists of two independent locations providing peering connectivity with local peering (NIX) and transit internet connectivity provided by several different upstream providers (Tier1 ISPs).

As to AntiDDoS, O2 uses platform implemented in the network with regard to various parameters such as size, geolocation, etc.

The implementation consists of 3 sections:
- CP, which includes the analytical part of the system,
- TMS containing mitigation part,
- PI - portal interface for customers.

All configuration changes of TMS are performed in a CP device. The CP device creates BGP peering with the affected routers (ISP border routers) such as BGP host (RRC route reflector client) and receives all BGP notifications received or forwarded by ISP routers. The CP device is connected to border routers to receive NetFlow data, used as the main source for analyzing the behavior and traffic. Once the CP device flags some traffic as suspicious, request will be sent to TMS for BGP rerouting the suspicious traffic for further investigation. If the traffic is classified as a DoS/DDoS attack, TMS will discard the unwanted traffic, or send it back via the original route to be later delivered to the destination.

O2 Antispam

O2 Antispam is a service using the system to detect spam. Principally, the service is a public e-mail gateway in the O2 infrastructure, in which a unique account is created for the user to administer the security policy of a protected domain or multiple domains Next, in the domain provider location, using the MX record, change of delivery to the email gateway, serving as protection, will be made. The email gateway will then offer the user a total security solution as a service bearing in mind the plethora of various internet threats.

Malware (i.e. viruses, Trojan horses, spyware, etc.), spam, vulnerabilities, networks of infected computers (botnets), fraudulent emails, files and websites (phishing and pharming) and many more represent potential security threats to enterprises and their business. In addition to its own antispam functionality, O2 Antispam offers quarantine for the captured messages (to eliminate what is called “false positive”). The service can be implemented separately not requiring other services such as NGFW.

O2 Security Expert Centre

The aim of deploying O2 SEC is to boost the security of the IT environment and get a picture of what is happening on the network and endpoints in order to better identify and eliminate ongoing threats in a timely manner.
The service provides the following functionalities:

- collection, storage and analysis of logs of the defined systems,
- security monitoring (no need for customer to do monitoring internally).
- A central model of security monitoring/control for all organizations within a group.

The Service uses tools provided as part of the Service operated by O2. HW/SW probes are placed in the customer location to monitor traffic in the network (network probe). The tools include, in particular:

- Log management
- SIEM

The service includes a combination of complementary services aimed at protecting customers against all sorts of cyber threats that can bypass standard perimeter protection, antivirus systems to pose long-term or permanent threats to customer security and business, while creating an environment compliant with all legislative requirements. O2 SEC includes the 24x7x365 monitoring with proactive security control and periodical reviewing of cyber security events. The proposed solution provides a multitenant environment allowing the customer to select the setting of the form of visibility for individual supervised entities i.e. selective approach in terms of policies and reporting.

Logs are collected from devices defined by the customer and sent to what is called collectors. Collector is a collection point in the customer network installed as a virtual appliance in an HA setup in customer's DMZ network.
The collectors are connected to the firewall in the O2 Security Expert Centre via a secure connection (VPN, TLS, etc.). Stream processors process logs using log management functionalities, real-time or non-real-time SIEM. The solution is built as an HA active - active cluster.

O2 SEC includes systems for detecting anomalies in network traffic. The systems monitor the O2 SEC environment as a whole and provide audit trails. Another part of O2 SEC is the ticketing system, used as one of the communication channels between O2 SEC and the customer. Customers can use a web interface.
The offered solution is designed as highly available (HA) with implicit load balancing.

Software

Cloud and backup services

Cloud and backup services are structured into several PODs representing clusters of interconnected servers with hypervisor. Located in data centers, the clusters provide computing power to run customer environments. The role of hypervisor is played by market leading virtualization platform, run on a multi-tenant layer, a portal allowing customers to manage their environments. All servers in the clusters are equipped with SSDs and use vSAN to deliver great data speed and availability.
In both data centers there are separate PODs for SQLaaS. The PODs are optimized to run SQL and contain a high-frequency CPU. The servers in the PODs are fully licensed to run SQL databases. Along with the infrastructure, SPLA licenses are offered for the services: OS Windows server Standard license, RDS license, Application license for MS SQL Standard and Enterprise, RHEL license.
The VDC Backup service uses specialized software from Veeam, which provides advanced features for data backup and recovery in a virtualized environment.

O2 Next Generation Firewall

The company uses a firewall that connects all security and network components to ensure seamless integration. This enables the convergence of network and security features to deliver consistent user experience and resilient security position across all types of environments, including on-premises, cloud, hybrid, and convergent IT/OT/IoT infrastructure.

O2 AntiDDoS

The company uses a solution used to detect DDoS attacks. The system allows you to monitor network traffic and use data for smart traffic analysis, usage optimization, intelligent network expansion planning, threat elimination and reporting for customers and users.
The system is able to remove malicious parts from a communication session without disrupting other key network services.

O2 Antispam

The company uses an operating system that ranks among the largest cybersecurity platforms on the market, organically built on a common governance and security framework. It connects all necessary security and networking components to ensure

seamless integration. This enables the convergence of network and security functions to ensure a consistent user experience and resilient security posture across all types of environments, including on-premise, cloud, hybrid and converged IT/OT/IoT infrastructures.
The system is an organically evolving system augmented with new features to increase the potential to provide unprecedented visibility and enforcement in hybrid environments. Additionally, the system accelerates security operations through AI-driven prevention, automation and real-time response. Furthermore, the system offers secure network management, increased prevention, early detection and real-time response, and reduced risk of various cyber threats.

O2 Security Expert Centre
O2 SEC takes cyber security as no.1 priority using professional tools from renowned manufacturers. The workplace has a sophisticated software ecosystem designed to monitor and immediately identify all potential cyber threats. The software used for log management and SIEM services enables compliance with relevant cybersecurity legislation, GDPR and ISO 27001.

People

The actual operation and development of Cloud services requires the involvement of several different roles ranging from technical to commercial ones. The operation of these services is the responsibility of O2 IT Services, taking care of the technical operation of the service, including the Service Desk. The operation of security services is provided by O2 Czech Republic. Key technical roles for cloud services include Solution Architect, Service Manager and Operations Specialist. Commercial, security and network infrastructure fall among the roles of O2 Czech Republic. The roles include Product Manager, Segment Manager, Sales and Presales Manager, Security Specialist and Network Infrastructure Specialist. All roles of security services are delivered by O2 Czech Republic.
To confirm the level of competency of our core service providers, VMware, Veeam Software and Fortinet, we maintain a certain level of partnership, evidence of which is the required number of specialized certifications. You can check our partnership level on our vendors' websites - VMware, Veeam Software and Fortinet. Our goal is to continuously increase the level of partnership and competence, confirmed by the certifications obtained by our specialists.
The services of the O2 Security Expert Centre are provided by competent security staff. The key security roles include L1 Security Operator (a team of L1 operators working 24/7 in charge of security supervision, evaluation of alerts and events from monitoring systems), L2 Security Analyst (L2 Analysts operating in 8/5 mode with standby outside standard business hours whose tasks include more profound analysis based on L1 level findings, reporting and communication with customers) and L3 Security Architect (a team of L3 architects working in 8/5 mode with the possibility of standby outside standard business hours, and responsibilities including communication with suppliers, onboarding, and technical support to other teams).
Competent system administrator is responsible for setting up and deleting access accounts to the Services. Administrator activities are carried out in accordance with internal regulations. Periodical checking of access takes place once a year to make sure that all accesses are properly controlled and comply with the defined security requirements. This ensures that data and systems are protected from unauthorized access and misuse. System

administrators play a key role in managing access accounts and maintaining security standards.

Procedures

O2 Czech Republic is committed to maintaining top-level safety for its systems and infrastructure. This includes to ensure relevant confidentiality, integrity, and availability of data and systems through its internal policies and procedures.
O2 Czech Republic has implemented - as part of the integrated management system - a unified management system for policies and regulations. The policies and procedures relate to service processes, including the management and designing of product and service lifecycles, customer process management (customer onboarding and offboarding), change management processes, operational monitoring, incident management, and more. The goal of the policies and procedures is to ensure the security and protection of data and systems. O2 Czech Republic regularly reviews and updates the policies and procedures to ensure their compliance with the latest security standards and technologies.
Creating and maintaining strong safety awareness among employees is another important part of O2's focus. O2 Czech Republic provides training and educates its employees to be able to recognize and respond to potential security threats.
With its approach, O2 Czech Republic demonstrates its commitment to maintain a safe environment for its customers and protect sensitive information. Safety and security represent no.1 priority for O2 Czech Republic, forming an integral part of our business.
O2 Czech Republic is aware of the continuing evolution of security threats and vulnerabilities. Having this in mind, we regularly monitor and review our systems and infrastructure to identify any potential security risks and to adopt efficient measures to minimize the occurrence.

In addition, O2 Czech Republic cooperates with information security experts and monitors the latest trends and technologies to be able to respond to the new threats and implement best practices and measures to ensure adequate security.
The protection of customer privacy is another important aspect of security. O2 Czech Republic complies with all relevant laws and regulations pertaining to the protection of personal data and is committed to the correct and secure processing of such data. O2 customers can be sure that their data is protected and processed with the utmost care and security.
O2 Czech Republic pays enormous attention to security as such as well as the protection of personal data and systems. The commitment to safety can be demonstrated in several key areas such as:

- Security infrastructure: O2 Czech Republic invests in modern security technologies and infrastructure is able to detect and respond to potential threats. For example, the company uses advanced firewall systems and systems for detecting and preventing attacks.
- Monitoring and detection: O2 Czech Republic regularly monitors its systems and networks to identify suspicious activities or anomalies. If a potential security incident is detected, the company responds immediately and takes steps to minimize the damage.
- Employee training: O2 Czech Republic recognizes that security measures can only be effective if employees are adequately informed and trained. Having this in

mind, O2 delivers regular training to employees to inform them of the latest security threats and best practices for protecting data and hardware.

- Protection against DDoS attacks: O2 Czech Republic also provides protection against DDoS (Distributed Denial of Service) attacks and AntiSpam measures. DDoS attacks are attacking that target network or web server congestion to deny user access. O2 Czech Republic uses advanced technologies and infrastructure to detect and avert DDoS attacks to keep its services available to users.
- Security policies and procedures: O2 Czech Republic has strict security policies and procedures in place to serve as a framework for protecting data and systems. The policies include rules for accessing sensitive information, password security, data encryption, and other security precautions.
- Regular updates and backups: O2 Czech Republic regularly updates its hardware and software to ensure the latest security patches and protection against known vulnerabilities. In addition, O2 performs regular data backups to minimize the risk of losing data in the event of a disaster or attack.

O2 Czech Republic is actively engaged in collaboration with security organizations and offices to share information about new threats and cooperate in solving them. This is our contribution to the overall improvement of digital security.
O2 Czech Republic makes considerable efforts to ensure that our customers are secured and their personal data thoroughly protected. Our investing in modern technologies, periodical monitoring and employee training demonstrate our commitment to security and data protection.

All internal policies and regulations (a list of which is summarized at the end of this section) are periodically reviewed and audited.

Data

Data protection represents a key element for O2 Czech Republic to the provision of its services. O2 is committed to compliance with all relevant legal regulations, including GDPR (General Data Protection Regulation) and ZoEK (Electronic Communications Act). This chapter deals with the types of data used to provide services and the measures adopted by O2 Czech Republic to ensure the confidentiality, integrity and availability of the data. The types of data used for our services are as follows:

- Content of communication: O2 Czech Republic conveys communication between customers and other entities. The content of the communication is conveyed without O2 having access to the content. This means that all transmitted data is protected from unauthorized access.
- Customer contact information: O2 Czech Republic stores customer contact information such as name, address, phone number, and email. This information is necessary for the communication with customers as well as for the provision of services.
- Contracts and communication with customers: O2 Czech Republic stores all contracts and communications with customers containing crucial information about the services including the terms and conditions. These documents are protected and stored in compliance with relevant legal requirements.

- Usage (traffic) data needed for the billing of services provided to customers and proving the legitimacy of billing: O2 Czech Republic collects traffic data necessary for the correct billing of customer services and for proving their legitimacy. This data is protected and processed in compliance with the internal policies and regulations.
- Other traffic data needed for analyzing errors and security of communication in the networks: O2 Czech Republic collects traffic data necessary for the correct billing of customer services and for proving their legitimacy. This data is protected and processed to minimize risks and provide network security.
- Data stored by the customer in the provided (cloud) services: O2 Czech Republic provides cloud services in which customers can store their data. This data is protected and secured against unauthorized access and loss. As O2 Czech Republic does not have access to the content of the data the confidentiality and privacy of customers is preserved.

Data and personal data protection measures: O2 Czech Republic has established internal policies and regulations to ensure the confidentiality, integrity and availability of data and personal data. The policies and regulations are in line with legislative requirements such as GDPR and the Electronic Communications Act, as well as the standards making up the integrated management system, including ISO 27001.
The defined policies and regulations set out responsibilities, powers, and procedures for the area of data and information protection including data access control, use of appropriate data protection tools such as firewall, intrusion prevention system (IPS), intrusion detection system (IDS), and security information and event management (SIEM). These measures are used to identify and detect threats and vulnerabilities to ensure safety of data and communication.
Data protection and personal data protection requirements are also incorporated in agreements between O2 Czech Republic and its customers. The agreements set out for both parties their obligations in compliance with applicable legislation.
O2 Czech Republic is responsible for the protection of customer data incl. personal data and takes this obligation very seriously. As indicated above, O2 strives to continuously improve its procedures and technologies to deliver maximum protection for all data including personal data.

PHYSICAL SECURITY

O2 Data Centers are designed to guarantee maximum security and privacy for customer devices and data. The data centers are owned by CETIN a.s., a sister organization of O2, operating non-IT data center technology and security services, including access control and security.
In order to protect the assets, the O2 Security unit installs technical and mechanical protection tools following relevant regulations, sets regime measures to create a uniform standard for access control and the scope of security of O2 facilities, and carries out all necessary periodical inspections.

Access control
Based on the security zoning of the Data Centre, the level of access control security is defined. The entry to the Data Centre is allowed to authorized/registered personnel using

multiple authentications of contactless cards and PIN on the access control readers. Highly protected DC areas require the combination of the above with biometric systems. Every person moving in the DC premises is visibly marked. All visitors to the data center must be accompanies by a DC employee.
O2 Security is responsible for checking compliance with the access rules as well as for the conducting of audits to verify compliance with the incident response procedures by the DC access control staff.

24x7x365 security monitoring
The perimeter, interior, areas containing supporting technology and the technological rooms are monitored by security and camera systems, supervised by authorized security staff.
All elements, functional and IT, of the data center are monitored by IT monitoring center staff.

Fire protection
All areas of the DC are secured with elements of the electric fire alarm system, the technology rooms include VESDA laser early detection systems and a system of automatic stable fire extinguishing system with inert gases.

Power supply and redundance
Power supply to the data center is protected by powerful uninterruptible power supply (UPS) units feeding dually customer's power distribution units (PDU). All data centers are protected against long-term power failure by diesel generators backing up the UPS system.
A backup of minimum N+1 ensures business continuity even in the event of a failure of one of the UPS.
Diesel generators contain fuel for at least 24 hours of operation without the need for refilling. If necessary, the supplier is able to deliver some more fuel. Cooling is provided by powerful, fully replaceable air conditioning units.
All our data centers are built and operated under the TIER III standard.

ENDPOINT PROTECTION

The protection of company endpoint includes monitoring and protecting endpoints from cyber threats. The protected endpoints include desktops, laptops, smartphones, tablets, and other devices. There are various cybersecurity solutions you can install and monitor to protect the aforementioned devices from cyber threats, irrespective of whether these are in or out of the corporate network.

O2 has installed Endpoint Security (ENS) using proactive reporting of threats, able to deliver adequate protection throughout the entire lifecycle of an attack.
Endpoint Security Suite contains Endpoint Security and Endpoint Detection and Response.

ACCESS CONTROL

Access control policy

Access control is implemented mainly for controlling user access to protected (classified) information, preventing unauthorized access, altering, disclosure or theft of information and media, all at the level of physical and logical access control.
During access control, our competent staff cooperate mainly with the Security unit, the Personal Data Protection unit and the administrators who are in charge of the administration of information resources.

Access to networks and network services
Users are allowed to access networks and network services for which they are explicitly authorized.

User administration and access control
Physical access control is governed by the Company Entrance Control directive. The logical access control of users follows the Corporate Access and Rights Management directive and the Administrator Security Manual.
Users are required to proceed in accordance with the approved access rules. Managers may only approve requests that are necessary for the performance of an employee's job. Access control for external workers is ruled by third-party access control to internal information systems and the "External workers register".
Users are prohibited from seeking authentication data needed for accessing information resources, using an account other than the one assigned, and from connecting unapproved IT elements to the network. All users are obliged to report any suspicious behavior or security incident in accordance with the Definition and reporting of security incidents and events directive.
As a cloud service provider, O2 provides procedures and tools for the registration and de-registration of cloud service users. Moreover, O2 provides the customers with tools to manage user access rights and privileges.
As a cloud service provider, O2 provides the administrators with efficient tools to securely log in for the administration of the service, including monitoring and configuration of security elements.

CHANGE MANAGEMENT

The main goal of ICT Change Management is to make sure that standardized methods and procedures are used to deal with all changes effectively and quickly. It is also important that all service changes and configurations are recorded in the Configuration Management System. Another goal is to optimize overall business risk.

The goal of the ICT Change Management procedures is to respond to changing customer business requirements while minimizing incidents, failures, and duplications. It is equally important to respond to changing business and IT requirements so that services are aligned with the current business needs. In addition, it is necessary to ensure that all changes are recorded, evaluated, enabled, prioritized, planned, tested, implemented, documented and reviewed in a controlled fashion.

The procedure is binding in its entirety for all employees of O2 Czech Republic a.s., people working for O2 on a contractual basis (non-FTE, third-party) as well as for all other parties bound to comply with the Directive.

Change management is governed by several directive documents or other defined documents.

DISASTER RECOVERY

O2 defines the Business Continuity Management System (hereinafter referred to as the "BCMS" and the "Company"), creates the basic methodology and organizational prerequisites for the implementation of the Company's BCMS system. In connection with the Company's Business Continuity Management Policy (BCM Policy) and the company's governing documents (Organizational Rules, Security Rules), it defines the basic competencies of O2 management in the field of BCMS, sets out the principles of creation, the structure of BCMS and defines all elements and functions of the BCM system. The system enables O2 executives and the unit/s under their management to focus on meeting the BCMS tasks and obligations arising from the relevant legal regulations and contracts. Implemented in the company's environment, BCMS uses the best-known practice and experience acquired in the field of BCMS.

The concept of O2 BCMS is multilayer, in terms of territory and sector:

Layer 1 – In order to deal with the impact of internal (plus some external) emergencies on the company's business solved by the relevant units within standard processes without requiring major modification, the BCM system is designed as a system for managing emergency situations (operational accidents, failures, closures, incidents, problems, service outages, events, etc.) without activating corporate crisis teams. The planning, creation, method of activation (escalation of activities), activity, support and development fall within the competence of the relevant management.

Layer 2 – In order to deal with the impact of external emergencies (crisis situations) as well as internal emergencies (large-scale emergency situations) on the company's environment, exceeding the scope, capacity and competencies of individual company units requiring the application of non-standard (modified) processes and forms of management, the BCM system is designed as a crisis management system with the activation of the company's crisis team. The planning, creation, way of activation and development of BCM are the responsibility of the CNOC unit while the activation falls within the competence of the particular crisis team leader. The transition from the system of ad-hoc dealing with emergencies by a particular unit to the system of crisis management (at the regional or national level) is usually decided by the leader of the crisis team in cooperation with the unit's line management of the unit/s depending on the assessment and evolution of a particular emergency.

Processes and procedures (BCP, DRP) to address emergencies are periodically reviewed, tested and, if required, updated. All exercises and tests are recorded in Ramses.

BCP/DRP defines several documents and policies in the company.

VULNERABILITY MANAGEMENT

In the area of vulnerability management, the company has established basic rules, procedures, powers and responsibilities to efficiently manage the vulnerability of

information systems and technologies to minimize the risk of security incidents, potential losses and to reduce business risks.

Efficient vulnerability management program includes:
Responsibility for the continuous maintenance of the information system.
Continuous monitoring of the condition of updates and implemented information system patches.
Compliance with software vendor recommendations.
Continuous and ad-hoc countermeasures to minimize security risks and incidents.

The aim of vulnerability management is to ensure compliance with the recommendations of the manufacturer and the Security unit while timely eliminating all vulnerabilities.

As various vulnerabilities differ in how critical they are, each responsible person (administrator) must judge which software patch should be applied in order to minimize the business impact and to plan enough time for testing and implementation in line with the change management process.

It is the responsibility of the administrators to obtain all software patches from renowned, trusted support channels, such as the actual vendors or third-party vendors. Each software patch must be downloaded and applied to licensed software and where there is a support agreement in place.

In the event that objective reasons prevent the above activity the responsible person (admin) must apply for an exemption from the rule/s under the applicable Security Exception Management directive.

In places where there is open-source software without a trustworthy support channel, the responsible person must address the situation by applying the aforementioned exemption.

III. Attachment B
Description of a O2 Czech Republic service organization's principal service commitments and system requirements

ATTACHMENT B

DESCRIPTION OF A O2 CZECH REPUBLIC SERVICE ORGANIZATION'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Service Commitments

Commitments are declarations made by management to customers regarding the performance of O2 CZ System. Commitments to customers are communicated via Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

System requirements are specified in the Company's policies and procedures, which are available to all employees.

O2 CZ makes service commitments to its customers and has established system requirements as part O2 ITS service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. O2 CZ is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that O2 CZ service commitments and system requirements are achieved.

O2 CZ is subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which O2 CZ operates.

Security, Availability, Confidentiality, Privacy and Processing Integrity commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the O2 CZ website. Security, Availability, Confidentiality, Privacy and Processing Integrity commitments are standardized and included, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the O2 CZ System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.

- Security and confidentiality principles inherent to the fundamental design of the O2 CZ System are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.

- Availability principles inherent to the fundamental design of the O2 CZ System are designed to replicate critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.

- Privacy principles inherent to the fundamental design of the O2 CZ System are designed to protect the security and confidentiality of O2 CZ customer content to meet the service commitments.

- Processing integrity principles inherent to the fundamental design of the O2 CZ System are designed to protect the security and confidentiality of O2 CZ customer data in transit to meet the service commitments.

O2 Czech Republic establishes operational requirements that support the achievement of security, availability, confidentiality, privacy and processing integrity commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in O2 CZ system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various O2 CZ services and offerings. O2 CZ' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality, privacy and processing integrity.

AVAILABILITY

There is a documented procedure for capacity management. Capacity plans are prepared with warning and action thresholds set for monitored resources (compute, storage, memory). Appropriate monitoring tools are used for actual usage and capacity measurement. The current usage of resources and forecast of capacity demand is regularly reported to management.
Environmental threats are part of the list of threats in the risk assessment process. External environmental threats were considered, and data centers are located out of flood, earthquake areas.
CETIN as a vendor is responsible for implementation and operation of environmental protections. Detection measures are implemented, such as fire, smoke detectors, air quality detectors, and liquid leak detectors. Environment and operations monitoring, and alerts are part of each DC surveillance system with 24/7 onsite personnel presence. Maintenance and test plans are prepared for both data centers.
Data centers are designed and operated in compliance with TIER III requirements.
Data back-up processes are implemented according to the specifications of individual services in the scope of this report (configuration backups, replication at the storage level, synchronous data replication, etc.).
O2 has implemented business continuity management system according to ISO 22301 which covers both data centers. Business continuity plans with disaster recovery procedures are prepared for the services in the scope of this report. BCP/DRP include testing requirements (scope, frequency).

CONFIDENTIALITY

O2 sets out the rules and principles of information protection, including the powers and responsibilities for the identification, classification, processing and protection of confidential information.
In addition, a single system for document management, including rules for archiving and shredding, has been implemented in accordance with Act no. 499/2004 Coll., on Archiving and Records Management.
The rules for the protection of classified information pursuant to Act no. 412/2005 Coll., on the Protection of Classified Information and Safety Clearance, are set out in a separate internal regulation.

Procedures for the disposal of information depending on qualification level and medium i.e. printed document, electronic file on various media are in place.

PROCESSING INTEGRITY

As O2 Cloud services are primarily designed as Infrastructure as a Service, O2 does not process data belonging to customers. O2 security services are mostly analytical, monitoring and reporting services. In these cases, it is stipulated in a contract what data the customer must provide and for what purpose of processing. The contract also determines the format of the input and output data (including reporting), the method of data transmission, the rules for the protection and storage of data. Process integrity control also includes operational and safety monitoring of the services.

PRIVACY

As O2 Cloud services are primarily designed as Infrastructure as a Service, O2 does not process data belonging to customers. O2 security services are mostly analytical, monitoring and reporting services.
If the customer informs O2 that the scope of O2 Cloud services also involves the processing of personal data the terms and conditions will also obtain a clause specifying the relationship between the controller and the processor of personal data pursuant to GDPR.
O2 has set up processes to ensure compliance with all legislative requirements regarding protection of personal and other data. An internal regulation sets out the rules for the protection of personal data (GDPR), the protection of identification, traffic and location data and the confidentiality of communications (see the Electronic Communications Act) and the protection of trade secret.
Each contract resp. the terms and conditions include a clause on the protection of personal data. In addition, customers are informed about the protection of personal data on the O2 website (https://www.o2.cz/soukromi). The O2 website shows how O2 uses cookies and handles personal data of the customers both in the role of data controller (Personal Data Processing Policy) and data processor (List of Personal Data Processors). It also includes information on how complaints are dealt with including contact details of the Data Protection Officer and the right of each customer to escalate a complaint to the Office for Personal Data Protection.

O2 Czech Republic a.s.

Praha, Česká republika

ZPRÁVA O SYSTÉMOVÝCH A ORGANIZAČNÍCH KONTROLÁCH (SOC) 3

ZPRÁVA O KONTROLÁCH V SERVISNÍ ORGANIZACI RELEVANTNÍCH PRO POPIS SYSTÉMU SPOLEČNOSTI O2 CZECH REPUBLIC A.S. A O TRVALÉ UDRŽITELNOSTI SYSTÉMU A PROVOZNÍ EFEKTIVITĚ KONTROL PRO SPLNĚNÍ KRITÉRIÍ PRO ZABEZPEČENÍ, DOSTUPNOST, DŮVĚRNOST, INTEGRITU ZPRACOVÁNÍ A OCHRANU SOUKROMÍ.

PRO OBDOBÍ
OD 1. ČERVNA 2023 DO 30. LISTOPADU 2023

OBSAH

SHRNUTÍ

Rozsah	O2 Czech Republic a.s. (rozsah zahrnutých služeb viz níže)
Hodnocené období	1. června 2023 až 30. listopadu 2023
Uplatnitelné principy důvěry	Zabezpečení, dostupnost, důvěrnost, integrita zpracování a ochrana soukromí
Místa	Praha, Česká republika
Poskytovatelé dílčích služeb	O2 IT services s.r.o.
Výsledek hodnocení	bez výhrad

Služby společnosti O2 Czech Republic a.s. zahrnuté do předmětu zprávy:

- Virtuální datové centrum (VDC)
- Soukromý cloud
- Virtuální datové centrum – SQLaaS
- Zálohování MBR
- Zálohování VDC
- Veeam Cloud Connect
- NGFW Advanced
- NGFW Premium
- O2 AntiDDoS Standard
- O2 Antispam
- Security Expert Centre – SIEM (služby SIEM)
- Security Expert Centre – LM (správa protokolu)
- Security Expert Centre

I. Zpráva nezávislého auditora služeb

I. ZPRÁVA NEZÁVISLÉHO AUDITORA SLUŽEB

Adresát: Představenstvo společnosti O2 Czech Republic a.s.

Účel

U společnosti O2 Czech Republic a.s. („O2 Czech Republic“ nebo „servisní organizace“) jsme posuzovali průvodní popis jejího systému pod názvem „Popis systému servisní organizace společnosti O2 Czech Republic a.s.“ za období od 1. června 2023 do 30. listopadu 2023 (popis), a to na základě kritérií stanovených v odstavci 1.26 Návodu AICPA pro vypracování zpráv ohledně kontrol u servisních organizací relevantních pro zabezpečení, dostupnost, integritu zpracování, důvěrnost a ochranu soukromí (SOC 3®) (popisná kritéria), jakož i trvalou udržitelnost návrhu a provozní efektivitu kontrol zahrnutých do popisu za období od 1. června 2023 do 30. listopadu 2023 pro splnění kritérií zabezpečení, dostupnosti, integrity zpracování a důvěrnosti dle ustanovení části 100 TSP, *Principy, kritéria a ukázky služeb důvěry pro zabezpečení, dostupnost, integritu zpracování, důvěrnost a ochranu soukromí (příslušná kritéria služeb důvěry)*.

Odpovědnosti servisní organizace

O2 Czech Republic poskytla průvodní prohlášení označené „Prohlášení vedení společnosti O2 Czech Republic“ (dále jenom „prohlášení“) o pravdivosti prezentace popisu na základě popisných kritérií a udržitelnosti návrhu a provozní účinnosti kontrol v něm popsaných za účelem splnění platných kritérií služeb důvěry. Společnost O2 Czech Republic je odpovědná za vypracování popisu a prohlášení, včetně úplnosti, přesnosti a způsobu prezentace popisu a prohlášení; uvedení služeb zahrnutých do popisu; identifikaci rizik, které by zabránily splnění platných kritérií služeb důvěry; vypracování návrhu, implementaci a zdokumentování kontrol s trvale udržitelným návrhem a účinný provoz pro splnění příslušných kritérií služeb důvěry uvedených v popisu.

Odpovědnosti auditora služeb

Naší povinností je na základě šetření vyjádřit náš názor na prohlášení vedení, že kontroly v systému byly v období od 1. června 2023 do 30. listopadu 2023 účinné, aby bylo dosaženo rozumné jistoty, že servisní závazky a systémové požadavky servisní organizace byly na základě příslušných kritérií služeb důvěry naplněny.

Naše posouzení probíhalo v souladu se standardy atestace stanovenými AICPA. Tyto standardy vyžadují, abychom naše hodnocení naplánovali a provedli s cílem dosáhnout rozumné jistoty ohledně pravdivosti prohlášení vedení ve všech zásadních ohledech. Věříme, že získané důkazy jsou dostatečné a vhodné pro poskytnutí rozumného odůvodnění našeho názoru.

O2 Czech Republic využívá k poskytování infrastruktury společnost O2 IT services, dílčí servisní organizaci. Popis uvádí, že udržitelně navržené a efektivně provozované kontroly doplňující dílčí servisní organizace jsou společně s kontrolami ve společnosti O2 Czech Republic nezbytné ke splnění servisních závazků a systémových požadavků O2 CZ v souladu

s příslušnými kritérii služeb důvěry. Popis představuje kontroly společnosti O2 CZ, příslušná kritéria služeb důvěry a typy kontrol doplňující dílčí servisní organizace předpokládané v návrhu kontrol společnosti O2 CZ. Naše hodnocení zahrnovalo služby poskytované dílčí servisní organizací a zhodnotili jsme také vhodnost návrhu či provozní účinnost těchto doplňujících kontrol dílčí servisní organizace.

Jedním z požadavků je naše nezávislost a splnění našich etických povinností v souladu s příslušnými etickými požadavky vztahujícími se k zadanému úkolu. Naše posouzení zahrnovalo:

- porozumění systému, servisním závazkům a systémovým požadavkům servisní organizace;
- hodnocení rizik, že kontroly nebudou na základě příslušných kritérií služeb důvěry účinné pro dosažení servisních závazků a systémových požadavků společnosti O2 CZ;
- provádění postupu s cílem zajistit důkazy ohledně toho, zda jsou kontroly v rámci systému efektivní pro dosažení servisních závazků a systémových požadavků společnosti O2 CZ na základě příslušných kritérií služeb důvěry.

Nevyhnutelná omezení

Účinnost jakéhokoliv systému interní kontroly nevyhnutelně zahrnuje určitá omezení, včetně možnosti lidské chyby a obejití kontrol.

V důsledku své povahy nemusí kontroly vždy fungovat efektivně při poskytnutí rozumné jistoty, že servisní závazky a systémové požadavky servisní organizace budou dle příslušných kritérií služeb důvěry splněny. Stejně tak jsou projekce do budoucnosti u jakýchkoliv závěrů ohledně účinnosti kontrol spojeny s rizikem, že takové kontroly se stanou nepřiměřenými v důsledku změny podmínek, nebo v důsledku zhoršení míry dodržování zásad či postupů.

Názor

Dle našeho názoru je prohlášení vedení ohledně toho, že kontroly v rámci zahrnutého rozsahu služeb společnosti O2 CZ byly v období od 1. června 2023 do 30. listopadu 2023 účinné a dokázaly poskytnout rozumnou jistotu, že servisní závazky a systémové požadavky společnosti O2 CZ byly na základě příslušných kritérií služeb důvěry pravdivé ve všech podstatných ohledech.

BDO Audit s.r.o.

31.01.2024

Prohlášení vedení servisní organizace společnosti O2 Czech Republic a.s.

PROHLÁŠENÍ VEDENÍ SERVISNÍ ORGANIZACE SPOLEČNOSTI O2 CZECH REPUBLIC A.S.

Neseme odpovědnost za vypracování návrhů, implementaci, provoz a zajištění údržby účinných kontrol zahrnutých služeb v rámci servisní organizace společnosti O2 Czech Republic (dále jenom „O2 CZ“), a to po celou dobu: od 1. června 2023 do 30. listopadu 2023 s cílem poskytnout rozumnou jistotu, že servisní závazky a systémové požadavky společnosti O2 CZ byly splněny na základě příslušných kritérií služeb důvěry relevantních pro zabezpečení, dostupnost, důvěrnost, integritu zpracování a ochranu soukromí (příslušná kritéria služeb důvěry) stanovených v TSP, části 100, 2017 (aktuální verze 2022), Kritéria služeb důvěry pro zabezpečení, dostupnost, integritu zpracování, důvěrnost a ochranu soukromí v Kritériích služeb důvěry AICPA. Náš popis omezení systému je uveden v příloze A a uvádí aspekty systému, na něž se naše prohlášení vztahuje.

Hodnocení účinnosti kontrol v rámci systému po celé období: od 1. června 2023 do 30. listopadu 2023 jsme provedli s cílem poskytnout rozumnou jistotu, že servisní závazky a systémové požadavky společnosti O2 CZ byly na základě příslušných kritérií služeb důvěry splněny. Cíle společnosti O2 CZ pro systém v rámci uplatňování příslušných kritérií služeb důvěry jsou součástí jejích servisních závazků a systémových požadavků relevantních pro příslušná kritéria služeb důvěry. Hlavní servisní závazky a systémové požadavky týkající se příslušných kritérií služeb důvěry jsou uvedeny v příloze B.

Jakýkoliv systém interní kontroly nevyhnutelně zahrnuje určitá omezení, včetně možnosti lidské chyby a obejití kontrol. V důsledku těchto nevyhnutelných omezení může servisní organizace dosahovat rozumné, nikoliv však absolutní, jistoty, že její servisní závazky a systémové požadavky jsou splněny.

Prohlašujeme, že kontroly uvedené v popisu byly účinně provozovány po celé období: od 1. června 2023 do 30. listopadu 2023 s cílem poskytnout rozumnou jistotu, že servisní závazky a systémové požadavky společnosti O2 CZ byly na základě příslušných kritérií služeb důvěry splněny.

MICHAL KREJČÍK
9. 2. 2024

RADEK SIKTANC
9. 2. 2024

JAN HRUŠKA
9. 2. 2024

II. Příloha A
Popis omezení systému společnosti O2 CZ

II. PŘÍLOHA A

POPIS OMEZENÍ SYSTÉMU SPOLEČNOSTI O2 CZECH REPUBLIC A.S.

O2 Cloud přináší nové možnosti pro budování moderní globální infrastruktury IT. O2 Cloud umožňuje zlepšení služeb zákazníkům, urychlení procesů, omezení provozní složitosti (náklady na instalaci a provoz, správu a kontrolu majetku), stejně jako vyšší zabezpečení.

Služby zabezpečení O2 Security zahrnují firewall budoucí generace, ochranu proti útokům DDoS a nevyžádané poště na ochranu zákazníků komunikujících přes internet, e-mailem či prostřednictvím firemních IT.

O2 Security Expert Centre nabízí díky nástrojům správy protokolu, SIEM a odbornému bezpečnostnímu týmu kompletní ochranu prostředí ICT zákazníka.

Tato zpráva byla vypracována za účelem poskytnutí informací o interních kontrolách společnosti O2, které mohou být relevantní pro zákazníky hledající zabezpečení, dostupnost, integritu zpracování, důvěrnost a ochranu soukromí.

Rozsah zahrnutý do této zprávy zahrnuje následující služby:

Cloudové služby (O2 Cloud)
- Virtuální datové centrum (VDC)
- Soukromý cloud
- Virtuální datové centrum – SQLaaS
- Zálohování MBR
- Zálohování VDC
- Veeam Cloud Connect

Služby zabezpečení (O2 Security)
- NGFW Advanced
- NGFW Premium
- O2 AntiDDoS Standard
- O2 Antispam

Služby Security Expert Centre (O2 SEC)
- Security Expert Centre – SIEM (služby SIEM)
- Security Expert Centre – LM (správa protokolu)
- Security Expert Centre

Rozsah míst, na něž se tato zpráva vztahuje, zahrnuje zařízení nacházející se v České republice:
- Praha, Za Brumlovkou 266/2, 140 00 (sídlo vedení)
- Praha, V lomech 2339/1, 149 00 (datové centrum Chodov)
- Praha, K Zahrádkám 2065/2, 155 00 (datové centrum Stodůlky)

PROFIL SPOLEČNOSTI

O2, přední telekomunikační operátor na českém trhu, nadále plní své poslání nasazovat technologie zlepšující každodenní život lidí. Společnost O2 poskytuje hlasové, internetové a datové služby zákazníkům od domácností přes malé a středně velké podniky až po velké korporace a vládní organizace. Společnost O2 v této chvíli buduje svou mobilní síť páté generace (5G), kterou do komerčního provozu uvedla jako první. Mobilní síť O2 zahrnuje rovněž virtuální operátory nabízející své služby pod názvy BLESKmobil, Tesco Mobile a MOBIL OD ČEZ. Současně je společnost O2 největším poskytovatelem internetu pro domácnosti a podniky, který je nabízen až na 99 % místech.

Díky své službě O2 TV je O2 rovněž největším provozovatelem TV po internetu. Díky zakoupení mnoha sportovních licencí dokáže společnost O2 nabízet svým zákazníkům nejžádanější sportovní obsah na českém trhu. Společnost O2 je také klíčovým hráčem v oblasti služeb hostování a cloudu, stejně jako řízených služeb a ICT. Vzhledem k tomu, že dochází k zásadním proměnám oboru telekomunikací, O2 se rovněž zaměřuje na vývoj a nabídku netradičních telekomunikačních služeb. K těm patří zejména finanční služby, jako jsou pojištění hardwaru nebo mobilní cestovní pojištění.

HLAVNÍ SERVISNÍ ZÁVAZKY A SYSTÉMOVÉ POŽADAVKY

Cílem společnosti O2 Czech Republic je poskytovat telekomunikační služby špičkové kvality. Společnost O2 definuje svou strategii a cíle v souladu se svým posláním přinášet výhody zákazníkům a dosahovat relevantního obchodního zisku.

Servisní závazky:

Společnost O2 Czech Republic efektivně komunikuje své servisní povinnosti svým uživatelům prostřednictvím smluv, dohod o úrovni služeb a zveřejněných zásad. Servisní závazky zahrnují širokou paletu aspektů souvisejících se službami, které organizace poskytuje.

Příklady servisních závazků:

Jako příklad servisního závazku můžeme uvést vysokou míru dostupnosti služby. To znamená, že zákazníci se mohou spolehnout na to, že přístup ke svým telekomunikačním službám budou moci využívat kdykoliv s minimem výpadků.

Systémové požadavky:

Systémové požadavky hrají v podnikání společnosti O2 klíčovou roli. Systémové požadavky byly definovány tak, aby zajistily efektivní služby, splnění všech zákonných požadavků a naplnění cílů společnosti. Systémové požadavky jsou v souladu se Zákonem o kybernetické bezpečnosti (ZoKB), který byl implementován prostřednictvím systémových zásad, postupů, smluv a nařízení.

Příklady systémových požadavků:

Společnost O2 Czech Republic je povinna zabezpečit odpovídající dostupnost systému a jeho schopnost odolat přetížení, aby zákazníci mohli využívat plný potenciál všech

služeb. K tomu patří implementace záložní infrastruktury a neustálé monitorování.

Komunikace závazků a požadavků:

Transparentnost je klíčovou odpovědností vedení společnosti O2 Czech Republic. Díky zveřejnění klíčových servisních závazků a systémových požadavků umožňuje společnost O2 svým uživatelům získat dokonalý přehled o cílech společnosti O2 a vyhodnotit tak účinnost zavedených kontrol.

Důvěryhodnost služby:

Konkrétní servisní závazky a požadavky na systém společnosti O2 Czech Republic mají dopad na to, jak zákazníci vnímají spolehlivost a kvalitu našich služeb. Vysoká úroveň dostupnosti služby hraje klíčovou roli ve vnímání společnosti O2 Czech Republic jako důvěryhodného poskytovatele služeb.

Společnost O2 Czech Republic věnuje mimořádnou pozornost zajištění špičkové dostupnosti služeb. Pro dosažení tohoto cíle společnost zavádí robustní infrastrukturu a zaměřuje se na prevenci selhání systému. Vedle záložních systémů společnost O2 Czech Republic provádí například pravidelné inspekce a údržbu vybavení a infrastruktury pro minimalizaci rizika selhání.

Společnost O2 se zaměřuje na rychlou detekci a řešení případných problémů, které by mohly mít dopad na dostupnost služeb. Společnost O2 Czech Republic disponuje sofistikovanými monitorovacími nástroji a systémy, které umožňují rychlou reakci na případné potenciální incidenty, a to s cílem minimalizovat výpadky nebo omezení přístupu k některým službám.

Společnost O2 Czech Republic současně neustále inovuje a upgraduje své systémy a technologie pro vylepšení jejich funkcí a výkonu ve prospěch svých zákazníků. Společnost O2 pravidelně komunikuje s uživateli a informuje je o všech plánovaných intervalech údržby nebo jiných činnostech s potenciálním dopadem na dostupnost služeb.

Společnost O2 Czech Republic svým zákazníkům zajišťuje vynikající dostupnost služeb. Zavedením robustní infrastruktury, monitorování služeb, rychlé reakce na všechny potenciální problémy a neustálými inovacemi systému poskytuje společnost O2 zákazníkům nepřetržitý spolehlivý přístup ke všem službám.

ORGANIZAČNÍ STRUKTURA

V čele společnosti stojí představenstvo. Generální ředitel (CEO) je odpovědný představenstvu. Linie vedení organizační struktury s odpovědností přímo vůči generálnímu řediteli zahrnuje následující divize a jednotky: komerční divizi, divizi technologií, finanční divizi, divizi právních a regulačních záležitostí, divizi lidských zdrojů, jednotku zabezpečení, jednotku veřejné správy, divizi velkoobchodních služeb, jednotku firemní komunikace a oddělení generálního sekretariátu. Vrcholný management společnosti zahrnuje představenstvo společnosti, technologického ředitele (CTO), obchodního ředitele (CCO). Společnost má rovněž výkonný výbor, který je poradenským orgánem generálního ředitele. Členy výkonného výboru jsou ředitelé obchodní divize, technologické divize, finanční divize, divize právních a regulačních záležitostí, divize lidských zdrojů a oddělení firemní komunikace.

ZÁSADY A POSTUPY

Činnosti společnosti se řídí obecně závaznými právními předpisy, společenskou smlouvou a vnitřními řídicími dokumenty společnosti O2, které upravují veškeré vnitřní řídicí systémy a organizaci.
Řídicí dokumenty podrobně upravují principy, zásady a postupy interních řídicích činností s přihlédnutím k jejich specifickému významu, místu, technologii, cílům a dalším relevantním parametrům. Řídicí dokumenty na základě strategie, zásad a cílů společnosti detailně zapracovávají veškeré mandatorní prvky externí legislativy do podmínek společnosti.
Zásady správy a řízení systému dokumentů řízení společnosti jsou definovány v samostatném dokumentu.

PROSTŘEDÍ KONTROL

Společnost zavedla systém interních kontrol popsaný v řídicích dokumentech, který byl schválen představenstvem. Významnou roli v tomto systému hraje jednotka označovaná jako Interní audit společnosti O2, která je funkčně podřízena představenstvu. Interní audit poskytuje orgánům společnosti nezávislé a profesionální hodnocení systému interních kontrol a řízení, přičemž stav a vývoj posuzovaných oblastí jsou hodnoceny podle stávajících doporučených postupů. Interní audit navíc plní funkce interního auditu pro dceřiné společnosti O2. V závislosti na zjištěních auditu příslušní manažeři přijímají odpovídající nápravná opatření. Vnitřní audit společnosti O2 monitoruje, jak se se zjištěními nakládá a výsledky hlásí orgánům společnosti. Principy realizace interního auditu, včetně principů nezávislosti a objektivity, jsou popsány ve stanovách IA O2.

Základní princip uplatňovaný v účetních postupech společnosti zahrnuje kontrolu založenou na principu „čtyř očí“ a oddělení procesu vytváření a správy dat obchodního partnera od procesu plateb a vypořádání zaúčtovaných závazků. Současně je omezen počet lidí, kteří jsou oprávněni vytvářet, upravovat a schvalovat účetní záznamy v systému SAP a jejich seznam je pravidelně monitorován. Pro jednotlivé účetní doklady lze vždy identifikovat konkrétního uživatele, který doklad vytvořil nebo zrušil. Správnost účetních a finančních záznamů je průběžně kontrolována finanční divizí. Vybrané oblasti účetnictví a soulad interních procesů s platnou legislativou a interními pokyny a postupy ověřuje jednotka interního auditu. V případě nesouladu jsou neprodleně přijímána a uplatňována nápravná opatření. Účinnost systému interních kontrol, proces vytváření jednotlivých konsolidovaných daňových výkazů a proces externího auditu jsou monitorovány představenstvem.

Finanční divize zahrnuje oddělení nazvané „Zajištění příjmu“, jehož cílem je odhalovat potenciální ztráty příjmů v důsledku úniků dat. Tento komplexní proces zahrnuje veškeré účetní činnosti od iniciace CDR až po vystavení faktury zákazníkovi (účet).

Kontrolní prostředí zahrnuje také uplatňování, soulad a kontroly souladu s požadavky norem ISO pro řídicí systémy, zavedené v rámci integrovaného systému řízení. S ohledem na rozsah této zprávy jsou relevantní zejména následující normy:

- ISO 20000-1 Informační technologie – Řízení služeb,
- ISO 27001 Informační technologie – Techniky zabezpečení – Systém řízení zabezpečení informací doplněné požadavky normy ISO 27017 Informační technologie – Techniky zabezpečení – Postupy pro kontroly zabezpečení informací na základě normy ISO/IEC 27002 pro cloudové služby a normy ISO 27018

Informační technologie – Techniky zabezpečení – Postupy pro ochranu osobně identifikovatelných informací (OII) ve veřejných cloudech, které fungují jako zpracovatelé OII,
- ISO 22301 Zabezpečení a odolnost – Systém řízení kontinuity podnikání.

Soulad s výše uvedenými normami je kontrolován prostřednictvím interních auditů, pravidelných certifikací a inspekčních auditů prováděných renomovanými certifikačními orgány.

INFORMACE A KOMUNIKACE

Efektivní komunikace posiluje kontakt s lidmi a zlepšuje pochopení potřeb a očekávání externích a interních zákazníků, což přispívá k efektivnímu fungování společnosti.

Pro komunikaci se zákazníky platí ve společnosti O2 pět základních zásad (1. Říci vše, co je důležité, 2. Říkat pravdu, 3. Zajistit zpětnou kontrolu požadavků zákazníka, 4. Reprezentovat společnost O2, 5. Vystupovat slušně), přičemž tyto komunikační zásady je třeba uplatňovat v rámci celé společnosti, včetně interní komunikace.

Ve společnosti O2 je základním informačním kanálem pro všechny zaměstnance intranet, stejně jako e-mailová komunikace či SMS. Kromě elektronických kanálů jsou informace poskytovány rovněž osobně během jednání, setkání s vrcholným vedením nebo na setkáních mimo pracoviště.
Interní komunikace zahrnuje například komunikaci zásad a postupů společnosti O2, nové iniciativy a upozornění na informace a kybernetickou bezpečnost. Zavedeny jsou rovněž roční procesy stanovení cílů pro všechny vedoucí pracovníky, které jsou následně oznamovány zaměstnancům. Tyto cíle jsou předávány členům týmu prostřednictvím ročního a pololetního hodnocení.

Externí komunikace je zajišťována příslušnými funkcemi a rolemi v rámci společnosti: např.:
- komunikace se zákazníky: prodejní poradci, operátoři call centra, account manažeři, servisní manažeři, linka pomoci atd.;
- komunikace s veřejností a médii: jednotka firemní komunikace,
- komunikace s dodavateli: oddělení nákupu, logistiky, vedení prodeje, úřad strategie CTO,
- komunikace krizového řízení: krizový tým.

Pro externí komunikaci se využívá celá škála kanálů, včetně osobních setkání, telefonických hovorů až po elektronické nástroje jako jsou e-mail, chat, sociální sítě a firemní webové stránky, www.o2.cz.

MONITOROVÁNÍ

Monitorování provozu a bezpečnosti

Společnost O2 udržuje rozumná a přiměřená technická a organizační opatření, interní kontroly a postupy zabezpečení informací na ochranu svých informačních aktiv stejně jako dat všech zákazníků před náhodnou ztrátou, zničením nebo pozměněním, neoprávněným poskytnutím či přístupem nebo nezákonným zničením.
Společnost O2 využívá ke sledování provozu a zabezpečení množství automatizovaných monitorovacích systémů pro zajištění špičkového výkonu a dostupnosti služeb. Monitorování se využívá na úrovních uživatelských aplikací, uživatelských stanic, serverů a technologických stanic, bezpečnostních zařízení a síťových prvků. Vybrané body připojení sítě O2 s veřejnými datovými sítěmi a rozhraní mezi vybranými bezpečnostními zónami jsou monitorovány IDS. Provoz mezi veřejnými sítěmi, sítěmi třetích stran a sítí společnosti O2 je kontrolován prostřednictvím firewallu. Konfigurace firewallů vychází z principu „co není povoleno, je zakázáno".
Monitorování provozu a zabezpečení je sledováno příslušnými procesy řízení incidentů, včetně řízení zabezpečení pro případ incidentu.
Požadavky na provozní monitorování prvků informačního systému splňují veškeré legislativní požadavky (zejména pak GDPR) a samostatné řídicí dokumentace.
Jako poskytovatel cloudových služeb společnost O2 poskytuje zákazníkům možnosti protokolování v závislosti na typu služby a monitorování fungování (provozu) těchto cloudových služeb.

Interní audit
Ve svém dokumentu Naše obchodní principy (viz níže) definuje společnost O2 svůj závazek uplatňovat odpovídající kontrolní mechanizmy na hodnocení a řízení rizik pro společnost O2, její zaměstnance a její pověst. Z tohoto důvodu společnost založila jednotku interního auditu, aby byla zajištěna účinnost všech procesů interního řízení a řízení rizik orgánů a vedení společnosti, stejně jako dodržování doporučení řádných postupů firemního řízení. Interní audit je nezávislá a objektivní činnost vycházející z filozofie přidané hodnoty díky zlepšení interních operací společnosti. Interní audit pomáhá společnosti O2 dosahovat cíle díky systematickému metodickému postupu hodnocení a zvyšování efektivity systému řízení rizik, procesů řízení a kontroly a firemního řízení. Činnosti interního auditu se řídí zásadami Mezinárodního rámce profesionálních postupů (IPPF): a) klíčovými principy, b) Kodexem jednání, c) normami, d) definicí interního auditu. Činnosti auditu jsou dále prováděny v souladu s příslušnými právními předpisy a interními řídicími dokumenty, které upravují provádění interního auditu. Interní audit poskytuje nezávislé a objektivní ujištění, že společnost zajišťuje: soulad s požadavky právních předpisů a dalšími povinnými požadavky, spolehlivost informací, účinnost procesů řízení rizik, opatrné hospodaření a ochranu aktiv společnosti.
Interní audit společnosti O2 hraje roli ve třetí linii obrany v rámci modelu tří linií IPPF. V tomto modelu představuje první linii obrany provozní management, druhou linii různé funkce rizik a kontroly souladu, které jsou součástí řízení společnosti O2, zatímco třetí linie zahrnuje nezávislé ověřování.

KODEX JEDNÁNÍ A ETIKA

Společnost dodržuje doporučení Českého kodexu firemního řízení z roku 2018, jehož obecné zásady vycházejí z platné legislativy České republiky. Doporučení jsou inspirována rovněž srovnatelnými národními kodexy firemního řízení (zejména pak německým a rakouským kodexem) a mezinárodními normami firemního řízení (zejména pak Principy firemního řízení G20 / OECD z roku 2015). Odpovědnost za podporu zajištění firemního řízení a vedení, včetně plnění požadavků Českého kodexu firemního řízení z roku 2018, nese sekretariát společnosti, který je organizačně součástí divize

právních a regulačních záležitostí.
Kodex dodržování předpisů je součástí interní kultury společnosti O2 Czech Republic a.s. a představuje její přístup k dodržování právních předpisů upravujících normy etiky a odpovědného podnikání. Opatření vycházející z výše uvedených zásad se označují jako „program souladu s předpisy“ a zaměřují se to, aby bylo dodržování zásad součástí priorit vedení společnosti O2. Primárním cílem těchto opatření je nastavit v rámci společnosti O2 interní mechanizmy, aby se zabránilo veškerým nezákonným činnostem, a v případě, že k nim dojde, aby byly identifikovány a aby na ně bylo vhodným způsobem reagováno.
Společnost O2 má komplexní a propojený systém vnitřních předpisů a postupů pro zajištění dodržování zákonů a nařízení. Výchozím a ústředním bodem jsou „Naše obchodní principy“, které představují zdroje hodnot a principy pro definování našich vnitřních předpisů. Mnoho vnitřních předpisů výslovně odkazuje na Naše obchodní principy, podporuje povědomí o principech a jejich význam. Všechny oblasti popsané v Našich obchodních principech tvoří tradiční součást právního řádu země. Společnost O2 ve svých interních předpisech dále popisuje způsob, jakým mají její zaměstnanci a orgány postupovat v případě specifických situací v souladu s interními procesy O2.

Tento systém je vnímán jako opatření ve smyslu ustanovení § 8, odst. 2 zákona č. 418/2011 Sb.

Naše obchodní principy jsou jak vnitřním předpisem schváleným představenstvem, tak dokumentem zveřejněným na webových stránkách společnosti O2 (v části „Odpovědný přístup“). Původní verze těchto obchodních principů je v českém jazyce. Naše obchodní principy jsou k dispozici i na anglické verzi webových stránek společnosti O2.
Za obsah a aktualizaci školení nese odpovědnost úředník pro soulad s předpisy. Cílem školení je vysvětlit zaměstnancům obsah a význam Našich obchodních principů a základní principy a zásady vyplývající z klíčových vnitřních předpisů, které musí všichni zaměstnanci dodržovat pro eliminaci rizika nezákonného jednání. Základní verze školení je povinná pro všechny zaměstnance společnosti O2.

Pracovněprávní zásady upravují základní povinnosti všech zaměstnanců společnosti O2 vyplývající z jejich pracovněprávního vztahu. Pracovněprávní zásady vycházejí z Našich obchodních principů. Jejich nedílnou součást tvoří Zásady přijímání a poskytování darů a pohostinství a Zásady konfliktu zájmů.

Zásady pro podepisování jsou dalším klíčovým vnitřním předpisem, který upravuje vnitřní postupy zaměstnanců společnosti O2 při jednání ve jménu společnosti O2 navenek.

Pro dosažení cílů stanovených v Kodexu dodržování předpisů a pro zajištění prevence zavedla společnost O2 interní systém hlášení (whistleblowing) jako základní prvek pro hlášení stížností ohledně potenciálně nezákonného jednání s dopadem na společnost O2. Whistleblowerovi, který splní podmínky pro podání hlášení v souladu se Zákonem o ochraně whistleblowerů, je zajištěna odpovídající ochrana.

PROCES HODNOCENÍ RIZIK

Řízení rizik je jedním ze základních nástrojů efektivního systému řízení společnosti, jehož cílem je poskytovat podporu při plnění vize a strategie společnosti. Systém řízení rizik je vyvinut jako integrální nástroj vnitřní kontroly společnosti. Riziko se identifikuje na základě pravidelného hodnocení příslušnými manažery, na základě návrhů Řízení rizik a dalších jednotek společnosti. Rizika jsou hodnocena z perspektivy potenciálního finančního dopadu a pravděpodobnosti výskytu. Členové představenstva jsou průběžně informováni o všech zásadních rizicích pro společnost, jakož i o způsobech jejich řízení.

Řízení provozních rizik v oblasti zabezpečení informací a kontinuity podnikání probíhá v souladu s příslušnou metodologií. Metodologie se provozuje na místních serverech společnosti O2. V souladu se zákonnými požadavky pro kybernetickou bezpečnost jsou v těchto hodnoceních provozních rizik zohledněny relevantní hrozby a slabá místa. Osoby odpovědné za implementaci obchodních plánů a trvale udržitelný vývoj společnosti musí přihlédnout k následujícím třem oblastem:

- potenciální škody způsobené bezpečnostním selháním;
- skutečná pravděpodobnost relevantních slabých míst v důsledku převládajících hrozeb ve srovnání se zavedenými bezpečnostními opatřeními;
- význam slabých míst aktiv pro možné hrozby.

Společnost O2 provádí hodnocení rizik pro všechny systémy společnosti a situace vyplývající z kontextu organizace.

ŘÍZENÍ LIDSKÝCH ZDROJŮ

Obchodní úspěch a prosperita podnikání společnosti O2 závisí nejenom na dlouhodobém vztahu se zákazníky, kteří společnost O2 vnímají jako stabilního, silného a spolehlivého partnera, který uchová veškerá data zákazníků v důvěrnosti. Aby nedošlo k podkopání důvěry zákazníků při plnění jejich očekávání, k ohrožení naší pověsti a s cílem vyloučit z veřejných projektů rizika, naše zaměstnance pro specifické pozice vybíráme pečlivě jak z hlediska kvalifikace, tak integrity.

Výběr zaměstnanců je postaven na jasných kritériích z hlediska bezpečnostní vhodnosti, důvěryhodnosti, spolehlivosti a čistého trestního rejstříku. Kritéria jsou u každého zaměstnance revidována jak před, tak během jeho pracovněprávního poměru, a to v souladu s postupy upravenými v našich Bezpečnostních předpisech. Kritéria výběru zaměstnanců jsou stanovena divizí lidských zdrojů a veškeré bezpečnostní aspekty jsou konzultovány s jednotkou Zabezpečení.

V závislosti na typu citlivých informací musí všichni zaměstnanci, kteří při výkonu své funkce přicházejí do styku s citlivými informacemi, podepsat příslušné prohlášení o zachování důvěrnosti.

Zaměstnanci společnosti O2 musí povinně absolvovat kurzy zahrnující různá témata, včetně Našich obchodních principů, ochrany informací a GDPR. Školení je nutno pravidelně opakovat. Bezpečnostní školení je povinné pro všechny zaměstnance společnosti O2 a všechny externí (nezávislé) osoby a organizace pracující v prostorách společnosti O2.

Na všechny zaměstnance se vztahuje pravidelné Hodnocení výkonu a talentu. Hodnocení zahrnuje plnění individuálních cílů, jednání a přístup, což zahrnuje také dodržování firemní kultury, komunikaci a spolupráci v rámci týmu, stejně jako aktivní, logický a efektivní přístup k řešení problémů. Výsledek hodnocení zahrnuje také identifikaci potřeb dalšího vzdělávání a individuálního rozvoje.

KLÍČOVÉ ODPOVĚDNOSTI

Ve společnosti O2 odpovědnosti stanovují především Organizační zásady, které shrnují základní informace o společnosti, určují systém vnitřního řízení a organizace, definují odpovědnosti jednotlivých firemních orgánů, jednotek a jednotlivých zaměstnanců, stanovují linie odpovědnosti jednotek a odpovědnost vůči orgánům společnosti, včetně systému dokumentace vnitřního řízení.

S ohledem na služby popisované v této zprávě SOC3 hrají klíčovou roli následující jednotky společnosti O2:
Týmy řízení produktu zajišťují a koordinují vývoj produktů a služeb, včetně jejich uvedení na trh; řídí životní cyklus produktů a služeb.
Síťové týmy se starají o provoz služeb zabezpečení společnosti O2, včetně provozu nezbytné infrastruktury; další týmy se věnují poskytování služeb SEC O2 zákazníkům společnosti O2, a to včetně provozu nezbytné infrastruktury.
Jednotka Zabezpečení definuje a uplatňuje strategii a bezpečnostní zásady společnosti, řídí a definuje bezpečnostní opatření, propaguje zavádění opatření a kontroluje jejich dodržování ve všech oblastech fyzického, informačního a kybernetického zabezpečení.

Dodavatelé využívaní společností O2, jmenovitě CETIN (sesterská organizace) a společnost O2 IT Services (dceřiná organizace) nesou rovněž velký díl odpovědnosti.

Společnost CETIN vlastní datové centra využívaná společností O2 pro provoz jejích cloudových služeb. Společnost CETIN tedy společnosti O2 poskytuje služby pro provoz infrastruktury mimo IT, nese odpovědnost za dostupnost, stejně jako za fyzickou ochranu datových center a přístup k datovým centrům. Datová centra jsou certifikována pro TIER/RATE III.
Společnost O2 IT Services provozuje hardware a virtualizační platformu, které se využívají pro cloudové služby společnosti O2, a zabezpečuje poskytování linky pomoci.

SYSTÉMOVÉ KOMPONENTY VYUŽÍVANÉ PRO POSKYTOVÁNÍ SLUŽBY

Infrastruktura

Cloudové a zálohovací služby
Poskytování cloudových a zálohovacích služeb je rolí společnosti O2 ITS, organizace odpovědné za provozní část služeb, jako jsou O2 VDC, Soukromý cloud O2, Zálohování VDC O2 a Zálohování O2. Služby jsou provozovány v datových centrech společnosti CETIN ve dvou lokalitách, Praha Chodov (DC CH) a Praha Stodůlky (DC JZM) s nepřetržitým monitorováním.
Serverová infrastruktura je vystavěna na farmě serverů od předních světových dodavatelů ve spojení s nejmodernějšími virtualizačními technologiemi s vysokou mírou

dostupnosti. Všechny servery včetně infrastruktury jsou propojeny záložním způsobem pro minimalizaci odstávek kvůli selhání technologií. Garantovaná dostupnost služby je 99,9 %.

Firewall O2 příští generace
NGFW je navržen na základě koncepce koncentrace prvotřídních bezpečnostních prvků HW a centralizovaného zabezpečení na jednom místě. Je tomu tak, neboť toto řešení poskytuje přednosti z hlediska nákladů, výkonu a odolnosti, které chybějí u koncepce rozprostřeného zabezpečení. Díky využití centralizovaného zabezpečení lze dosáhnout stejné či vyšší úrovně zabezpečení při nižších nákladech na pořízení a provoz.

Centralizované služby přes komunikační infrastrukturu dramaticky snižují pravděpodobnosti proniknutí z vnějšího prostředí do interního IT prostředí zákazníka a vytvářejí podmínky k tomu, aby zákazník a poskytovatel mohli lépe koordinovat své kroky ve snaze o boj s potenciálními hackery.
NGFW je geograficky záložní infrastruktura zabezpečení vyvinutá zálohováním produktivních prvků do dvou identických větví umístěných na dvou různých místech, čímž lze dosáhnout skvělou spolehlivost a dostupnost služby. NGFW se nachází v hostovacích centrech, která splňují přísné bezpečnostní požadavky s přísnými parametry, které jsou navrženy a provozovány na úrovni Vrstvy III (v souladu s klasifikací Uptime Institute).

Prostředí splňuje následující požadavky na zabezpečení výpočetního výkonu a komunikace:

- záložná datová konektivita je připojena ke dvěma nezávislým směrům zakončeným na samostatné technologii v různých budovách/zařízeních;
- komunikační infrastruktura používaná pro poskytování služeb je technicky a geograficky zálohovaná;
- komunikační infrastruktura je umístěna do bezpečného prostředí hostovacího centra nebo rovnocenného prostředí;
- přístup k řídicímu systému prvků a služeb (místní a vzdálený) je kontrolován v prostředí odděleném od zákaznického prostředí; a
- infrastruktura je kontrolována zkušenými odborníky s odpovídajícími certifikacemi.

Bezpečnostní požadavky jsou zaručeny a dodržovány po celou dobu trvání smlouvy. Síť O2 CZ ISP se skládá ze dvou nezávislých lokalit poskytujících konektivitu na rovnocenné úrovni.

O2 AntiDDoS
Síť O2 CZ ISP se skládá ze dvou nezávislých lokalit poskytujících konektivitu na rovnocenné úrovni, místní rovnocennou konektivitou (NIX) a konektivitou pro přenos přes internet zajišťovanou několika různými poskytovali pro odchozí data (Tier1 ISPs).

Ve vztahu k AntiDDoS využívá společnost O2 platformu zavedenou do sítě s ohledem na různé parametry jako jsou velikost, zeměpisné umístění atd.

Implementace zahrnuje 3 části:
- CP zahrnující analytickou část systému,
- TMS obsahující část pro zmírnění,
- PI - portálové rozhraní pro zákazníky.

Veškeré změny konfigurace TMS se provádějí v zařízení CP. Zařízení CP vytváří rovnocenné propojení BGP s dotčenými směřovači (hraniční směřovače ISP) jako jsou hostitel BGP (RRC route reflector client) a přijímá všechna oznámení BGP přijatá nebo přeposlaná směřovači ISP. Zařízení CP je připojeno k hraničním směřovačům pro příjem dat NetFlow, které se používají jako hlavní zdroj pro analýzu chování a provozu. Poté, co zařízení CP určitou část provozu označí za podezřelou, do TMS se vyšle požadavek na přesměrování BGP podezřelého provozu pro další šetření. Pokud bude provoz klasifikován jako útok typu DoS/DDoS, TMS nežádoucí provoz vyloučí nebo jej odešle zpět původní trasou pro pozdější doručení zpět do místa určení.

O2 Antispam
O2 Antispam je služba využívající systém ke zjišťování spamu. Služba je v podstatě veřejnou e-mailovou bránou v infrastruktuře společnosti O2, v níž je vytvořen jedinečný účet pro uživatele pro správu bezpečnostních zásad chráněné domény nebo několika domén Next v místě poskytovatele domény s použitím záznamu MX, pro provedení změny doručování na e-mailovou bránu, což slouží jako ochrana. E-mailová brána následně uživateli nabídne řešení celkového zabezpečení jako službu se zohledněním množství různých internetových hrozeb.

Malware (tj. viry, trojské koně, spyware, etc.), spam, slabá místa, sítě infikovaných počítačů (botnety), podvodné e-maily, soubory a webové stránky (phishing a pharming) a mnohé další představují potenciální bezpečnostní hrozby pro firmy a jejich podnikání. Kromě vlastní funkce ochrany proti spamu O2 Antispam nabízí také karanténu pro zachycené zprávy (pro odstranění „falešně pozitivních“ případů). Službu lze zavést samostatně, takže se nevyžadují další služby jako je NGFW.

O2 Security Expert Centre
Cílem nasazení O2 SEC je posílit zabezpečení prostředí IT a získat přehled o tom, co se děje v síti a koncových bodech pro snazší včasnou identifikaci a eliminaci aktuálních hrozeb.
Služba poskytuje následující funkce:

- shromažďování, ukládání a analýza protokolů definovaných systémů,
- monitorování zabezpečení (aniž by zákazník musel provádět monitorování interně),
- centrální model monitorování/kontroly zabezpečení pro všechny organizace ve skupině.

Služba využívá nástroje poskytované v rámci služby provozované společností O2. V místě zákazníka se aplikují sondy HW/SW určené ke sledování provozu v síti (síťové sondy). Nástroje zahrnují především:

- správu protokolu,
- SIEM.

Tato služba zahrnuje kombinaci komplementárních služeb zaměřených na ochranu zákazníků proti všem druhům kybernetických hrozeb, které mohou obejít standardní obvodovou ochranu, antivirové systémy, a představují dlouhodobou nebo trvalou hrozbu pro bezpečnost a podnikání zákazníka; současně také vytváří prostředí odpovídající všem legislativním požadavkům. O2 SEC zahrnuje nepřetržité monitorování s proaktivní bezpečnostní kontrolou a pravidelnou revizí událostí kybernetické bezpečnosti. Nabízené řešení poskytuje prostředí s více uživateli, což zákazníkovi umožňuje vybrat nastavení formy viditelnosti pro jednotlivé dozorované subjekty, tj. selektivní přístup z hlediska zásad a hlášení.

Protokoly se shromažďují ze zařízení určených zákazníkem a odesílají do tzv. kolektorů. Kolektor je sběrný bod v síti zákazníka, nainstalovaný jako virtuální zařízení v uspořádání HA v síti DMZ zákazníka.
Kolektory jsou připojeny k firewallu v O2 Security Expert Centre přes zabezpečené připojení (VPN, TLS atd.). Procesory toku dat zpracovávají protokoly s využitím funkcí správy protokolu, SIEM v reálném čase či nikoliv. Řešení je vytvořeno jako klastr aktivní - aktivní HA.

Služba O2 SEC zahrnuje systémy pro zjišťování anomálií v síťovém provozu. Systém monitoruje prostředí O2 SEC jako celek a zajišťuje záznamy pro audit. Další částí O2 SEC je tiketovací systém používaný jako jeden z komunikačních kanálů mezi O2 SEC a zákazníkem. Zákazníci mohou využívat webové rozhraní.
Nabízené řešení je navrženo jako vysoce dostupné (HA) s implicitním vyvažováním zatížení.

Software

Cloudové a zálohovací služby

Cloudové a zálohovací služby jsou strukturovány do několika POD, které představují klastry vzájemně propojených serverů s hypervizorem. Klastry umístěné v datových centrech poskytují výpočetní výkon pro provoz zákaznických prostředí. Rolí hypervizoru plní přední virtualizační platforma na trhu, která běží na vrstvě s více uživateli, portálu, který zákazníkům umožňuje spravovat jejich prostředí. Všechny servery v klastrech jsou vybaveny disky SSD a využívají vSAN pro zajištění vyšší rychlosti a dostupnosti dat.
V obou datových centrech jsou oddělená POD pro SQLaaS. POD jsou optimalizovány pro provoz SQL a obsahují vysokofrekvenční CPU. Servery v POD jsou plně licencovány pro spouštění databází SQL. Společně s infrastrukturou se pro následující služby nabízejí licence SPLA: Standardní licence OS Windows server, licence RDS, aplikační licence pro MS SQL verze Standard a Enterprise, licence RHEL.
Služba Zálohování VDC využívá specializovaný software Veeam, který nabízí pokročilé funkce pro zálohování a obnovu dat ve virtualizovaném prostředí.

Firewall O2 příští generace

Společnost využívá firewall, který propojuje všechny bezpečnostní a síťové komponenty pro zajištění bezproblémové integrace. To umožňuje konvergenci síťových a bezpečnostních funkcí pro zajištění konzistentní zkušenosti zákazníků a odolnou pozici co se týče bezpečnosti ve všech typech prostředí, včetně místních, cloudových, hybridních a konvergovaných infrastruktur IT/OT/IoT.

O2 AntiDDoS

Společnost využívá řešení používané ke zjišťování útoků typu DDoS. Systém vám umožňuje monitorovat síťový provoz a využívat data pro chytrou analýzu provozu, optimalizaci využití, inteligentní plánování rozšiřování sítě, eliminaci hrozeb a poskytování hlášení zákazníkům a uživatelům.
Systém dokáže odstranit škodlivé části komunikační relace bez narušení dalších klíčových síťových služeb.

O2 Antispam

Společnost využívá operační systém, který patří k největším platformám kybernetické bezpečnosti na trhu a byl původně vytvořen na společném rámci řízení a zabezpečení. Propojuje všechny nezbytné bezpečnostní a síťové komponenty pro zajištění

bezproblémové integrace. To umožňuje konvergenci síťových a bezpečnostních funkcí pro zajištění konzistentní zkušenosti zákazníků a odolnou pozici co se týče bezpečnosti ve všech typech prostředí, včetně místních, cloudových, hybridních a konvergovaných infrastruktur IT/OT/IoT.
Systém se rozvíjí organicky a je posilovaný o nové funkce pro zvyšování potenciálu poskytovat nesrovnatelný přehled a uplatňování zásad v rámci hybridních prostředí. Tento systém navíc urychluje bezpečnostní operace díky prevenci založené na AI, automatizaci a odezvě v reálném čase. Systém dále nabízí řízení bezpečné sítě, zvýšenou prevenci, včasnou detekci a odezvu v reálném čase, stejně jako omezení rizik s ohledem na různé kybernetické hrozby.

O2 Security Expert Centre
O2 SEC klade kybernetickou bezpečnost na 1. místo a používá k tomu profesionální nástroje od renomovaných výrobců. Pracoviště má sofistikovaný softwarový ekosystém navržený pro monitorování a okamžitou identifikací všech potenciálních kybernetických hrozeb. Software používaný pro správu protokolů a služby SIEM umožňuje soulad s příslušnými předpisy v oblasti kybernetické bezpečnosti, GDPR a s normou ISO 27001.

Lidé

Samotný provoz a vývoj cloudových služeb vyžaduje zapojení několika různých rolí od technických až po komerční. Odpovědnost za provoz těchto služeb nese společnost O2 IT Services, která se stará o technický provoz služby, včetně linky pomoci. Provoz bezpečnostních služeb zajišťuje společnost O2 Czech Republic. Klíčové technické role pro cloudové služby zahrnují architekta řešení, servisního manažera a provozního specialistu. Komerční, bezpečnostní a síťová infrastruktura patří mezi role společnosti O2 Czech Republic. K těmto rolím patří produktový manažer, segmentový manažer, manažer prodeje a předprodeje, bezpečnostní specialista a specialista na síťovou infrastrukturu. Všechny role bezpečnostních služeb poskytuje společnost O2 Czech Republic. Pro potvrzení úrovně dovedností našich základních poskytovatelů služeb, VMware, Veeam Software a Fortinet, udržujeme jistou úroveň partnerství, což je prvek vyžadovaný mnoha specializovanými certifikacemi. Naše úrovně partnerství si můžete prohlédnout na webových stránkách našich dodavatelů – VMware, Veeam Software a Fortinet. Naším cílem je neustále zvyšovat úroveň partnerství a dovedností, což potvrzují certifikace dosažené našimi speciality.
Služby O2 Security Expert Centre jsou poskytovány zkušeným bezpečnostním personálem. Ke klíčovým bezpečnostním rolím patří Bezpečnostní operátor úrovně 1 (nepřetržitě pracující tým operátorů úrovně 1 je pověřený dohledem nad zabezpečením, hodnocením výstrah a událostí z monitorovacího systému), bezpečnostní analytik úrovně 2 (analytici úrovně 2 pracují v režimu 8 hodin denně 5 dní v týdnu s pohotovostními službami mimo naši běžnou provozní dobu a k jejich úkolům patří hlubší analýza na základě zjištění úrovně 1, hlášení a komunikace se zákazníky) a bezpečnostní architekt úrovně 3 (tým architektů úrovně 3 pracuje v režimu 8 hodin denně 5 dní v týdnu s možností pohotovostních služeb mimo naši běžnou provozní dobu, a k jeho úkolům patří komunikace s dodavateli, nábor a technická podpora pro ostatní týmy).
Kompetentní správce systému nese odpovědnost za konfiguraci a odstraňování přístupových účtů ke službám. Činnosti správce se provádějí v souladu s vnitřními předpisy. Pravidelné kontroly přístupu probíhají jednou ročně, aby se zajistilo, že veškeré přístupy jsou řádně kontrolovány a jsou v souladu s definovanými bezpečnostními požadavky. To zabezpečuje, že data a systémy jsou chráněny před neoprávněným přístupem a zneužitím. Správci systému hrají klíčovou roli při správě

přístupových účtů a dodržování bezpečnostních standardů.

Postupy

Společnost O2 Czech Republic je odhodlána udržovat špičkové zabezpečení svých systémů a infrastruktury. To zahrnuje zabezpečení příslušné důvěrnosti, integrity a dostupnosti dat a systémů prostřednictvím vnitřních zásad a postupů.
Společnost O2 Czech Republic v rámci svého integrovaného systému řízení zavedla jednotný systém správy zásad a předpisů. Zásady a postupy se týkají servisních postupů, včetně řízení a vypracování návrhu životního cyklu produktů a služeb, řízení procesu zákazníka (registrace a odchod zákazníka), procesů řízení změn, monitorování provozu, řízení nehod a dalších. Cílem zásad a postupů je zajistit zabezpečení a ochranu dat a systémů. Společnost O2 Czech Republic pravidelně reviduje a aktualizuje své zásady a postupy, aby byl zajištěn jejich soulad s nejnovějšími bezpečnostními normami a technologiemi.
Společnost O2 se současně intenzivně zaměřuje na vytváření a uchovávání povědomí o bezpečnosti mezi zaměstnanci. O2 Czech Republic zabezpečuje školení a vzdělává své zaměstnance, aby dokázali rozpoznat bezpečnostní hrozby a reagovat na ně.
Tímto přístupem společnost O2 Czech Republic prokazuje své odhodlání udržovat bezpečné prostředí pro své zákazníky a chránit citlivé informace. Bezpečnost a ochrana představují prioritu č. 1 společnosti O2 Czech Republic, a jsou nedílnou součástí našeho podnikání. Společnost O2 Czech Republic si je vědoma neustálého rozvoje bezpečnostních hrozeb a slabých míst. S tímto vědomím pravidelně monitorujeme a revidujeme naše systémy a infrastrukturu, abychom identifikovali veškeré potenciální bezpečností rizika a přijali účinná opatření pro minimalizaci jejich výskytu.

Společnost O2 Czech Republic navíc spolupracuje s odborníky na informační bezpečnost a sleduje nejnovější trendy a technologie, které jí mohou pomoci v reakci na nové hrozby, a zavádí doporučené postupy a opatření pro zajištění odpovídajícího zabezpečení.
Ochrana soukromí zákazníků představuje další významný aspekt zabezpečení. Společnost O2 Czech Republic dodržuje veškeré příslušné zákony a nařízení týkající se ochrany osobních údajů a zavázala se ke správnému a bezpečnému zpracování takových údajů. Zákazníci společnosti O2 mají jistotu, že jejich údaje jsou chráněny a zpracovávány s maximální péčí a bezpečností.
Společnost O2 Czech Republic věnuje mimořádnou pozornost zabezpečení, stejně jako ochraně osobních údajů a systémů. Závazek zachování bezpečnosti prokazujeme v několika klíčových oblastech, jako je:

- Bezpečnostní infrastruktura: společnost O2 Czech Republic investuje do moderních bezpečnostních technologií a infrastruktury, aby dokázala zjistit potenciální hrozby a reagovat na ně. Společnost například využívá pokročilé firewallové systémy a systémy pro detekci a prevenci útoků.
- Monitorování a detekce: společnost O2 Czech Republic pravidelně monitoruje své systémy a sítě s cílem identifikovat podezřelou činnost či anomálie. V případě zjištění potenciálního bezpečnostního incidentu společnost neprodleně reaguje a podniká kroky pro minimalizaci škod.
- Školení zaměstnanců: společnost O2 Czech Republic si je vědoma, že bezpečnostní opatření mohou být účinná, pouze pokud budou její zaměstnanci řádně informováni a vyškoleni. S tímto vědomím společnost O2 svým zaměstnancům poskytuje pravidelná školení, aby je informovala o největších bezpečnostních hrozbách a doporučených postupech pro ochranu dat a hardwaru.
- Ochrana proti úrokům typu DDoS: společnost O2 Czech Republic rovněž poskytuje

ochranu proti úrokům typu DDoS (Distributed Denial of Service) a opatření proti spamu. Úroky typu DDoS mají za cíl zahltit cílovou síť nebo webový server pro zamezení přístupu uživatelů. Společnost O2 Czech Republic využívá pokročilou technologii a infrastrukturu pro detekci a varování před útoky DDoS, aby její služby zůstaly uživatelům nadále k dispozici.

- Bezpečnostní zásady a postupy: společnost O2 Czech Republic zavedla přísné bezpečnostní zásady a postupy, které slouží jako rámec pro ochranu dat a systémů. Tyto zásady zahrnují pravidla pro přístup k citlivým informacím, zabezpečení hesla, šifrování dat a další bezpečnostní opatření.
- Pravidelné aktualizace a zálohy: společnost O2 Czech Republic pravidelně aktualizuje svůj hardware i software, aby zajistila nejnovější bezpečnostní opravy a ochranu proti známým zranitelným místům. Společnost O2 navíc provádí pravidelné zálohování dat pro minimalizaci rizika ztráty dat v případě havárie nebo útoku.

Společnost O2 Czech Republic se aktivně podílí na spolupráci s bezpečnostními organizacemi a úřady pro sdílení informací o nových hrozbách a spolupracuje s nimi na jejich řešení. To představuje náš příspěvek k celkovému zvyšování digitální bezpečnosti. Společnost O2 Czech Republic vynakládá nemalé úsilí na zajištění bezpečnosti svých zákazníků a pečlivou ochranu jejich osobních údajů. Naše investice do moderních technologií, pravidelné monitorování a školení zaměstnanců prokazují naše odhodlání zajistit bezpečnost a ochranu dat.

Veškeré interní zásady a nařízení (jejichž seznam je shrnutý v závěru této části) jsou pravidelně revidovány a auditovány.

Data

Ochrana dat představuje klíčový prvek při poskytování služeb společnosti O2 Czech Republic. Společnost O2 se zavázala dodržovat soulad se všemi příslušnými právními předpisy, včetně GDPR (Obecného nařízení o ochraně údajů) a ZoEK (Zákona o elektronické komunikaci). Tato kapitola pojednává o typech dat používaných k poskytování služeb a opatřeních přijatých společností O2 Czech Republic pro zajištění důvěrnosti, integrity a dostupnosti dat. Pro naše služby využíváme následující typy dat:

- Obsah komunikace: společnost O2 Czech Republic zajišťuje komunikaci mezi zákazníky a dalšími subjekty. Obsah komunikace je předáván, aniž by k němu měla společnost O2 přístup. To znamená, že veškerá přenášená data jsou chráněna před neoprávněným přístupem.
- Kontaktní údaje zákazníka: společnost O2 Czech Republic ukládá kontaktní údaje zákazníka, jako jsou jméno, adresa, telefonní číslo a e-mail. Tyto informace jsou nezbytné pro komunikaci se zákazníky, stejně jako pro poskytování služeb.
- Smlouvy a komunikace se zákazníky: společnost O2 Czech Republic ukládá veškeré smlouvy a komunikaci se zákazníky, které obsahují klíčové informace ohledně služeb, včetně obecných podmínek. Tyto dokumenty jsou chráněny a ukládány v souladu s příslušnými zákonnými požadavky.

- Data o využití (provozu) pro fakturaci služeb poskytovaných zákazníkům a poskytování odůvodnění pro fakturaci: společnost O2 Czech Republic shromažďuje data nezbytná pro správnou fakturaci služeb zákazníkům a pro poskytnutí jejich odůvodnění. Tato data jsou chráněna a zpracovávána v souladu s interními zásadami a předpisy.
- Další data o provozu pro analýzu chyb a zabezpečení komunikace v sítích: společnost O2 Czech Republic shromažďuje data nezbytná pro správnou fakturaci služeb zákazníkům a pro jejich odůvodnění. Tato data jsou chráněna a zpracovávána pro minimalizaci rizik a zajištění bezpečnosti sítě.
- Data uchovávána zákazníkem v poskytovaných (cloudových) službách: společnost O2 Czech Republic poskytuje cloudové služby, v nichž mohou zákazníci ukládat svá data. Tato data jsou chráněna a zabezpečena proti neoprávněnému přístupu a ztrátě. Vzhledem k tomu, že společnost O2 Czech Republic nemá přístup k obsahu dat, jsou důvěrnost a ochrana soukromí zákazníků zajištěny.

Opatření na ochranu dat a osobních údajů: společnost O2 Czech Republic vypracovala interní zásady a předpisy pro zajištění důvěrnosti, integrity a dostupnosti dat a osobních údajů. Tyto zásady a předpisy jsou v souladu se zákonnými požadavky, jako jsou GDPR a Zákon o elektronické komunikaci, stejně jako s normami, které tvoří integrovaný systém řízení, včetně ISO 27001.
Stanovené zásady a předpisy upravují odpovědnosti, pravomoci a postupy pro oblast ochrany dat a informací, včetně kontroly přístupu k datům, využití přiměřených nástrojů na ochranu dat, jako jsou firewally, systémy na ochranu proti proniknutí (IPS), systémy detekce proniknutí (IDS) a řízení bezpečnosti informací a událostí (SIEM). Tato opatření jsou využívána pro identifikaci a detekci hrozeb a zranitelných míst s cílem zajistit bezpečnost dat a komunikace.
Požadavky ochrany dat a osobních údajů jsou zapracovány také do smluv mezi společností O2 Czech Republic a jejími zákazníky. Smlouvy upravují povinnosti obou stran s ohledem na platnou legislativu.
Společnost O2 Czech Republic nese odpovědnost za ochranu dat zákazníků, včetně osobních údajů, a tuto povinnost bere velmi vážně. Jak bylo uvedeno výše, společnost O2 se snaží neustále vylepšovat své postupy a technologie, aby poskytovala maximální ochranu všech dat, včetně osobních údajů.

FYZICKÉ ZABEZPEČENÍ

Datová centra společnosti O2 jsou navržena pro zajištění maximální bezpečnosti a ochrany soukromí pro zařízení i data zákazníků. Datová centra jsou ve vlastnictví společnosti CETIN a.s., sesterské organizace společnosti O2, která provozuje technologie datových center mimo IT a bezpečnostní služby, včetně kontroly a zabezpečení přístupu. Pro ochranu aktiv společnosti instaluje jednotka bezpečnosti společnosti O2 technické a mechanické nástroje ochrany v souladu s příslušnými předpisy, stanovuje režim opatření pro vytvoření jednotného standardu pro kontrolu přístupu a rozsah zabezpečení zařízení společnosti O2, a provádí veškeré nezbytné pravidelné kontroly.

Kontrola přístupu
Úroveň zabezpečení řízení přístupu se definuje na základě rozdělení datového centra na bezpečnostní zóny. Vstup do datového centra je povolen oprávněnému/registrovanému personálu na základě několikanásobného ověření bezkontaktními kartami a kódem PIN

na čtečkách kontroly přístupu. Vysoce chráněné oblasti DC vyžadují kombinaci výše uvedeného s biometrickým systémem. Každá osoba, která se pohybuje v prostorách DC, musí být viditelně označena. Všichni návštěvníci datových center musí být doprovázeni pracovníkem DC.
Jednotka bezpečnosti společnosti O2 nese odpovědnost za kontrolu dodržování zásad přístupu, stejně jako provádění auditů s cílem ověřit dodržování postupů reakce na incidenty kontroly přístupu do DC personálem DC.

Nepřetržité bezpečnostní monitorování
Okolí, vnitřek, oblasti obsahující podpůrné technologie a technologické místnosti jsou monitorovány bezpečnostními a kamerovými systémy pod dozorem oprávněného bezpečnostního personálu.
Veškeré prvky, funkční i IT, datových center jsou monitorovány personálem střediska monitorování IT.

Protipožární ochrana
Všechny oblasti DC jsou zajištěny prvky s elektrickým protipožárním systémem, technologické místnosti zahrnují laserový systém včasné detekce VESDA a systém automatického stabilního hasicího systému s inertními plyny.

Elektrické napájení a redundance
Elektrické napájení datových center je chráněno jednotkami nepřetržitého napájení (UPS), které zajišťují duální napájení jednotek elektrického napájení zákazníka (PDU).
Všechna datová centra jsou chráněna proti dlouhodobému výpadku elektrického napájení dieselovými generátory, které fungují jako záloha pro systém UPS.
Minimální záloha N+1 zabezpečuje kontinuitu i v případě výpadku některého ze systémů UPS.
Dieselové generátory obsahují palivo na dobu minimálně 24 hodin provozu bez potřeby doplnění. V případě potřeby dodavatel dokáže zajistit dodávku dalšího paliva. Chlazení je zabezpečováno plně nahraditelnými vzduchotechnickými jednotkami.
Všechna naše datová centra jsou vybudována a provozována v souladu s normou TIER III.

OCHRANA KONCOVÝCH BODŮ

Ochrana firemních koncových bodů zahrnuje monitorování a ochranu koncových bodů před kybernetickými hrozbami. Chráněné koncové body zahrnují stolní počítače, notebooky, chytré telefony, tablety a další zařízení. K dispozici jsou různá řešení kybernetické bezpečnosti, které můžete nainstalovat a monitorovat pro ochranu výše uvedených zařízení před kybernetickými hrozbami bez ohledu na to, zda se nacházejí ve firemní síti či nikoliv.

Společnost O2 nainstalovala Zabezpečení koncového bodu (ENS) s použitím proaktivního hlášení hrozeb, které dokáže poskytnout přiměřenou ochranu po celou dobu existence útoku.
Sada zabezpečení koncového bodu zahrnuje zabezpečení koncového bodu a detekci a reakci koncového bodu.

KONTROLA PŘÍSTUPU

Zásady kontroly přístupu

Kontrola přístupu se uplatňuje zejména pro kontrolu přístupu uživatelů k chráněným (klasifikovaným) informacím, zabránění neoprávněnému přístupu, pozměňování, poskytování nebo krádeži informací a médií, to vše jak na fyzické, tak na logické úrovni kontroly přístupu.
Během kontroly přístupu náš kompetentní personál spolupracuje především s jednotkou bezpečnosti, jednotkou ochrany osobních údajů a správci, kteří jsou pověření správou informačních zdrojů.

Přístup k sítím a síťovým službám
Uživatelé mohou využívat přístup k sítím a síťovým službám, k němuž mají výslovné oprávnění.

Správa uživatelů a kontrola přístupu
Fyzické kontroly přístupu se řídí firemní směrnicí o kontrole vstupu. Logická kontrola přístupu uživatelů je v souladu s firemní směrnicí o řízení přístupu a oprávnění a bezpečnostním manuálem pro správce.
Uživatelé jsou povinni postupovat v souladu se schválenými postupy pro přístup. Manažeři smí schválit pouze žádosti nezbytné pro splnění úkolu zaměstnance. Kontrola přístupu pro externí pracovníky se řídí podle kontroly přístupu třetích stran k interním informačním systémům a „rejstříkem externích pracovníků“.
Uživatelé mají zakázáno pokoušet se o ověřování dat nezbytných pro přístup k informačním zdrojům s použitím účtu odlišného od toho, který jim byl přidělen, stejně jako připojovat k síti neschválené prvky IT. Všichni uživatelé jsou povinni hlásit jakékoliv podezřelé chování nebo bezpečnostní incidenty v souladu s definicí směrnice o hlášení bezpečnostních incidentů a událostí.
Jako poskytovatel cloudových služeb nabízí společnost O2 postupy a nástroje pro registraci a zrušení registrace uživatelů cloudových služeb. Společnost O2 navíc zákazníkům nabízí nástroje pro řízení přístupových práv a oprávnění uživatelů.
Jako poskytovatel cloudových služeb nabízí společnost O2 správcům efektivní nástroje pro bezpečné přihlašování pro správu služby, včetně monitorování a konfigurace prvků zabezpečení.

ŘÍZENÍ ZMĚN

Hlavním cílem Řízení změn ICT je zajistit používání standardizovaných metod a postupů pro efektivní a rychlé zpracování všech změn. Je rovněž důležité, aby byly veškeré změny služby a konfigurací zaznamenány do Systému správy konfigurace. Dalším cílem je optimalizovat celková obchodní rizika.

Cílem postupů Řízení změn ICT je reagovat na měnící se obchodní požadavky zákazníků při současné minimalizaci incidentů, selhání a duplikací. Stejně tak důležitá je reakce na měnící se obchodní a IT požadavky, aby byly služby v souladu s aktuálními obchodními potřebami. Navíc je třeba zajistit, aby byly všechny změny zaznamenány, zhodnoceny, povoleny, naplánovány, testovány, zavedeny, zdokumentovány a zkontrolovány kontrolovaným způsobem, a aby byly stanoveny jejich priority.

Postup jako celek je závazný pro všechny zaměstnance společnosti O2 Czech Republic a.s., osoby pracující pro společnost O2 na smluvním základě (mimo FTE, třetí strany), stejně jako pro všechny ostatní strany povinné dodržovat tuto směrnici.

Řízení změn je upraveno v několika řídicích dokumentech nebo jiných definovaných dokumentech.

ZOTAVENÍ PO HAVÁRII

Společnost O2 definuje Systém řízení obchodní kontinuity (Business Continuity Management System, dále jen „BCMS“ a „společnost“), vypracovává základní metodologii a organizační předpoklady pro zvedení systému BCMS. V souvislosti se Zásadami řízení obchodní kontinuity společnosti (Zásady BCMS) a dokumentech o řízení společnosti (Organizační zásady, Bezpečnostní zásady) definuje společnost základní kompetence vedení O2 v oblasti BCMS, stanovuje principy vytváření, strukturu BCMS a definuje veškeré prvky a funkce systému BCM. Systém umožňuje výkonným pracovníkům spoelčnosti O2 a jednotkám pod jejich vedením zaměřit se na plnění úkolů BCMS a povinností vyplývajících z příslušných právních předpisů a smluv. BCMS využívá po zavedení do prostředí společnosti známé doporučené postupy a zkušenosti získané v oblasti BCMS.

Koncepce BCMS společnosti O2 je vícevrstvá z hlediska území a sektoru:

Vrstva 1 – Pro vypořádání se s dopadem interních (i některých externích) nouzových situací na podnikání společnosti, které řeší jednotlivé jednotky v rámci standardního procesu bez potřeby výraznějších změn, je BCMS navržen jako systém pro řízení nouzových situací (provozní nehody, selhání, uzávěrky, nehody, problémy, výpadky služeb, události atd.) bez aktivace firemního krizového týmu. Plánování, vytváření, metody aktivace (činnosti eskalace), činnosti, podpora a vývoj spadají do kompetencí příslušného vedení.

Vrstva 2 – Pro vypořádání se s dopadem externích nouzových situací (krizových situací), stejně jako interních nouzových situací (rozsáhlých nouzových situací) na prostředí společnosti, které překračují rozsah, kapacity a kompetence jednotlivých firemních jednotek a vyžadují uplatnění nestandardních (upravených) procesů a forem řízení, je BCMS navržen jako systém krizového řízení s aktivací krizového týmu společnosti. Plánování, vytváření, způsob aktivace a vývoj BCMS patří mezi povinnosti jednotky CNOC, zatímco jeho aktivace spadá do kompetencí konkrétního vedoucího krizového týmu. O přechodu ze systému ad-hoc řešení nouzových situací konkrétní jednotkou na systém krizového řízení (na regionální nebo národní úrovni) obvykle rozhoduje vedoucí krizového týmu ve spolupráci s vedením jednotek v závislosti na posouzení a vývoji specifické nouzové situace.

Procesy a postupy (BCP, DRP) pro řešení nouzových situací jsou pravidelně revidovány, testovány a dle potřeby aktualizovány. Veškerá cvičení a testy jsou zaznamenávány do systému Ramses.

BCP/DRP definuje několik dokumentů a zásad v rámci společnosti.

ŘÍZENÍ ZRANITELNÝCH MÍST

V oblasti řízení zranitelných míst společnost zavedla zásady, postupy, pravomoci a odpovědnosti pro efektivní řízení zranitelných míst informačních systémů a technologií

pro minimalizaci rizika bezpečnostních incidentů, potenciálních ztrát a omezení obchodních rizik.

Účinný program řízení zranitelných míst zahrnuje:
Odpovědnost za neustálou údržbu informačního systému.
Průběžné monitorování stavu aktualizací a implementace oprav informačního systému.
Soulad s doporučeními dodavatelů softwaru.
Průběžné a ad-hoc protiopatření pro minimalizaci bezpečnostních rizik a incidentů.

Cílem řízení zranitelných míst je zajistit soulad s doporučeními výrobce a jednotkou Bezpečnosti při současném včasném odstranění všech zranitelných míst.

Vzhledem k tomu, že jednotlivá zranitelná místa se liší v tom, do jaké míry jsou kritická, odpovědná osoba (správce) musí posoudit, která softwarová oprava se má uplatnit, aby se minimalizoval dopad na podnikání, a musí vyhradit dostatek času na testování a implementaci v souladu s procesem řízení změn.

Správcové jsou odpovědní také za zajištění všech softwarových oprav z renomovaných a důvěryhodných podpůrných kanálů, jako jsou samotní dodavatelé nebo nezávislí dodavatelé. Jednotlivé softwarové opravy je třeba stáhnout a aplikovat na licencovaný software a v případech, kdy existuje smlouva o podpoře.

V případě, že objektivní důvody brání výše uvedené činnosti, odpovědná osoba (správce) musí uplatnit výjimku ze zásad v souladu s platnou směrnicí o Řízení bezpečnostních výjimek.

V případech, kdy existuje zdroj typu open source bez důvěryhodného podpůrného kanálu, musí odpovědná osoba situaci vyřešit uplatněním výše uvedené výjimky.

III. Příloha B
Popis hlavních servisních závazků a systémových požadavků servisní organizace společnosti O2 Czech Republic

PŘÍLOHA B

POPIS HLAVNÍCH ZÁVAZKŮ A SYSTÉMOVÝCH POŽADAVKŮ SERVISNÍ ORGANIZACE SPOLEČNOSTI O2 CZECH REPUBLIC

Servisní závazky

Závazky představují prohlášení učiněné vedením vůči zákazníkům ohledně výkonu systému společnosti O2 CZ. Závazky vůči zákazníkům jsou komunikovány prostřednictvím Smluv o úrovni služeb a/nebo Smluv o zpracování dat. Smlouvy o zpracování dat definují povinnosti v oblasti bezpečnosti a ochrany soukromí, které musí zpracovatelé údajů dodržet pro splnění povinností organizace ve vztahu ke zpracování a zabezpečení dat zákazníka.

Systémové požadavky

Systémové požadavky jsou stanoveny v zásadách a postupech společnosti, které jsou k dispozici všem zaměstnancům.

Společnost O2 CZ přijímá servisní závazky vůči svým zákazníkům a vytvořila systémové požadavky jako součást své služby O2 ITS. Některé z těchto závazků jsou klíčové pro poskytování služby a souvisí s příslušnými kritérii služby důvěry. Společnost O2 CZ nese odpovědnost za dodržování svých servisních závazků a systémových požadavků a za vypracování návrhu, zavedení a provoz účinných kontrol v rámci systému pro poskytnutí rozumné jistoty, že servisní závazky a systémové požadavky společnosti O2 budou dodržovány.

Na společnost O2 CZ se vztahují příslušné předpisy, stejně jako národní právní předpisy a nařízení ohledně ochrany soukromí v právních řádech zemí, kde společnost O2 CZ působí.

Závazky v oblasti zabezpečení, dostupnosti, důvěrnosti, ochrany soukromí a integrity zpracování vůči zákazníkům jsou zdokumentovány a komunikovány prostřednictvím Smluv o úrovni služeb (Service Level Agreement, SLA) a dalších smluv se zákazníky, stejně jako formou popisu nabídky služeb, který je umístěný na webových stránkách společnosti O2 CZ. Závazky v oblasti zabezpečení, dostupnosti, důvěrnosti, ochrany soukromí a integrity zpracování jsou standardizovány a zahrnuty například v následujících dokumentech:

- Principy zabezpečení a důvěrnosti související se základním návrhem systému společnosti O2 CZ jsou navrženy tak, aby vhodným způsobem omezovaly neoprávněný interní i externí přístup k datům a aby byla data jednoho zákazníka řádně oddělena od ostatních zákazníků.

- Principy zabezpečení a důvěrnosti související se základním návrhem systému společnosti O2 CZ jsou navrženy tak, aby chránily data jak v limitech prostředí, kde se obsah zákazníka ukládá, tak mimo něj, aby byly splněny servisní závazky.

- Principy dostupnosti související se základním návrhem systému společnosti O2 CZ jsou navrženy tak, aby replikovaly kritické systémové komponenty napříč několika oblastmi dostupnosti a aby byly uchovávány a monitorovány autoritativní zálohy pro zajištění úspěšné replikace pro splnění servisních závazků.

- Principy ochrany soukromí související se základním návrhem systému společnosti O2 CZ jsou navrženy tak, aby chránily bezpečnost a důvěrnost obsahu zákazníků společnosti O2 CZ, aby byly splněny servisní závazky.

- Principy integrity zpracování související se základním návrhem systému společnosti O2 CZ jsou navrženy tak, aby chránily bezpečnost a důvěrnost dat zákazníků společnosti O2 CZ během přenosu, aby byly splněny servisní závazky.

Společnost O2 Czech Republic stanovila provozní požadavky, které podporují dosažení závazků v oblasti zabezpečení, dostupnosti, důvěrnosti, ochrany soukromí a integrity zpracování, dodržení příslušných právních předpisů a nařízení a dalších systémových požadavků. Tyto požadavky jsou komunikovány v zásadách a postupech společnosti O2 CZ, dokumentaci návrhu systému a smlouvách se zákazníky. Zásady zabezpečení informací definují celoorganizační přístup k ochraně systémů a dat. Patří sem zásady související se způsobem navržení systému a jeho vývojem, s provozem systému, řízením interních obchodních systémů a sítí a postupy náboru a školení zaměstnanců. Kromě těchto zásad byly zdokumentovány standardní provozní postupy pro provádění specifických manuálních a automatických procesů nezbytných pro provoz a vývoj různých služeb a nabídek společnosti O2 CZ. Servisní závazky a systémové požadavky společnosti O2 CZ byly dosaženy na základě příslušných kritérií služeb důvěry pro zabezpečení, dostupnost a důvěrnost, ochranu soukromí a integritu zpracování.

DOSTUPNOST

Existuje zdokumentovaný postup řízení kapacit. Plány kapacit jsou vypracovávány s varováními a akčními limity stanovenými pro monitorované zdroje (výpočetní výkon, úložiště, paměť). K měření skutečného využití a kapacity se používají vhodné monitorovací nástroje. Aktuální využití zdrojů a předpověď poptávky po kapacitě jsou pravidelně hlášeny vedení.
Součástí seznamu hrozeb v rámci procesu hodnocení rizik jsou i ekologické hrozby. Posuzovány jsou externí ekologické hrozby a datová centra jsou umístěna mimo oblasti záplav a zemětřesení.
Společnost CETIN jako dodavatel nese odpovědnost za implementaci a provoz ekologických ochranných prvků. Jsou zavedena opatření na detekci, jako jsou požární a kouřové detektory, detektory kvality vzduchu a detektory úniku kapalin. Monitorování prostředí a provozu a varování jsou součástí všech kontrolních systémů DC s nepřetržitou přítomností personálu na místě. Pro obě datová centra existují vypracované plány údržby a testování.
Datová centra jsou navržena a provozována v souladu s požadavky TIER III.
Procesy zálohování dat jsou zavedeny v souladu se specifikacemi jednotlivých služeb zahrnutých do této zprávy (zálohy konfigurace, replikace na úrovni úložiště, synchronní replikace dat atd.).
Společnost O2 zavedla systém řízení obchodní kontinuity v souladu s normou ISO 22301 vztahující se na obě datová centra. Pro služby zahrnuté do této zprávy byly vypracovány plány obchodní kontinuity s postupy zotavení po havárii. BCP/DRP zahrnují požadavky na testování (rozsah, frekvenci).

DŮVĚRNOST

Společnost O2 stanovuje zásady a principy ochrany informací, včetně pravomocí a odpovědností za identifikaci, klasifikaci, zpracování a ochranu důvěrných informací.
Navíc byl zaveden jednotný systém pro řízení dokumentace, včetně zásad pro archivování a skartování, a to v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě.
Zásady ochrany klasifikovaných informací v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, jsou upraveny v samostatném vnitřním předpisu.

Jsou zavedeny postupy pro likvidaci informací v závislosti na úrovni kvalifikace a médiu, tj. pro tištěné dokumenty, elektronické soubory na různých médiích.

INTEGRITA ZPRACOVÁNÍ

Vzhledem k tomu, že cloudové služby společnosti O2 jsou primárně navrženy jako infrastrukturní služba, společnost O2 nezpracovává data patřící zákazníkům. Služby zabezpečení společnosti O2 jsou především analytické, monitorovací a vykazovací. V těchto případech se sjednává smlouva obsahující vymezení, která data je zákazník povinen poskytnout a pro jaké účely zpracování. Smlouva rovněž stanoví formát vstupních a výstupních dat (včetně vykazování), metodu přenosu dat, zásady ochrany a skladování dat. Kontrola integrity zpracování zahrnuje rovněž provozní a bezpečnostní monitorování služeb.

OCHRANA SOUKROMÍ

Vzhledem k tomu, že cloudové služby společnosti O2 jsou primárně navrženy jako infrastrukturní služba, společnost O2 nezpracovává data patřící zákazníkům. Služby zabezpečení spolehnouti O2 jsou především analytické, monitorovací a vykazovací.
Pokud zákazníci společnost O2 informují, že rozsah cloudových služeb společnosti O2 zahrnuje rovněž zpracování osobních údajů, budou do všeobecných podmínek zaraženy také ustanovení upravující vztah mezi správcem a zpracovatelem osobních údajů v souladu s GDPR.
Společnost O2 nastavila procesy pro zajištění souladu s veškerými zákonnými požadavky ohledně ochrany osobních údajů a jiných dat. Vnitřní předpisy stanovují zásady pro ochranu osobních údajů (GDPR), ochranu údajů o identifikaci, provozu a umístění a důvěrnost komunikace (viz Zákon o elektronické komunikaci), stejně jako ochranu obchodních tajemství.
Každá smlouva, resp. všeobecné podmínky zahrnují ustanovení o ochraně osobních údajů. Navíc jsou zákazníci o ochraně osobních údajů informováni také na webových stránkách společnosti O2 (https://www.o2.cz/soukromi). Webové stránky společnosti O2 informují o tom, jak společnost O2 využívá soubory cookie a zpracovává osobní údaje zákazníků v postavení správce údajů (Zásady zpracování osobních údajů) i zpracovatele údajů (Seznam zpracovatelů osobních údajů). Zahrnují rovněž informace o zpracování stížností, včetně kontaktních údajů na úředníka pro ochranu údajů a informacích o právech zákazníka eskalovat stížnost k úřadu pro ochranu osobních údajů.