DESCRIPTION
of the
GBS Cloud Services

Business User, hereinafter referred to as **"Customer"** and/or **"User";**

and

„GBS Europa GmbH", with registered office and registered address in: An der Zur Giesserei 19-27B, 76227 Karlsruhe, Germany, hereinafter referred to as **"Provider"** and/or **"GBS"**.

1 PREAMBLE:

GBS provides a Security Cloud Service ("**Service**"). The customer receives a central service with different components based on the selected subscription, which integrates with the customer's Office 365 / Exchange Online environment.

This service description contains detailed information on the various functions available to the customer in relation to e-mail security, depending on the subscription chosen by the customer.

The following technical requirements apply to the use of the services on the part of the customer:

- Use of Exchange Online or O365;
- Internet access; and
- an up-to-date Internet browser.

GBS provides the customer with a detailed overview of the technical requirements on the Internet. The provision and transmission of the technical requirements is not the subject of this service description.

2 Specifications

2.1 Malware protection for email

This service provides advanced malware detection and protection mechanisms that allow the customer to apply their own security policies and preferences to email traffic while having complete visibility and control.

GBS's malware protection for email is a combination of proprietary detection mechanisms and integration with leading third-party anti-malware engines. The customer can choose from a list of anti-malware engines, e.g. McAfee, Avira, Sophos and Kaspersky. Based on the customer's choice, one or a combination of several of the above will be used as part of the solution.

Suspicious emails can either be flagged, blocked, or quarantined for further review and processing.

Der Service erkennt und analysiert auch die wahre Dateierweiterung, erkennt das Dateiformat und bietet die Möglichkeit bestimmte Dateiformate zu blockieren.

2.2 SPAM protection for e-mail

The service offers enhanced anti-SPAM protection that combines GBS's own content recognition engine with the industry-leading SPAM rating mechanisms of Sophos or Kaspersky, depending on the customer's choice, to achieve maximum protection, visibility, and flexibility.

The content recognition engine analyzes both the body and content of the attachments and attempts to identify suspicious text and meanings, while third-party engines are mainly used for RBL checks and reputation validation.

There are numerous actions that can be performed. They depend on the provider's policies, so the customer has control over the behavior of the systems at all times. The default settings are: mark as spam, block, quarantine, etc., but it is also possible to configure much more complicated workflows and processes.

3 Message encryption for e-mail

This service allows the customer to encrypt e-mail communication at the message level. It creates a PDF file that contains the email body and the embedded attachments, and then protects the PDF file with a password. The flexible configuration settings allow the provider to apply different policies and give the user the appropriate flexibility. The password can be preset, assigned dynamically or requested by the recipient.

This feature can be applied in conjunction with content recognition based on confidentiality, keywords, etc.

This service provides a unique user experience because neither the sender nor the recipient has to leave their email environment to use it. By default, the passkey/password exchange for decryption is communicated directly between the two users either by email or by other means. Users can even set static passwords – e.g. John sets one password <password> for communicating with Jean and another for communicating with Reymond.

It can also be used for internal communications when sensitive data is transmitted.

3.1 Server-to-server encryption for email

This service sets up server-to-server encryption using the industry-standard PGP or S/MIME protocols. This ensures that both email servers always exchange encrypted communication.

This service is extremely useful for encrypting sensitive data with known third parties, e.g. with an external legal advisory firm or an external financial advisory firm. In this way, it is ensured that the data flow between the two companies is always encrypted.

NOTE: Using S/MIME also requires that there is a certificate manager that is another service described below.

3.2 Key/Certificate Management for Email

This service allows organizations to centrally manage all certificates/keys that are used. This applies when using the S/MIME encryption mechanism.

3.3 E-mail Data Loss Prevention

This service works in conjunction with the GBS content recognition engine and allows the customer to apply data policies to email flow, enforce the 4-eyes principle, and detect anomalies in email flow. The service can detect either the content or behavior, as well as trigger a workflow that requires approval for communication.

If sensitive data is detected, the system can trigger a workflow for the 4-eyes principle and suspend the delivery of the e-mail until it is released. The system also notifies the approver that approval is pending.

If a user starts generating suspicious email activity, e.g. sending emails to external parties at non-standard times, sending a large number of small emails outside the

company, etc., the system would detect this and trigger an alarm about suspicious behavior that can protect against stolen credentials or a malicious insider.

3.4 Attachment conversion for email

This service allows the customer to detect files with active content and convert them to files with no active content instead of blocking them while the original file remains in quarantine if needed. This allows the customer to protect their email communications from attachments with active content if they come from trusted and whitelisted domains.

3.5 Signature management for e-mails

With signature management, individualized signatures can be created and attached to e-mails as a disclaimer (so-called trailer) based on rules.

E-mails addressed to external recipients can be provided with greetings, company information, disclaimers, waivers, legal notices, etc. and, if necessary, with images, logos, vCards or other trailer file attachments.

Due to the flexibility of the service, individual trailers for departments, groups, Internet domains or individuals can be attached to any place in the e-mail and limited in time. Uncomplicated configuration and central administration (also via departments such as .B marketing) enable optimal use and support a uniform appearance of your company to the outside world.

3.6 Out-of-office management for emails

This service enables central absence management that can be used to redirect, forward or generate automated responses. This is possible both for one-off absences (e.g. for the period of vacation, illness or a business trip) and for periodic absences on certain days of the week (e.g. for part-time employees). A retroactive forwarding can also be realized, e.g. in the event that an employee has forgotten to set up a forwarding before the start of the holiday. With appropriate configuration, out-of-office notifications can also be automatically sent to the sender and/or delegate.

The service thus ensures that no important e-mails remain unprocessed and/or unanswered in the event of (planned or unforeseen) absence.

This is particularly important when it comes to time-critical information, invoices, or requests for quotations, for example.

GBS offers the following service within the technical and operational possibilities.

3.7 Protect against threats to SharePoint Online

This service provides advanced malware detection and protection mechanisms that help the customer ensure that no malicious files are stored on SharePoint Online.

The service is a combination of proprietary detection mechanisms and integration with leading third-party anti-malware engines. The customer can choose from a list of anti-malware engines, e.g. McAfee, Avira, Sophos and Kaspersky. Based on the customer's choice, one or a combination of several of the above will be used as part of the solution.

Suspicious files are identified both during upload/saving and based on a predefined audit plan and quarantined for further review and processing.

3.8 Protection against threats for MS Teams

This service provides advanced malware detection and protection mechanisms that ensure that no malicious files are stored on MS Teams in the "Files" section.

The service is a combination of proprietary detection mechanisms and integration with leading third-party anti-malware engines. The customer can choose from a list of anti-malware engines, e.g. McAfee, Avira, Sophos and Kaspersky. Based on the customer's choice, one or a combination of several of the above will be used as part of the solution.

Suspicious files are identified both during upload/saving and based on a predefined audit plan and quarantined for further review and processing.

4 Services from GBS

4.1 Components of the Cloud Security Service

The service consists of various components. Among the most important are:

a) Core System

The central component, which provides all the services described, is installed and set up in an environment based on Microsoft Azure with an architecture that provides high availability of services and the necessary performance.

Some of the additional features not listed in Article 1 "Statement of Work":

- Connect to the customer's Azure Active Directory;
- Connect to the customer's Exchange Online/Office 365;
- Auditing and logging;
- Connecting to Third-Party Technologies.

b) WebClient

The WebClient gives the customer access to his data, configuration settings, statistical information and auditing information. The WebClient also offers users various options, depending on the assigned roles and rights.

Key features include:

- Configuration of signatures;
- Preview signatures;
- Central absence management;
- roles and rights;
- Password Manager.

c) Console

Some of the advanced configurations must be performed through the MMC console.

For more information, see the iQ.Suite product documentation.

4.2 Customer-specific services

Der Kunde kann mit GBS kundenspezifische Leistungen vereinbaren, wie z. B. individuelle Systemanpassungen, Beratung zur Nutzung auf Basis von Best Practices, Design und Erstellung von Signaturen oder einen Proof of Concept. Der genaue Leistungsumfang wird in einem separaten Dokument festgehalten.

4.3 Access

The Account Holder's access to the management and use of GBS's services is via the Internet. Any access requires that the account holder authenticates himself with an access code consisting of an e-mail address and a password. These are awarded by the customer.

Further additional details on secure initial authentication will be communicated to the customer on information pages on the Internet. The administrator can set up users to use the modules.

5 Support and fault acceptance

a) General SLA information can be found on the Internet under https://www.gbs.com

b) Online Documentation

Provision of online support in the form of FAQs;

Tips, instructions, etc. in German and English.

c) Fault acceptance and hotline support

The acceptance of fault reports is available 24/7 as an online service desk. Under the service number, GBS also answers product-related and general questions about the operation of GBS products.

Product-related and general questions will only be answered on weekdays (Monday to Friday) from 8:00 a.m. to 8:00 p.m. CET.

The customer support referred to in point (b) shall be available only to the Administrator or his deputy; the remaining users are not entitled to support.

All information about these support services, including service hours and contact details, can be found on the Internet at https://www.gbs.com.

6 Operation of server and system components

All server and system components required for the operation of the solutions are operated in a technically and organizationally secure, powerful computer network that is protected against attacks and unauthorized access from the Internet.

The solution is multi-client capable. The environment and operation take place within the European Union and thus in compliance with the European data protection directives. Depending on the choice and configuration of the services by the customer, some data may be processed outside the European Union.

Further information can be found in our DPA and in the respective special conditions for the data processing of the sub-processors. The computer network is connected to the Internet via the Internet backbone at the latest transmission speed.

The services for the operation of the data center are available with an average availability of 99.9% on an annual average.

The following features apply to operation and system management:

- Operating time 24/7;
- Automatic detection of errors within the computer network.

7 Operational Deployment

The access data for the activation of the service will be sent to the customer or the administrator named by the customer by e-mail when GBS first provides the service.

8 Compatibility with older hardware and operating software

GBS continuously updates the software to adapt it to new or updated versions of the operating systems.

Older device and operating system versions are supported for as long as possible. However, for technical reasons, it is not possible to ensure that they run on all available hardware types, nor can outdated operating system versions be supported indefinitely. GBS reserves the right to discontinue support for outdated operating system versions with advance notice or to discontinue support for certain platforms altogether.

9 Term and Termination

The solution will be made available to the customer with a minimum term of 12 (twelve) months. The notice period is 30 (thirty) calendar days to the end of the term. If the service is not terminated in due time, it will be extended by 12 (twelve) months in each case.

The Customer may test the Solution free of charge 30 (thirty) calendar days in advance. The trial period automatically ends 30 (thirty) calendar days after activation without a contract being concluded.