Sicherheitsdokument

Sage HR Bewerbermanagement Smart (Karriereportal)

Stand: 4.12.2023

Sage

Inhaltsverzeichnis

1 Inhalt

Dieses Dokument beschreibt die Sicherungsmaßnahmen, welche für das Sage HR Bewerbermanagement Smart (Karriereportal) verwendet werden. Es wird in die verschiedenen Teilbereiche unterschieden, aus welchen heraus der Zugriff auf die Daten erfolgt.

2 Technische Rahmenbedingungen

2.1 Sicherheit und Verschlüsselung

Jeder Kunde/Mandant wird auf eigenen, ausschließlich für ihn bereitgestellten Containern, betrieben. Um die Sicherheit weiter zu erhöhen, werden die notwendigen Dienste zum Betrieb des Bewerbermanagement Smart auf mehrere Container verteilt. So wird z.B. die Datenbank in einem eigenen Container betrieben. Außerdem wird jeder Mandant in einem separaten Netzwerk betrieben, das für andere Mandanten unzugänglich ist.

Alle Zugriffe auf das Bewerbermanagement Smart erfolgen mittels TLS Verschlüsselung.

Die Benutzerzugriffe zur Verwaltung der Lösung werden zusätzlich zum Benutzernamen und Passwortkombination über eine 2-Faktor Authentisierungslösung abgesichert.

Weiterhin werden die Benutzerzugangsdaten nur auf der 2-Faktor Authentisierungslösung gespeichert und verwaltet. Dadurch ist sichergestellt, dass aus dem Bewerbermanagement Smart keine Zugangsdaten entwendet, werden können.

Die Kommunikation zwischen dem Bewerbermanagement Smart Server und der 2-Faktor Lösung ist ebenfalls verschlüsselt. Damit wird verhindert, dass Angreifer kritische Daten abfangen oder ggf. verändern können.

<u>Die Einstellungen/Konfigurationsoptionen des Bewerbermanagement Smart Servers sind doppelt abgesichert:</u>

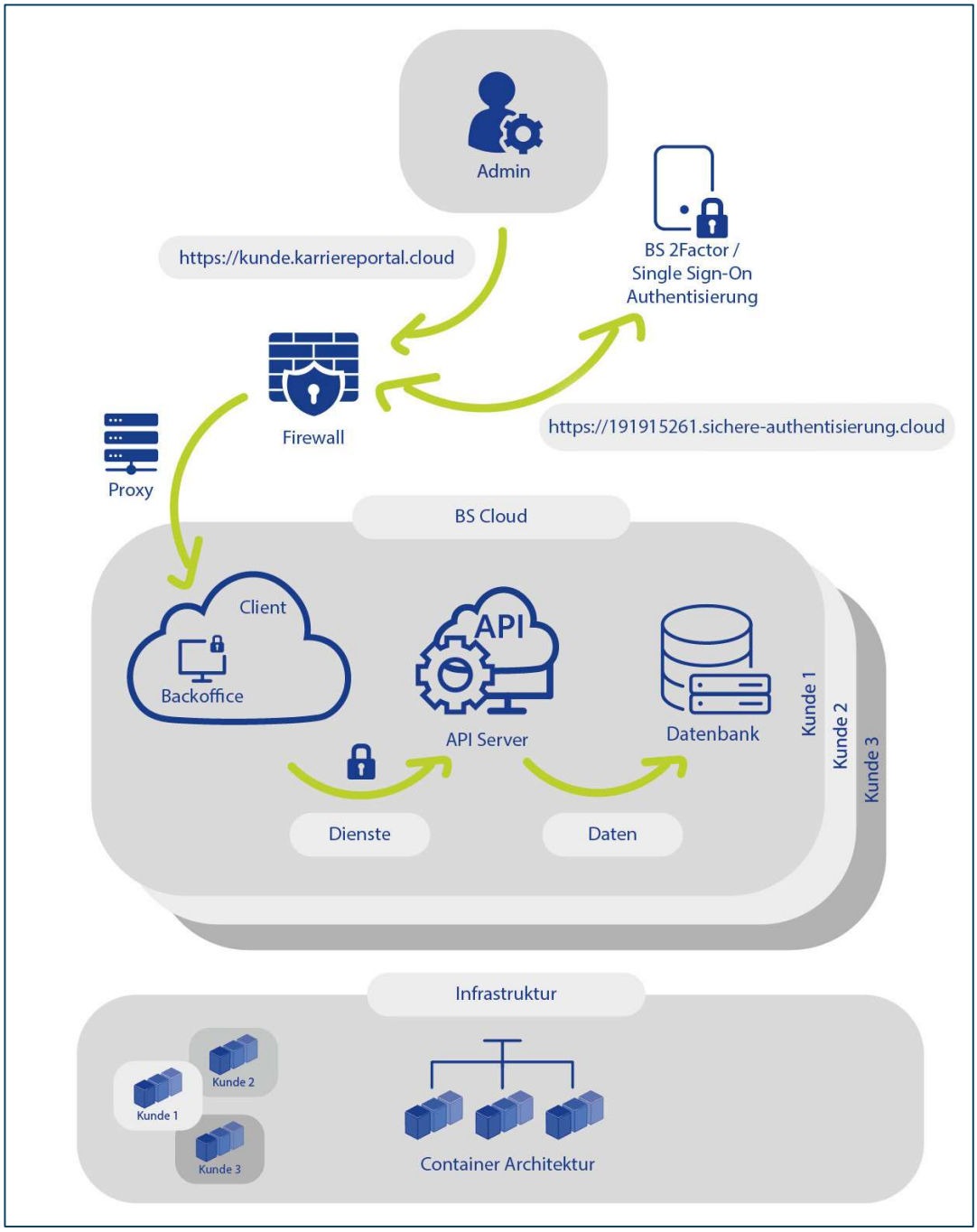
1. Einstellungen, die für den Administrator vorgesehen sind, werden bei normalen Benutzern nicht angezeigt.
2. Die Einstellungen des API Services können nur vom Administrator geöffnet werden.

<u>Der API Server wird zusätzlich durch eine Trennung der Funktionen weiter abgesichert:</u>

1. Funktion: Anonyme Benutzer können nur auf frei zugängliche Informationen zugreifen wie z. B. die FAQs. Nur ein anonymer Benutzer ist berechtigt Bewerbungen anzulegen.
2. Funktion: Nur Administratoren können Stammdaten ändern.
3. Funktion: Nur berechtigte Benutzer können auf die Daten für die Synchronisation mit der HR Suite zugreifen.

2.2 Ablauf und Absicherung der Administratoranmeldung

Der Administrator meldet sich sicher (TLS verschlüsselt) am Bewerbermanagement Smart an. Um die Sicherheit zusätzlich zu erhöhen, erfolgt die Authentisierung über eine 2-Faktor Lösung. Diese 2-Faktor Authentisierung identifiziert und autorisiert den Benutzer zum Zugriff und stattet den Admin-Benutzer mit den notwendigen administrativen Berechtigungen aus.



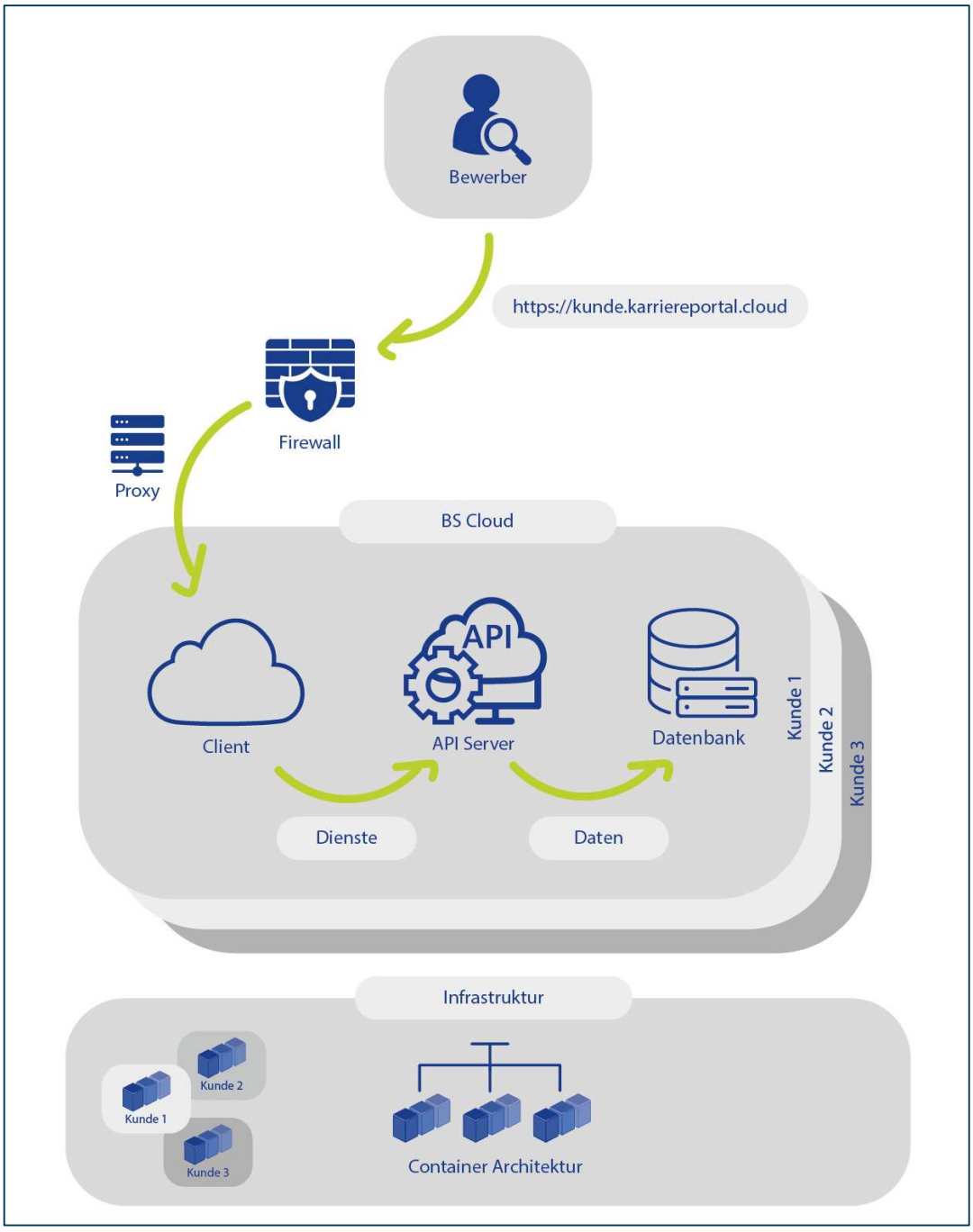
2.3 Nutzung des Produkts aus Sicht des Bewerbers

Der Bewerber öffnet die Internetseite des Bewerbermanagement Smart ebenfalls über eine TLS verschlüsselte Verbindung.

Da es sich um einen anonymen Benutzer handelt, muss dieser sich nicht authentisieren.

In diesem Fall greift der Bewerber auf die 1. Funktion des API-Bereichs für anonyme Benutzer zu. Dieser öffentlich sichtbare Bereich stellt nur lesende Informationen bereit, welche vom Bewerber nicht geändert werden können z. B. die FAQs, die Unternehmensbeschreibung, das Stellenprofil etc.

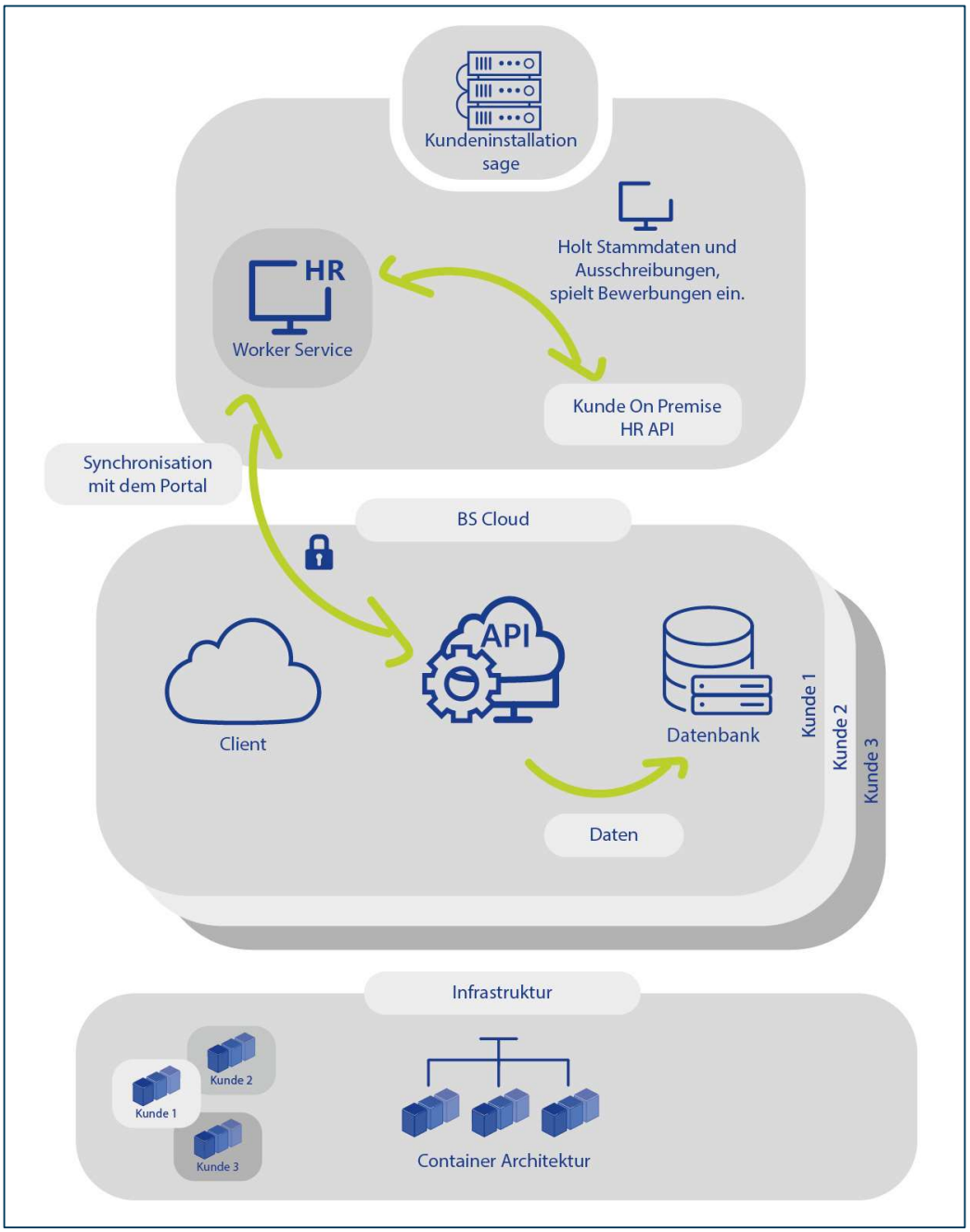
In diesem Bereich kann der anonyme Benutzer seine Bewerbung erstellen.



2.4 Ablauf der Datenübertragung von und zur HR Suite

Ausschließlich die HR Suite des Kunden initiiert die Übertragungen vom und zum Bewerbermanagement Smart. Es erfolgt keinerlei Zugriff bzw. Steuerung der HR Suite durch das Bewerbermanagement Smart. So werden z. B. die Bewerbungen immer von der eigenen HR Suite abgeholt (heruntergeladen) und z. B. die offenen Stellen und Daten der eigenen HR Suite dem Bewerbermanagement Smart zur Verfügung gestellt (hochgeladen).

Alle Verbindungen hierzu sind ebenfalls TLS verschlüsselt. Um diese Verbindung einzurichten, wird dem Administrator ein verschlüsseltes Passwort generiert, welches innerhalb der HR Suite konfiguriert wird. Das Passwort befindet sich innerhalb der HR Suite immer in verschlüsselter Form und kann nur durch den HR Dienst zur Übermittlung der Daten entschlüsselt werden. Insofern ein neues Passwort generiert wird, verliert das bisherige automatisch seine Gültigkeit.



3 Systemanforderungen

1. Internetverbindung / Internetzugriff mit freigeschaltetem Port 443
2. Firewall, die auf *.karriereportal.cloud Get/Put/Post/Delete zulässt
3. aktueller Internet Browser:

Edge	Firefox	Chrome	Safari (macOS)	Safari (iOS)	IE
>= 91	**>= 78**	**>= 90**	**>= 14**	**>= 12.5**	**11 (partial support)**

4 Datenvorhaltung im Rechenzentrum

4.1 Allgemeines

Die Infrastruktur wird in Rechenzentren betrieben, welche sich ausschließlich in Deutschland befinden. Diese genügen hohen Anforderungen an Sicherheit und Verfügbarkeit. Die genutzte Hardwareinfrastruktur befindet sich im Eigentum eines deutschen Betreibers um Zugriffe von unsicheren Drittländern, z. B. durch den Cloud Act, zu unterbinden. Die folgende Beschreibung stellt die vereinbarten Qualitätsmerkmale des Rechenzentrums dar.

4.2 Zutrittskontrolle und Alarmsystem

Das Rechenzentrum verfügt über einen Zutrittsschutz und Zutritte werden protokolliert. Der Zutritt zum Rechenzentrum ist nur über die Authentifizierung mit zwei unabhängigen Merkmalen möglich. Das Rechenzentrum verfügt über eine Einbruchmeldeanlage mit Alarmierung einer 24x7 erreichbaren Sicherheitszentrale, in der Verfahren für den Alarmierungsfall definiert sind.

4.3 WAN-Anbindung

Die Kommunikationseinrichtungen des Rechenzentrums werden über die USV Anlage notgespeist. Die Anbindung an öffentliche Netze ist redundant ausgelegt.

4.4 Stromversorgung

An das öffentliche Stromnetz ist das Rechenzentrum zur Erhöhung der Ausfallsicherheit über zwei Hauseinführungen angeschlossen. USV und Dieselgeneratoren sind vorhanden. Die Anlagen zur Sicherung der Energieversorgung werden je nach technischer Anforderung regelmäßig getestet. Wartungen der Stromversorgung finden geplant und regelmäßig statt.

4.5 Klimatisierung & Brandmeldeanlage

Das Klimatisierungssystem ist redundant ausgelegt. Die Anlagen zur Klimatisierung werden regelmäßig je nach technischer Anforderung getestet. Wartungen der Klimatechnik finden geplant und regelmäßig statt.

Eine Brandmeldeanlage mit Sensoren zur Brandfrühesterkennung ist installiert. Die Alarmierung erfolgt an eine 24x7 erreichbare Sicherheitszentrale, in der Verfahren für den Alarmierungsfall definiert sind. Wartungen der Brandschutztechnik finden geplant und regelmäßig statt.

4.6 System-Monitoring

Im Rahmen der Servicebereitstellung werden verschiedene Monitoring Werkzeuge eingesetzt. Alle überwachten Systemparameter werden in einem zentralen Monitoring System gesammelt und führen dort zu einer kontinuierlichen Statusüberwachung.

4.7 Zertifizierung

Der hohe Qualitätsstandard der genutzten Colocationplätze im Rechenzentrum wird durch Zertifizierungen nach ISO9001, ISO27001 und DIN EN 50600 unterstrichen.

4.8 Backup

Die Kundenserver werden täglich gesichert und haben eine Vorhaltezeit von 7 Kalendertagen zur kostenfreien Wiederherstellung der Kundendaten bei durch den Betreiber verschuldeten Datenverlust.

4.9 Passwortregeln für die Benutzeraccounts

Um die Sicherheit zu gewährleisten, wurden sichere Passwortrichtlinien eingerichtet. Von dieser Regel sind keine Ausnahmen möglich.

4.10 Betriebszeit des bereitgestellten SaaS Services

Die Betriebszeit des Rechenzentrums beträgt 24x7 an 365 Tagen im Jahr.

Die Zeiten außerhalb Mo. - Sa. 07:30 - 18:30 Uhr gelten als mögliches Wartungsfenster, welche ohne weitere Ankündigung für eine Wartung genutzt werden können.

5 Penetrationstest

5.1 Sage Standards

Bei der Anbindung von ISV / HR Rockstar-Lösungen werden Security Maßnahmen, wie beispielsweise die des Secure Software Development Lifecycle (S-SDLC), eingesetzt. Dazu gehört auch die Durchführung von Penetration Tests.

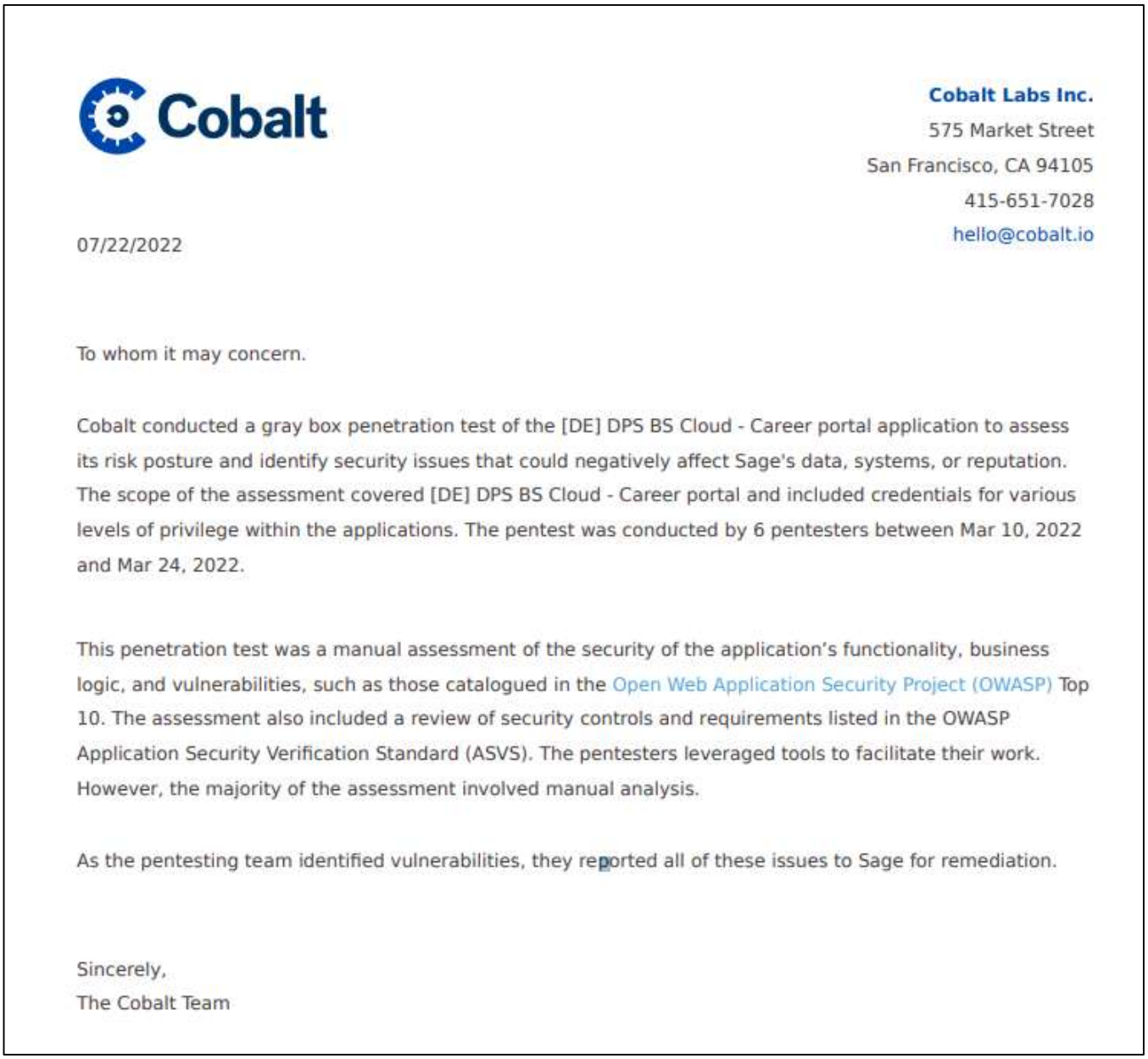
Hier finden Sie weitere Informationen auf unserer globalen Webseite:

https://www.sage.com/en-gb/trust-security/

https://www.sage.com/en-gb/trust-security/security/technical/software-development/

5.2 Bestätigung erfolgreich bestandene Prüfung

Die Firma Cobalt hat im März 2022 einen Penetrationstest für das Bewerbermanagement Smart durchgeführt. Die Prüfung hat die DPS BS Cloud erfolgreich bestanden.



Cobalt

Cobalt Labs Inc.
575 Market Street
San Francisco, CA 94105
415-651-7028
hello@cobalt.io

07/22/2022

To whom it may concern.

Cobalt conducted a gray box penetration test of the [DE] DPS BS Cloud - Career portal application to assess its risk posture and identify security issues that could negatively affect Sage's data, systems, or reputation. The scope of the assessment covered [DE] DPS BS Cloud - Career portal and included credentials for various levels of privilege within the applications. The pentest was conducted by 6 pentesters between Mar 10, 2022 and Mar 24, 2022.

This penetration test was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those catalogued in the Open Web Application Security Project (OWASP) Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

As the pentesting team identified vulnerabilities, they reported all of these issues to Sage for remediation.

Sincerely,
The Cobalt Team

Sage bzw. DPS BS führt jährliche Audits und Security-Tests für dieses Cloudprodukt durch.

Sage GmbH
Franklinstraße 61 – 63
60486 Frankfurt am Main

+49 69 50007-0
info@sage.de

www.sage.com