






SICHERHEITSKONZEPT BKMS® SYSTEM

Die Business Keeper AG (BKAG) stellt Systeme zur Erfassung anonymer Hinweise von Hinweisgebern sowie zu deren Bearbeitung durch den Kunden zur Verfügung. Das patentierte und zertifizierte Business Keeper Monitoring System (BKMS® System) ist ein Verfahren zur nachhaltigen Prävention und Bekämpfung von Verstößen gegen gesetzliche, ethische und unternehmensinterne Normen. Hinweise zu verschiedensten Schwerpunkten können aufgenommen werden.

Das BKMS® System wird als anonyme Kommunikationsplattform auf der einen Seite von Hinweisgebern (Mitarbeiter in Unternehmen und Verwaltungen oder Bürgern) zur Abgabe anonymer Hinweise genutzt. Auf der anderen Seite erhält ein Hinweisbearbeiter (Korruptionsbeauftragte, Ombudsleute, Revision im Unternehmen oder in der Verwaltung) die Meldungen und kann über die Kommunikationsplattform mit dem Hinweisgeber in einen anonymen Dialog treten.

Die Anwendung des BKMS® Systems schließt folgende Dienste ein:

-  Nutzung des Web- und Anwendungsservers
-  Aktualisierung der Anwendung auf den jeweiligen Entwicklungsstand
-  Zugangssicherheit
-  Datensicherheit
-  Benutzersupport zu Geschäftszeiten der BKAG



Die Nutzung von Software über das Internet als ASP-Konzept (Application Service Providing) wird zukünftig die Anwendungsmöglichkeiten für Unternehmen und Verwaltungen nicht nur technologisch ergänzen, sondern wirtschaftlich maßgeblich Kosten reduzieren. Sie amortisieren sich im Durchschnitt bereits nach 1,3 Jahren (Erhebungen von IDC, SevenOne Media sowie NFO Infratest 2003). Das BKMS® System ist daher zukunftsweisend auf Basis eines ASP-Konzeptes entwickelt worden. Die Investitionen für Computerprogramme, Hardware, Updates, interne Vernetzung, Pflege und IT-Fachpersonal werden maßgeblich reduziert bzw. entfallen.

Wichtige Voraussetzung für den Einsatz von ASP-Konzepten ist die Sicherheit vor unbefugtem Zugriff auf Daten, die wir hier für das BKMS® System in Grundzügen erläutern.

Zertifikat

Die Zertifizierung wurde von einem öffentlich bestellten und vereidigten Sachverständigen erstmals am 16. Juli 2004 durchgeführt. Gegenstand der Überprüfung waren umfangreiche physikalische und programmtechnische Analysen, welche die Sicherheit des Systems und des verwendeten Servers nachwiesen. Das Zertifikat wird seitdem kontinuierlich bei jedem Update des BKMS® Systems aktualisiert.

Das Gutachten bestätigt im Einzelnen:

-  die Anonymität des Hinweisgebers ist geschützt,
-  die Entschlüsselung der direkt vom Kunden empfangenen Meldungen durch Dritte oder die Business Keeper AG selbst ist nicht möglich.

Dipl.-Inf. Markus Müller**Öffentlich bestellter und vereidigter Sachverständiger**

Von der IHK Nord Westfalen öffentlich bestellt und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung im Bereich Telekommunikation, insbesondere Internet

Zertifikat

Hiermit bestätigt der Unterzeichner der Firma

Business Keeper AG
Bayreuther Straße 35
10789 Berlin

aufgrund der am 15.12.2010 technisch untersuchten Version des Business Keeper Monitoring Systems und der verwendeten Serverumgebung,

dass die Anonymität des Hinweisgebers geschützt ist und bei der Verwendung von sicheren Passwörtern, weder die Firma Business Keeper AG noch Dritte, mit einem realistischen Aufwand die Meldungen entschlüsseln oder interpretieren können.

Die Untersuchungen beziehen sich auf die Softwareversion des Sicherheitsmoduls mit folgenden Prüfsummen:

bkwebsecurity.jar

MD5:
 1b1e6b43804bea0170f30cf9c02fcc45

SHA-256:
 bd4570f7bb1e2171c246dac7a137e395988c2bde55c85e16b8e986e091e83495

Dieses Zertifikat basiert auf den im Gutachten **G11 0228 1** festgestellten Untersuchungsergebnissen. Das Zertifikat verliert sofort seine Gültigkeit, wenn die Protokollierungseigenschaften der Server oder die Softwareversion des Sicherheitsmoduls verändert werden.

48308 Senden, den 1.3.2011



Dipl.-Inf. Markus Müller
 Sachverständiger



Anschrift:

Schlossfeld 47
 48308 Senden

Tel. 02597 / 9 66 50
 Fax 02597 / 9 66 51

Sparkasse Coesfeld
 Kto. 9025669 BLZ 40154530

Physikalische Sicherheit

Die Anwendung BKMS® System wird auf dedizierten Servern in einem Hochsicherheitsrechenzentrum betrieben, in welchem beispielsweise auch die Europäische Zentralbank ihre Server betreibt. Ein aktueller SAS 70 Report Germany 2008 für das Rechenzentrum liegt vor. Die Internet-Plattform ist in die bestehenden nationalen und internationalen Netzstrukturen integriert und verfügt über breitbandige Anbindungen zu den wichtigsten Knotenpunkten weltweit.

Die Betriebssicherheit der Server im Hochsicherheitsrechenzentrum wird durch eine automatische Erkennung von Hardware-Störungen innerhalb des Rechnernetzes gewährleistet. Die Administration und Pflege des Servers obliegt ausschließlich der BKAG. Der Zugriff bei einem zu behebernden Hardwarefehler wird durch Spezialisten des Rechenzentrums nur nach Freigabe durch die BKAG ermöglicht. Eine Interpretation von Meldungen durch die BKAG oder durch das Instandhaltungsteam ist in keinem Fall möglich.

Zugriff und Datenübertragung

Das Rechenzentrum ist durch eine aktiv kontrollierte Firewall gesichert. Auf dem Server sind nur die für die Anwendung und Pflege erforderlichen Dienste installiert. Ein von innen gestarteter Datentransfer sowie ein direkter Zugriff auf den Server sind nicht möglich. Damit wird zusätzlich zur Firewall sichergestellt, dass keine Aktivierung eines Datentransfers durch einen unberechtigten Dritten herbeigeführt werden kann.

Mit einer dritten Sicherheitsstufe wird die Datenbank durch eine Firewall gesichert, die nur Anfragen vom lokalen System beantwortet. Das System wird mit Sicherheitsupdates kontinuierlich aktualisiert.

Zur Qualitätssicherung wird jährlich ein Penetrationstest durchgeführt.

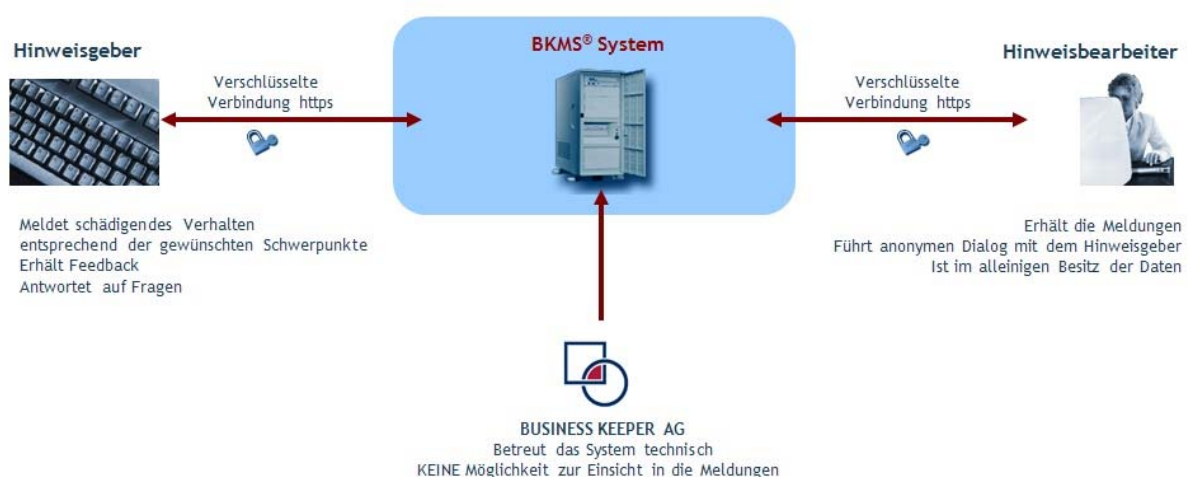


Abb. 1: Sicherheitskonzept BKMS® System

Die Datenübertragung vom Hinweisgeber zum Server als auch vom Bearbeiter zum Server wird mittels https durchgeführt. Eine direkte Kommunikation des Hinweisgebers mit dem Bearbeiter ist über diesen Weg nicht möglich. Die BKAG verwendet für die reine Datenübertragung eine Standardverschlüsselung. Die Sicherheit bei der Übertragung der verschlüsselten Daten wird mit der verwendeten Standardverschlüsselung gewährleistet und bedarf keiner gesonderten Technik. Diese Verschlüsselung wird auch von Banken und Organisationen, die brisante und sehr sicherheitsrelevante Daten übertragen, angewendet.

Alle Verbindungen von der BKAG zum Serversystem für Systempflege und Datensicherung geschehen über SSH.

Schutz vor automatisierten Zugriffen – Sicherheitsabfrage

Als Funktion zum Schutz vor automatisierten Angriffen wird eine Sicherheitsabfrage verwendet. Die Anwendung generiert mit Hilfe eines Zufallsgenerators eine alphanumerische Zeichenfolge, die von der Anwendung in eine Grafik eingebunden wird. Vor Eintritt in den Hinweisgabe- bzw. Hinweisbearbeitungsprozess muss die Zahlen-Buchstaben-Kombination manuell übertragen werden.



Abb. 2: Sicherheitsabfrage BKMS® System






Der Webserver besitzt ein registriertes Serverzertifikat, mit welchem eine eindeutige sichere Legitimation gewährleistet wird. Damit wird garantiert, dass alle Meldungen und Korrespondenzen über eine eindeutige SSL-Verbindung stattfinden.

Anonyme Plattform und Meldedaten

Bei der Entwicklung der Kommunikationsplattform wurde größter Wert auf die Anonymitätswahrung des Hinweisgebers und die Sicherheit der Meldung vor unbefugten Zugriffen gelegt.







Die Anonymitätswahrung des Hinweisgebers wird durch eine geschützte mehrstufige Anmeldeprozedur mit selbst gewähltem Pseudonym und Kennwort erreicht. Mit Hilfe einer individuellen Verschlüsselung werden Meldungsdaten, Postfachdaten und Bearbeitungsdaten vor Zugriffen Dritter geschützt. Nur der legitimierte Empfänger kann die Daten interpretieren. Das Sicherheitssystem verwehrt unbefugten Dritten jeglichen Zugriff.

Damit ist Folgendes gewährleistet:

-  Eine Meldung kann nur von dem autorisierten Bearbeiter des Kunden gelesen werden, an dessen Account sie geschickt wurde.
-  Der Hinweisgeber bleibt absolut anonym und kann trotzdem mittels Postkasten mit dem Bearbeiter der Meldung kommunizieren.
-  Der vom Hinweisgeber eingerichtet Postkasten ist nur von ihm als Besitzer des Postkastens zugänglich.
-  Dritte können weder Meldungsdaten im Bereich eines Kunden noch Meldungen im Postfach interpretieren.
-  Meldungen eines Kunden-Accounts können nicht von der BKAG interpretiert werden.

Sicherheitsverantwortung des Kunden

Die Sicherheit der Kundendaten ist gewährleistet, wenn folgender Ablauf eingehalten wird:

-  Der verantwortliche Ansprechpartner beim Kunden erhält von der BKAG die Zugangsdaten zu seinem Kunden-Account auf dem Server.
-  Mit diesen Zugangsdaten meldet sich der Systemadministrator (Sysadm) an.
-  Der Sysadm ändert umgehend die Zugangsdaten für das entsprechende Kunden-Account. Somit wird sichergestellt, dass der Zugriff nur vom Kunden erfolgen kann. Kein Dritter einschließlich der BKAG hat ab diesem Zeitpunkt Zugriff auf das Kunden-Account.
-  Der Sysadm ändert nun sein Kennwort. Die Nutzung des Kunden-Account liegt jetzt vollständig in der Verantwortung des Kunden.
-  Nach einer erneuten Anmeldung des Sysadm generiert er einen kundenspezifischen Sicherheitsschlüssel (DatenPIN). Dieser ist unter Verschluss zu halten.
-  Erst danach wird vom Sysadm die vertraglich vereinbarte Anzahl der Bearbeiter eingerichtet und nach Genehmigungsstufen, Schwerpunktverantwortlichkeit und Berechtigungen frei geschaltet.

Sicherheitsverantwortung des Hinweisgebers

Die Anonymität des Hinweisgebers kann nur gewährleistet werden, wenn der Hinweisgeber durch seine Meldung und angehängte Dateien keine personenbezogenen Daten sendet oder bekannt gibt.

Datensicherung

Eine Datensicherung findet täglich einmal zu einem internen Server der BKAG über eine SSH-Verbindung statt. SSH ist eine sichere, standardisierte verschlüsselte Verbindung zur Übertragung von Daten.

Die Datensicherung gewährleistet, dass Melde- und Bearbeitungsdaten, die vom Kunden irrtümlich gelöscht wurden, auf dem Server wieder zur Verfügung gestellt werden können. Die verschlüsselten Daten können dann vom Kunden über seine individuellen Berechtigungen und Zugangsdaten entschlüsselt und damit gelesen und interpretiert werden. Das Sicherheitskonzept erlaubt zu keinem Zeitpunkt das Interpretieren der Daten durch die BKAG.

Das Sicherheitskonzept der BKAG stellt mit seinen Techniken und Abläufen für die Meldung sowie den Dialog den derzeit höchstmöglichen Standard dar und wird kontinuierlich anhand der neuesten Erkenntnisse erweitert.