Sicherheit Minddistrict-Applikation

FAQ Sicherheit der Applikation

1. Ist die Applikation sicher?

o Ja, unsere Applikation ist sicher. Wir arbeiten gemäß NEN7510 in Kombination mit WGBO/WBP und Bundesdatenschutzgesetz (BDSG).

o Das Zertifizierungsverfahren o.b.v. ISO 27001/2:2005 läuft. Diese ISO 27001 stimmt überein mit den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

2. Welche Sicherheitsmaßnahmen sind getroffen?

A) **Hosting Povider**. Intermax Data Center (ISO27001 zertifizierter Hosting Provider):

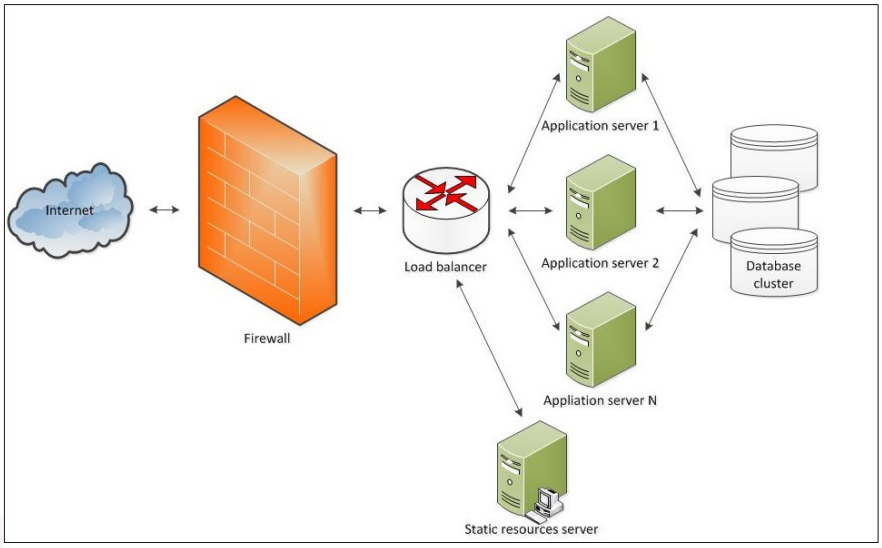
Minddistrict hat Intermax als seinen Hosting Provider ausgewählt. Intermax ist ein nach ISO27001 zertifizierter Hosting Provider. ISO27001 ist die Basis für die Serien der NEN 751x-Normen. Intermax stellt seine Dienste zahlreichen niederländischen Krankenhäusern und anderen medizinischen Einrichtungen zur Verfügung.

Intermax besitzt und verwaltet zahlreiche VMware-Cluster und stellt seinen Kunden virtuelle Maschinen zur Verfügung. Intermax betreut die Internet- und power connections, Netzwerke und Firewalls.

Die Virtualisierungstechnologien von VMware und Intermax erlauben es Minddistrict, seine Aktivitäten zu messen. Diese virtuellen Maschinen von Intermax sind Ubuntu/Linux-Server.

B) **Sicherheits-Webapplikation.** Die Applikation von Minddistrict baut auf der Benutzung von Zope - Technologien auf. Zope ist ein Framework für die Erstellung von Sicherheits-Webapplikationen, die für mehr als 10 Jahre genutzt werden können und herausragende Sicherheitsergebnisse erzielen.

C) **Separate Operationsumgebungen**. Getrennte Bereitstellungs-, Test- und Produktionsumgebungen (SSH-Zugang): Minddistrict hält die Bereitstellungs-, Test- und Produktionsumgebungen strikt getrennt. Die Produktionsarchitektur sieht wie folgt aus:



D) **Jeder Kunde mit eigener Datenbank.** Virtuell getrennte Datenbanken pro Einrichtung:

Minddistrict nutzt einen ZEO-Cluster, um die Anwendungsdaten zu speichern. Der Cluster besteht aus multiplen Knotenpunkten, um im Falle eines Server-Ausfalls die Daten weiterhin sicher bereitstellen zu können.
Die Daten jedes Minddistrict-Kunden werden separat in der Objekt-Datenbank gespeichert. Es ist z.B. nicht möglich, von der Applikation von Kunde A aus auf die Daten von Kunde B zuzugreifen.

E) **Firewall.** HW Firewall für die Applikation, SW Firewalls pro Server: Im äußeren Umkreis der Minddistrict-Infrastruktur überwacht eine zusätzliche Fortigate Hardware-Firewall den ein- und ausgehenden Datenverkehr. Die Firewall ist angewiesen, nur eingehenden HTTP- und HTTPS-Traffic aus dem Internet zuzulassen. Die Firewall kann auch so eingestellt werden, daß Denial-Of-Service Angriffe oder Throttle Traffic blockiert werden.

Auf den Servern hinter der ersten Firewall nutzen wir die iptables Software Firewalls, um den Traffic zwischen den Minddistrict-Servern zu überwachen.

F) **Sichere Verbindungen.** Die Applikation wird durch HTTPS (SSL) Verbindungen gesichert.

Eine HTTPS-Verbindung ist eine normale HTTP-Verbindung mit zusätzlicher SSL-Verbindung. Diese SSL-Verbindung verschlüsselt hierbei den HTTP-Verkehr, wodurch der Verkehr, falls er abgefangen wird, nicht gelesen werden kann, ohne den Verschlüsselungsalgorithmus zu entschlüsseln. Dies steht im Gegensatz zum normalen HTTP-Verkehr, der als unverschlüsselter Text über die Verbindung gesendet wird. Dadurch würde er bei einem Abfangen leicht auszulesen sein.

G) **Logging.** Audit Trails aller Benutzer werden beibehalten.

H) **Back-up** (pro Stunde): Die Applikationsdaten werden stündlich gesichert. Jede Nacht wird ein volles Back-up an einen externen Sicherungs-Server übertragen. Alle drei Monate wird ein verschlüsseltes Back-up dieses Zeitraumes an einen Tresor von ein Notar gesendet.

3. **Wie loggen sich die Benutzer ein?**
   a) Benutzername und Passwort: Es ist nicht möglich, durch die Passwort-vergessen-Funktion Benutzername und Passwort herauszubekommen.

   b) Hohe Sicherheit: Email mit Link statt Daten: Email ist ein unsicheres Medium. Zwar verschickt die Minddistrict-Applikation auch Emails, diese enthalten jedoch keine vertraulichen Informationen. Sie enthalten lediglich einen Verweis zur eigentlichen Nachricht, die sich in der Applikation befindet und per Log-in mit einem Passwort abrufbar ist.

4. **Es handelt sich um eine SAAS Applikation. Wie kann ein korrekter Umgang mit den Daten garantiert werden?**
   Durch den Abschluß eines entsprechenden SLA (Service Level Agreement), das die Erfüllung oben stehender Punkte gewährleistet.

5. **Wer kann meine Daten einsehen? Ist die Privatsphäre gesichert?**
   Nur bestimmte Mitarbeiter von Minddistrict haben Zugang zu den Produktionsservern.

   Softwarefehler werden niemals unter Verwendung von Hotfixes in der Produktionsumgebung behoben. Die Produktionsdatenbank wird auf eine Testmaschine heruntergeladen und die Daten vor der Fehlersuche anonymisiert. Nachdem der Fehler behoben ist, wird eine neue Version erstellt und installiert.

6. **Wie regelt Minddistrict die Geschwindigkeit der Applikation?**
   Die Serverlastverteilung entpackt den SSL -Verkehr und leitet ihn an die geeignete Applikation oder den Static Resources Server weiter.

   Static Resources (Video, Audio, JavaScript, CSS und Bilder) werden von extra für diese Aufgabe vorgesehenen Servern geliefert. Dies führt zu schnelleren Ladezeiten der Webseiten.