MiBida Security Paper

Infrastructuur: MiBida wordt gehost in Nederlandse datacentra die fysiek van elkaar gescheiden staan op 6 locaties in Nederland. Al deze centra zijn ISO27001, NEN9001, NEN7510 en PCI-DSS gecertificeerd. Deze servers zijn voorzien van een 4 uurs back-up cyclus over de 6 centra met een retention van 7 dagen.

Verbinding met de servers: MiBida maakt sec gebruikt van beveiligde verbindingen. Gebruikers maken gebruik van TLS verbindingen met A+ beveiligingsniveau. De server communiceren onderling via SSHv2-TL en alle communicatie voor onderhoud wordt getunneld over SSHv2.

Authenticatie: Voor authenticatie wordt in de basis gebruik gemaakt van password authenticatie met optionele Multi-Factor-Authenticatie (Location, IP, U2F, HOTP en TOTP). Wachtwoorden worden voor verzending naar de server gehasht (zo zijn deze nooit bij ons bekend) en worden gecontrolleerd door middel van een PBKDF2 algoritme. (met een variabel aantal iteraties afhankelijk van computatietijd).

Hier houden de meeste leveranciers op, en beschouwen ze de dienst als veilig, maar MiBida gaat verder.

Sleutelbos: Wanneer de authenticatie geslaagd is wordt met een zwaarder PBKDF2 algoritme een AES128 of AES256 sleutel gegenereerd, deze sleutel wordt vervolgens gebruikt om de sleutelbos van de gebruiker te ontsleutelen. Deze sleutelbos bevat 3 AES128 of AES256 sleutels en minimaal een RSA2048 sleutelpaar voor handtekeningen en een (sterkere) Elliptic Curve sleutelpaar voor sleuteloverdracht. De server load van deze stap maakt brute-forcing van wachtwoorden onmogelijk, dit maakt de authenticatie ook extra veilig.

Aangezien bij ons de wachtwoorden niet bekend zijn, is het voor ons ook onmogelijk om de sleutelbos van een gebruiker te openen zonder medewerking van de gebruiker.

Wachtwoord herstel: Wanneer de gebruiker voor het eerst inlogt wordt deze via een veilig kanaal een herstelcode aangeboden. Mocht de gebruiker zijn wachtwoord zijn vergeten dan kan de herstelcode (256-bit) met eventueel toevoeging van de ingestelde MFA worden aangewend om deze te herstellen. Aangezien wij geen toegang hebben tot de gegevens van de gebruiker, kunnen we zonder wachtwoord en herstelcode de klant niet verder helpen. Alle diensten die dit wel kunnen (Lees: 95% van alle internetdiensten) zijn per definitie “lek”. Personeel van de aanbieder kan dan ook zonder toestemming van de klant bij de gegevens van de klant.

Data: Alle rondom de cliënt opgeslagen gegevens worden opgeslagen met unieke AES sleutels, hiervoor word de volgende cipher gebruikt: AES/CTR/NoPadding (de suite hoeft geen padding toe te voegen omdat de kluis gegevens combineert en comprimeert in pages). De sleutels waarmee data is opgeslagen zijn alleen door middel van de sleutelbos van de gebruiker te bereiken. Om te voorkomen dat gegevens onopgemerkt gewijzigd kunnen worden zijn alle gegevens voorzien van een HMAC verificatie.

Sleuteloverdracht: Een gebruiker kan zelf bepalen wie toegang kan krijgen tot zijn gegevens, de sleutels waarmee data wordt versleuteld kunnen worden gekopieerd naar de sleutelbos van gebruikers of beveiligingsgroepen. Dit gebeurd via de Eliptic-Curve Key Exchange onder het ECIES encryptie schema of via een RSA4096 Key Exchange. Dit zorgt er voor dat een sleutel kan worden over gedragen van de ene naar de andere gebruiker zonder dat deze op enig moment voor derden zichtbaar hoeft te zijn.

MiBida veilige communicatie oplossingen

Chat: De berichtenservice maakt net als alle andere diensten van MiBida gebruik van de datakluis. Elk gesprek heeft een aparte sleutel die wordt gedeeld met de deelnemers in het gesprek. Omdat de chat vast versleuteld is, en daarnaast ook nog wordt verstuurd over een beveiligde verbinding spreekt men vaak van Double-Ratchet encryption. Merk op dat gegevens onder geen beding onversleuteld worden opgeslagen door bijvoorbeeld apps en andere MiBida applicaties. Ook wanneer je je mobile device kwijt raakt, zijn je gegevens veilig (dit in tegenstelling tot bijvoorbeeld WhatsApp).

Videocommunicatie: Voor videocommunicatie wordt gebruik gemaakt van directe P2P verbindingen die E2E (van gebruiker tot gebruiker) versleuteld zijn. Er zijn dus buiten de deelnemende gebruikers geen apparaten of diensten die de gegevens ontsleutelen. (Dit in tegenstelling tot bijvoorbeeld: Skype, Zoom en vele andere bekende videodiensten, waar gegevens op tussenliggende servers voor media verwerking ontsleuteld worden). Bij de videocommunicatie wordt gebruik gemaakt van verschillende cipher suites afhankelijk van de mogelijkheden van de deelnemers. Deze zijn echter allemaal van het hoogste beveiligingsniveau met Perfect Forward Secrecy (Waneer de computer van een van de deelnemers na het gesprek wordt gehackt is het gesprek alsnog niet te ontsleutelen). Veel gebruikte cipher suites zijn: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 met AES_CM_128_HMAC_SHA1_32 en TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 met AES_CM_128_HMAC_SHA1_32. De gebruikte suites zijn state-of-the-art en door de snelle doorontwikkeling beter dan in de bekende proprietary systemen zoals: Zoom en Skype waardoor deze in tegenstelling tot onze videocommunicatie niet voldoen aan de strenge Amerikaanse HIPAA normering (bovenop de in Nederland geldende NEN7510).

P2P-file exchange: Tijdens een videogesprek kunnen bestanden buiten onze servers om via het beschikbare beveiligde communicatiekanaal tussen de deelnemende gebruikers worden gedeeld. In onze ogen de meest veilige vorm van overdracht, je ziet aan wie je de bestanden gaat geven.

Notificaties: Ook notificaties WebPush (Web), FCM (Android) en APNS (Apple) worden point-to-point encrypted zodat ook deze alleen leesbaar zijn bij de rechtmatige ontvanger.

Copyright

Disclaimer

Dit document beschrijft producten en diensten van MiBida B.V. Genoemde producten en diensten mogen door MiBida B.V te allen tijde worden aangepast of stopgezet indien hierover geen verdere afspraken met de betreffende partij bestaan. Daarnaast is dit document bedoeld als instructief hulpmiddel bij installatie en kunnen er geen rechten ontleend worden aan de inhoud van het document.