Blue10 B.V.
Oude Middenweg 17
2491 AC Den Haag | NL

T +31 (0) 88 258 31 00
blue10@blue10.com
www.blue10.com

KVK 27195343
BTW NL809410199B01
ING Bank NL06INGB0683496832

WHITEPAPER

Security & Privacy

Laatste review: Januari 2025

1. Inleiding

Bij Blue10 geloven we in de kracht van automatisering. We ontwikkelen software die onze klanten helpt om handmatig en repeterend werk te elimineren en zijn in onze eigen organisatie ook altijd op zoek naar manieren om repeterend werk te automatiseren. We maken zowel in de dienstverlening aan onze klanten als voor onze eigen kantoorapplicaties zoveel mogelijk cloud applicaties. Onze eigen dienstverlening (de Blue10 dienst) is volledig gebaseerd op cloud technologie, waarbij toegewerkt wordt naar een volledig geautomatiseerd CI/CD (Continuous Integration / Continuous Delivery) proces. Dat onze infrastructuur, en daarmee onze dienstverlening, veilig en betrouwbaar moet zijn is een essentieel uitgangspunt dat dagelijks onze aandacht heeft. Veiligheid, beschikbaarheid en betrouwbaarheid vormen ons bestaansrecht.

In deze whitepaper geven we jou – als klant of prospect – inzicht in de belangrijkste maatregelen die we hebben getroffen om informatiebeveiliging en privacy in onze werkwijze, onze processen en onze systemen en infrastructuur te waarborgen.

2. Inhoudsopgave

3. Medewerkers

Een veilige omgeving, waarbij zorgvuldig met informatie wordt omgegaan, begint bij onze medewerkers. Tijdens de onboarding van nieuwe collega's besteden we aandacht aan screening en wijzen we nadrukkelijk op het belang van informatiebeveiliging en privacy. Iedere Blue10 medewerker tekent een geheimhoudingsverklaring en van medewerkers die toegang hebben tot klantdata verlangen we een VOG. In teambijeenkomsten wordt regelmatig aandacht besteed aan security en privacy om het kennis- en bewustwordingsniveau van onze mensen op peil te houden, en waar noodzakelijk volgen onze medewerkers specifieke trainingen om hun werkzaamheden bij Blue10 adequaat uit te kunnen voeren.

4. Informatiebeveiligingsbeleid

Blue10 heeft haar uitgangpunten op het gebied van informatiebeveiliging in beleidsregels vastgelegd en ziet actief toe op de naleving daarvan. Integraal onderdeel van dit beleid zijn policies en procedures op het gebied van wijzigingsbeheer, incidentmanagement, logische- en fysiek beveiliging en continuïteit. Het informatiebeveiligingsbeleid wordt periodiek door de directie herzien op basis van recente ontwikkelingen en dreigingsparameters.

5. Cloud only

Blue10 biedt een Cloud product aan haar klanten en ook intern worden alleen cloud applicaties gebruikt. Dit is, ook vanuit beveiligingsoogpunt, een zeer bewuste keuze. We hebben geen on-premise infrastructuur of een eigen datacenter, maar maken gebruik van public cloud services van gerenommeerde partijen, in het bijzonder van Microsoft Azure. Dit geldt zowel voor de (door)ontwikkeling van onze dienst als voor het operationele beheer. Blue10 maakt zoveel mogelijk gebruik van de PaaS (Platform as a Service) diensten van Microsoft Azure. Hierbij wordt de beveiliging op infrastructuurniveau geregeld door MS Azure, waarmee de kans op configuratiefouten en andere beveiligingsrisico's sterk gereduceerd wordt. De Azure-locatie ('region') waarop Blue10 is gehost is West-Europa (Amsterdam). Zie voor meer informatie over de beveiligingsmaatregelen van Microsoft Azure: https://www.microsoft.com/en-us/trustcenter/cloudservices/azure.

Voor optimale toegankelijkheid en aanvullende beveiliging van onze Blue10 dienst maken we gebruik van Azure Front Door als Content Delivery Netwerk (CDN) en het daaraan inherente Intelligent Network Threat Protection.

6. Security incident & event monitoring

Blue10 heeft procedures geïmplementeerd om op continue basis onze systemen en netwerken te monitoren op verdachte gebeurtenissen of afwijkingen die een indicatie kunnen zijn van beveiligingsproblemen of kwetsbaarheden (security incident & event monitoring (SIEM)). Wij maken daarbij gebruik van Microsoft Sentinel, een schaalbare en *cloud-native* SIEM-oplossing die naadloos aansluit bij onze op Azure gebaseerde architectuur.

7. Logische toegangsbeveiliging

Toegang tot informatie in de Blue10 systemen geven we uitsluitend aan medewerkers die deze toegang vanwege hun rol en functie in onze organisatie nodig hebben (*role based access)*. Daarbij maken we waar nodig onderscheid tussen rechten om informatie te wijzigen en rechten om informatie te raadplegen. Daar waar mogelijk gebruiken we geautomatiseerde middelen om authenticatie dan wel autorisatie af te dwingen (zoals Azure Active Directory en Azure Role Based Access (RBAC)).

Als medewerkers binnen Blue10 van functie veranderen of de organisatie verlaten worden hun rechten aangepast respectievelijk ingetrokken.

Voor *identity management* en authenticatie steunen we sterk op maatregelen die worden afgedwongen met Azure Active Directory. We maken een strikt onderscheid tussen de kantoortenant, waarbinnen Blue10 medewerkers gebruik kunnen maken van kantoorapplicaties, en de productietenant waarbinnen onze Blue10 dienst aangeboden wordt. Er kunnen situaties ontstaan waarin, al dan niet tijdelijk, bepaalde rechten moeten worden toegekend aan beheerders in het kader van probleemoplossing of incidentafhandeling. We gebruiken hiervoor Microsoft's Privileged Identity Management, dat zorgt voor een beheerste, tijdelijke en controleerbare rechtentoekenning.

We slaan klantgegevens op in gescheiden omgevingen binnen de Blue10 architectuur, te weten een klant specifieke container in Azure object storage (Blob) en een klant specifieke database binnen een connection pool van SQL Server. Dit draagt bij aan de logische scheiding van klantomgevingen en reduceert het risico van ongeautoriseerde toegang.

8. Fysieke toegangsbeveiliging

Blue10 werkt vanuit een eigen kantooromgeving in Den Haag. Door onze cloud filosofie en het ontbreken van een *on-premise* infrastructuur, in combinatie met ons clear screen/clean desk-beleid en encryptie van endpoints zoals laptops, is het risico van fysieke toegang tot (apparatuur of media met informatie) zeer beperkt. Desalniettemin besteden we veel aandacht aan het beperken van ongewenste fysieke toegang tot ons kantoor (zoals zonering, badges en kaartlezers, alarm en een bezoekersprotocol).

Voor de fysieke veiligheid van onze infrastructuur in datacenters van Microsoft steunen we op de maatregelen die Microsoft daartoe neemt. Vanzelfsprekend nemen we kennis van assurancerapportages en certificeringen die de kwaliteit van de door Microsoft genomen maatregelen aantonen.

9. Endpoint security

Blue10 hanteert als uitgangspunt dat vanuit beveiligingsoptiek geen klantdata wordt opgeslagen op endpoints (laptops, workstations, mobiele devices). Opslag van andere gegevens op deze endpoints vindt versleuteld plaats met behulp van BitLocker. Blue10 monitort en detecteert malware en kwetsbaarheden op endpoints door gebruik van producten als Intune en Microsoft Defender. Nieuwe endpoints worden voorzien van een goedgekeurde, standaard configuratie. Afwijkingen van die configuratie worden gedetecteerd en opgevolgd. Het gebruik van USB-sticks is niet toegestaan en is technisch onmogelijk gemaakt.

10. Encryptie

Klantgegevens worden opgeslagen in Azure object storage (Blob) en SQL Server databases. De data zijn versleuteld 'at rest', waarbij het sleutelbeheer door Microsoft wordt uitgevoerd. De verbinding tussen de klantomgeving en de Blue10-dienst ('data in transit') is versleuteld met TLS 1.2. Deze encryptiemaatregelen waarborgen de confidentialiteit van gegevens.

11. Logging en monitoring

Het vastleggen van relevante systeemgebeurtenissen (logging) is belangrijk vanuit het oogpunt van het afhandelen van incidenten, voor detectie van afwijkingen en voor de controleerbaarheid van uitgevoerde werkzaamheden. Blue10 maakt hiervoor gebruik van faciliteiten van Azure, met name Log Analytics workspaces en Sentinel (cloud-native SIEM). Loggevevens in Azure Log Analytics worden twee jaar bewaard.

Voor monitoring van systeemresources en performance maakt Blue10 eveneens gebruik van de uitgebreide functionaliteiten, dashboards en metrics van Microsoft Azure die een voortdurend inzicht geven in de prestaties van onze dienst en die alerts genereren op het moment dat vooraf gedefinieerde drempelwaarden worden bereikt. Zo kan tijdig worden ingegrepen als problemen ten aanzien van de 'gezondheid' van onze dienst dreigen te ontstaan. Voorbeelden van key processen die binnen de Blue10 dienst continu worden gemonitord:

- Beschikbaarheid infrastructuur
- Gemiddelde reactietijd website
- Reactietijd van een login-request
- Doorlooptijd per pagina van binnenkomst tot conversie;
- Doorlooptijd van het herkenningsproces per pagina
- Reactietijden tussen de Blue10 dienst en de verschillende boekhoudsystemen

12. Back-up & Restore

Alle databases draaien op het SQL Azure platform. Dit platform biedt ingebouwde redundantie, back-up en restore mogelijkheden. Blue10 maakt onderscheidt in twee typen back-ups:

1. Blue10 maakt volledige, point-in-time, back-ups op Microsoft Azure die voor een periode van 7 dagen worden bewaard. Dit betekent dat we, indien noodzakelijk, de situatie kunnen herstellen zoals die op een gegeven punt in de afgelopen zeven dagen was.
2. Daarnaast maakt Blue10 eenmaal per week een extra back-up op Microsoft Azure die voor een periode van 8 weken wordt bewaard.

Voor opslag van bestanden wordt gebruik gemaakt van Azure Blob Storage. Deze dienst biedt onbeperkte schaalbaarheid en ingebouwde redundantie. Bij verwijdering van bestanden in de Blob wordt gebruik gemaakt van soft delete. Dit houdt in dat bestanden tot 30 dagen na verwijderen nog te herstellen zijn.

13. Development

Blue10 richt zich sterk op het onderhoud en de doorontwikkeling van de Blue10 dienst. Blue10 ontwerpt en bouwt de software in eigen beheer en houdt daarmee maximale controle over de kwaliteit van hetgeen ontwikkeld wordt. Nieuwe releases van de Blue10 dienst worden via een proces van *continuous delivery* aan onze klanten ter beschikking gesteld, maar niet voordat een zorgvuldig ontwikkel- en wijzigingsbeheerproces is doorlopen. Daarbinnen maken we gebruik van solide ontwikkelstandaarden, een uitgebreid scala aan testen (unit-, component-, load- en regressietesten), *peer reviews* en geautomatiseerd ondersteunde kwaliteitscontrole op de coding waarvan geaccepteerde beveiligingsprincipes deel uitmaken. Het gehele ontwikkel- en deployment traject wordt ondersteund en gefaciliteerd door Azure DevOps.

14. Penetration testing

Minimaal één keer per jaar laat Blue10 een penetratietest uitvoeren op de applicatie-infrastructuur van haar dienst. De penetratietest wordt uitgevoerd door een onafhankelijke en gespecialiseerde externe partij, die vervolgens rapporteert over eventuele kwetsbaarheden in onze beveiliging en adviseert over te nemen maatregelen voor verbetering. Blue10 geeft actieve follow-up aan de bevindingen uit deze penetratietests.

15. Assurance

In toenemende mate wordt van organisaties verwacht dat ze aantoonbaar ‘in control’ zijn over hun activiteiten. Die aantoonbaarheid is voor vrijwel iedere organisatie op het gebied van interne processen al een enorme uitdaging. Het wordt een nog grotere uitdaging op het moment dat bepaalde diensten worden uitbesteed aan een serviceorganisatie, zoals Blue10. Klanten rekenen op de beveiliging, beschikbaarheid en integriteit van deze externe dienstverlening en zoeken daarnaast ook naar zekerheid dat die kwaliteit wordt geborgd.

Bij Blue10 geloven we in de kwaliteit van onze dienstverlening en vinden we het belangrijk dat we die kwaliteit ook aan onze klanten kunnen aantonen. Een ‘security en privacy whitepaper’ zoals dit document is daartoe niet voldoende. Daarom verstrekken we jaarlijks een tweetal assurance-rapporten over onze interne beheersing en informatiebeveiliging. Deze rapportages (volgens de ISAE 3402 respectievelijk de SOC2- standaard) beschrijven onze dienstverlening en de maatregelen die we hebben getroffen om de beheersing van de Blue10 dienst te borgen. Een onafhankelijke (register) IT-auditor toetst en beoordeelt of deze beschrijving overeenkomt met de werkelijkheid en of de beschreven maatregelen daadwerkelijk zijn geïmplementeerd en naar behoren functioneren. Hiermee helpen we onze klanten om aan te tonen dat ze, voor de activiteiten die ze aan Blue10 uitbesteden, ‘in control’ zijn. We vinden het nog belangrijker dat we met deze assurance rapporten de benodigde zekerheid, betrouwbaarheid en kwaliteit van onze diensten kunnen aantonen en dat dit een solide fundament biedt voor de keuze voor Blue10 als preferred dienstverlener én partner.

Klanten, prospects (en hun auditors) kunnen de meest recente assurancerapportages ter inzage krijgen. Voor meer informatie: https://www.blue10.com/certificeringen-blue10/

16. Data Pro code

Op het gebied van privacy, en dan met name in de rol van verwerker, conformeert Blue10 zich aan de Data Pro Code. Dit is een door de Autoriteit Persoonsgegevens goedgekeurde gedragscode die is opgesteld door NL Digital, de brancheverenigingvan IT bedrijven. Na een onafhankelijke audit worden we jaarlijks gecertificeerd voor het naleven van deze gedragscode, die aangeeft dat we zorgvuldig en in lijn met de AVG omgaan met persoonsgegevens die klanten ons voor verwerking toevertrouwen. Dit komt onder meer tot uitdrukking in het verstrekken en afsluiten van verwerkersovereenkomsten, intern toezicht door onze Functionaris Gegevensbescherming en een gestructureerd proces voor de correcte afhandeling van eventuele datalekken.

17. Responsible disclosure

Bij Blue10 vinden wij de veiligheid van onze systemen, ons netwerk en onze producten erg belangrijk. Ondanks dat wij veel zorg besteden aan informatiebeveiliging, kan het voorkomen dat een zwakke plek wordt ontdekt. Voor zover zo’n kwetsbaarheid door derden (niet zijnde Blue10 medewerkers, klanten, of onze leverancier) wordt vastgesteld, heeft Blue10 een *Responsible Diclosure*-beleid, waarin we afspraken maken met melders van kwetsbaarheden en ons committeren aan een serieuze en spoedige oplossing van eventuele problemen. Onze responsible disclosure is hier te vinden: https://www.blue10.com/responsible-disclosure/

18. Wat verwachten we van onze klanten?

Ondanks de inspanningen die Blue10 levert op het gebeid van informatiebeveiliging en privacy is een veilig en verantwoord gebruik van de Blue10 dienst ook afhankelijk van een aantal maatregelen waarvoor onze klanten zelf verantwoordelijk zijn.

Een toereikende IT infrastructuur.
Denk hierbij aan moderne werkstations of laptops voor medewerkers die van de Blue10 dienst gebruik maken, met een moderne browser die van de laatste versie-updates is voorzien. Vanzelfsprekend is ook de beschikbaarheid van een stabiele internetverbinding essentieel voor het gebruik van de Blue10 dienst.

Een keuze voor een authenticatiemethode die past bij het informatiebeveiligingsbeleid.
Blue10 biedt meerdere mogelijkheden voor gebruikers om aan in de Blue10 dienst in te loggen, uiteenlopend van een ‘gewone’ combinatie van gebruikersnaam en wachtwoord tot een koppeling met identity management in een bestaande Microsoft Active Directory.

Een zorgvuldige omgang met authenticatie-informatie.
Om ongeautoriseerde toegang en ongeautoriseerde boekingen te voorkomen zal de klant ervoor moeten zorgen dat authenticatie-informatie (zoals gebruikersnamen en wachtwoorden) vertrouwelijk zijn en blijven, en in lijn met het eigen beleid worden vernieuwd.

Een zorgvuldig gebruikersbeheer.
Klanten voeren zelf het beheer over geautoriseerde gebruikers en hun rechten in de Blue10 dienst. Het is van belang dat zij deze in lijn brengen en houden met hun eigen administratieve organisatie en interne controle-eisen op het gebied van bevoegdheden en functiescheidingen.

Een adequaat validatieproces.
Alhoewel de Blue10 dienst een voorstel doet van herkende waardes van een factuur en een daarbij horend codeer- en/of boekingsvoorstel, is het de verantwoordelijkheid van de klant om een dergelijk voorstel te controleren, valideren, en autoriseren. De juistheid van de verwerkte gegevens is en blijft een verantwoordelijkheid van de klant.

Solide beheer van stamgegevens.
Het beheer van stamgegevens is van essentieel belang in een administratieve omgeving, omdat foutieve stamgegevens kunnen zorgen voor diverse fouten later in de administratieve verwerking van de organisatie. De Blue10 dienst steunt in belangrijk mate op die stamgegevens en daarmee ook op de kwaliteit van de processen bij de klant om de juistheid van stamgegevens te waarborgen.

Informatieverstrekking.
Om goed en snel te kunnen reageren op eventuele storingen en problemen in het gebruik van onze dienst rekenen we erop dat onze klanten ons informeren over problemen die ze daarbij ondervinden. Feedback over onze dienstverlening of suggesties voor verbetering stellen we zeer op prijs en wordt proactief opgevolgd.