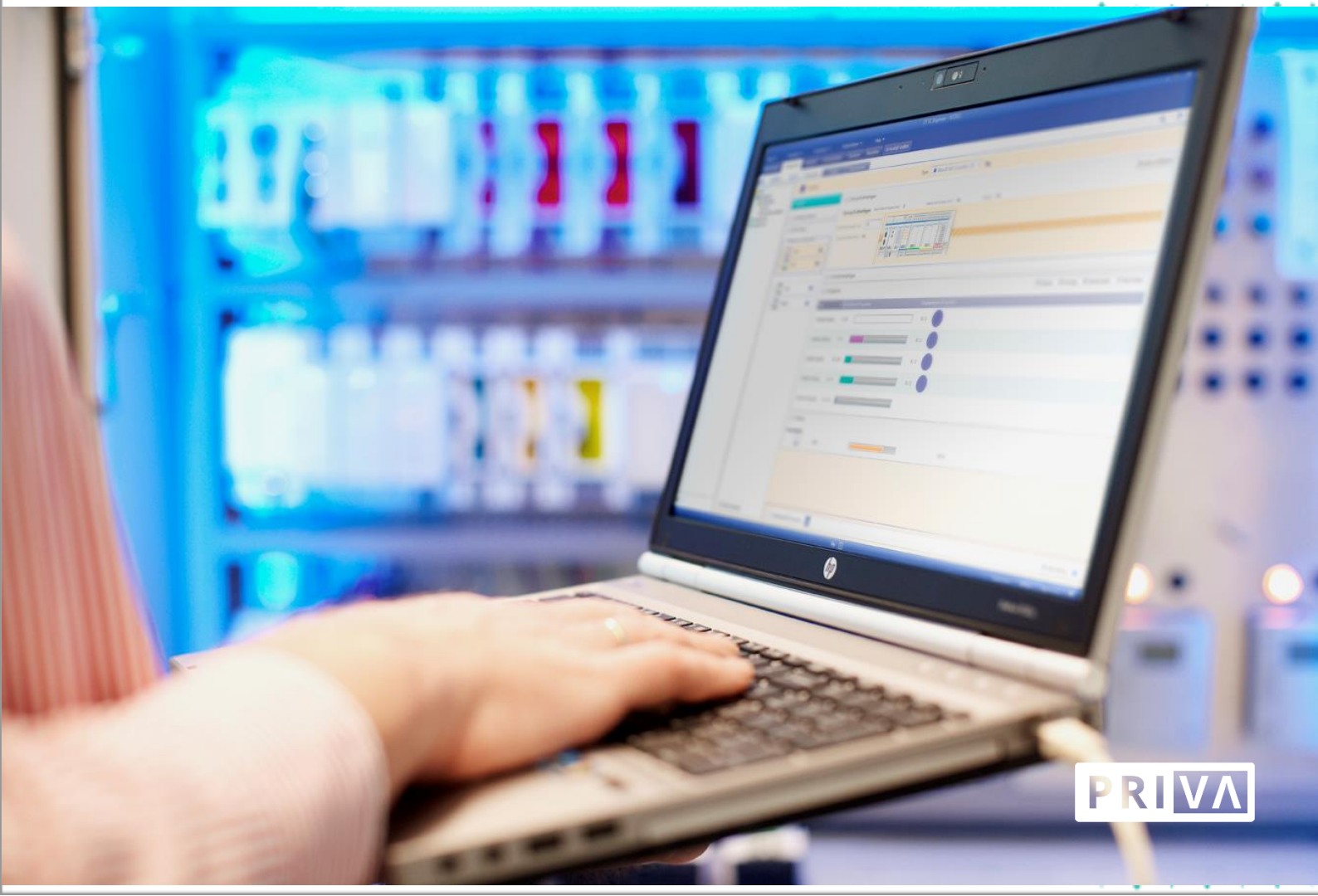
Informatiebeveiliging

Whitepaper



Deze whitepaper voor informatiebeveiliging geeft een algemeen overzicht van de informatiebeveiligingsmaatregelen genomen door Priva.

Dit is een publiek document om duidelijkheid te geven aan Priva's klanten en partners en transparant te zijn over de informatiebeveiligingsmaatregelen die geïmplementeerd zijn en onderhouden worden binnen Priva. In het geval van aanvullende vragen, kunt u contact opnemen met Priva's SQC-team (Security, Quality en Compliance) via sqc@priva.com

Inhoudsopgave

1. Organisatorische beveiligingsmaatregelen

Priva heeft een strategisch beleid dat de fundering is voor andere beleidsstukken. Dit strategisch beleid geeft hierdoor richting aan de verdere implementatie van informatiebeveiliging en kwaliteit binnen Priva. Het definieert het doel, inhoud, structuur, verantwoordelijkheden en het onderhouden van het beleid.

Om een dergelijk continuïteitsniveau te bieden, heeft Priva een Integrated Management System (IMS) geïmplementeerd in overeenstemming met de International Standards for Information Security (ISO/IEC 27001) en Quality Management (ISO/IEC 9001). N.B.: deze whitepaper is gericht op informatiebeveiliging. Ook geeft het IMS een duidelijk overzicht van alle beveiligingsmaatregelen. Bovendien is het IMS een handig hulpmiddel om de beveiliging van Priva continu te verbeteren. Priva hanteert strikte beleidslijnen en procedures door rekening te houden met de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen en diensten van Priva.

1.1 Compliance

Priva heeft een toegewijd SQC-team om ervoor te zorgen dat Priva voldoet aan de geldende normen. Zij overwegen welke controles, processen en maatregelen nodig zijn om aan deze normen te voldoen.

Priva voldoet aan de volgende normen op het gebied van informatiebeveiliging en privacy:

- ISO / IEC 27001 – Beheer van informatiebeveiliging
- AVG

1.2 Screening van medewerkers

Om ervoor te zorgen dat medewerkers en opdrachtnemers geschikt zijn voor de functies waarvoor zij in aanmerking komen, heeft Priva richtlijnen opgesteld voor de screening van iedereen die voor Priva werkzaam is. Priva houdt er rekening mee dat er een gegronde reden moet zijn en dat de screening noodzakelijk is om te verifiëren of iemands profiel en iemands verleden voldoen aan de gewenste vertrouwelijkheids- en integriteitsniveaus voor een specifieke functie binnen Priva. Totdat de screening met succes is uitgevoerd, wordt de medewerker niet toegewezen aan zijn rol.

1.3 Security awareness

Naast IMS-gerelateerde verantwoordelijkheden zijn er trainingen voor alle medewerkers zowel in dienst als ingehuurd (eindgebruikers van het Priva netwerk). De SQC-training van de Priva Academy is een verplichte training voor iedere medewerker of opdrachtnemer die bij Priva werkt. Een onderdeel van deze SQC-training is security awareness. Het is noodzakelijk om periodiek de SQC-training met succes af te ronden. Aan de hand van testen wordt de kennis van de medewerker getoetst. De medewerker dient voldoende kennis te hebben van de beveiligingsprincipes van Priva om de training met succes te kunnen doorlopen. Daarnaast zijn er enkele rollen die aanvullende security awareness sessies krijgen, op basis van het beveiligingsniveau van informatie waarmee iemand werkt.

1.4 Een toegewijd Information Security team

Priva heeft een toegewijd Information Security-team, als onderdeel van het SQC-team. Het Information Security-team is verantwoordelijk voor de uitvoering en coördinatie van de beveiligingsinitiatieven. Dit team ontwikkelt en implementeert bedrijfsinformatiebeveiligings- en privacybeleid en daaraan gerelateerde documenten. Daarnaast ontwikkelt dit team processen om de informatiebeveiliging binnen Priva te managen. Zij hebben in Priva-brede projecten een rol in het adviseren van diverse teams over beveiligingsrisico's en hoe deze risico's te beheersen.

2. Fysieke beveiliging

2.1 Priva kantoren

Priva regelt de toegang tot hun kantoren en faciliteiten met behulp van toegangskaarten, sloten en alarmen. Priva geeft toegang aan medewerkers en inhuur op basis van hun ‘need-to-know’ voor een specifieke rol. Bezoekers worden door de gebouwen geleid. De afdeling Human Resource (HR) wijst medewerkers en opdrachtnemers toe aan specifieke rollen. De afdeling Hospitality beheert de toegang tot kantoren en faciliteiten van Priva. Ook beoordelen zij periodiek de toewijzing van toegangskaarten. De toegang tot Priva-gebouwen wordt gecontroleerd door alarmsystemen om ongeautoriseerde fysieke toegang te detecteren, evenals door brandbeveiligingshulpprogramma's.

2.2 Priva’s serverruimte

Priva is eindverantwoordelijk voor de fysieke beveiliging, stroom, koeling en opslag in haar serverruimte waarbij voor bepaalde zaken externe expertise wordt ingezet, zoals voor brandbeveiliging. Toegang tot de servers in deze ruimte is beperkt tot bevoegd personeel. Elke andere toegang is alleen toegestaan na goedkeuring van de respectievelijke managers en moet worden begeleid door bevoegd personeel. De ruimte is met passende toegangscontroles beschermd tegen onbevoegd personeel.

2.3 Priva Cloud-diensten

Voor de Priva Cloud-diensten wordt gebruik gemaakt van de Microsoft Azure Cloud. Microsoft Azure is een cloudplatform dat een hoog beveiligingsniveau biedt, zoals wordt bevestigd door de meer dan 90 compliance-certificeringen die Microsoft bezit. Deze certificeringen worden vermeld op de compliance pagina van Azure. Gedetailleerde informatie over de beveiligingsmaatregelen van Microsoft is te vinden in het Microsoft Trust Compliance Center.

Naast Microsoft Azure hebben we onze Priva Cloud-diensten ontwikkeld. Microsoft Azure biedt ons beveiligde datacenters, beveiligde fysieke infrastructuur en standaardcomponenten. Hierdoor kan Priva zich richten op veilig software-ontwerp, veilige codering en veilige configuratie van onze Cloud-diensten. Bij de ontwikkeling en het gebruik van deze diensten passen wij bekende beveiligingsprincipes toe, zoals 'security by design' en 'defense in depth'.

Onze architecten en security specialisten werken nauw samen met de ontwikkelteams, zodat informatiebeveiliging een integraal onderdeel is van het ontwikkelproces. Tijdens de ontwikkeling testen we continu of onze producten en diensten voldoen aan het vereiste beveiligingsniveau. Dit wordt gedaan met behulp van risicobeoordelingen, geautomatiseerde tests en handmatige codebeoordelingen, in overeenstemming met ons beleid voor software ontwikkeling en ander informatiebeveiligingsbeleid.

Om ervoor te zorgen dat Priva (Cloud)diensten veilig zijn, huurt Priva ook onafhankelijke ethische hackers in om periodieke pentesten (penetratietests) uit te voeren. Bevindingen worden onderzocht en opgelost zodat het beveiligingsniveau continu wordt verhoogd. Wanneer een service- of hardware apparaat voldoende is beveiligd, verstrekken de ethische hackers een TPM (Third Party Memorandum) om hun bevindingen over het beveiligingsniveau formeel te bevestigen. Daarnaast is Priva ISO9001 en ISO27001 gecertificeerd.

3. Beveiliging van de infrastructuur

3.1 Netwerkbeveiliging

De netwerkbeveiliging en -bewaking van Priva biedt meerdere lagen van bescherming en verdediging. Firewalls worden gebruikt om het netwerk te beschermen tegen ongeautoriseerde toegang en kwaadaardig verkeer. De firewall-activiteit wordt gemonitord en er gelden strikte werkprocedures. Bovendien zullen firewall-wijzigingen de procedure voor wijzigingsbeheer volgen met een formele goedkeuring. Priva zet netwerksegmentatie in om haar systemen en informatie te beschermen. Voor ontwikkelpraktijken wordt gebruik gemaakt van een, van de productieomgeving gescheiden, testomgeving. De infrastructuur en applicaties worden gecontroleerd op verdachte activiteiten en gecontroleerd op eventuele (technische) kwetsbaarheden. Meldingen worden geactiveerd als er sprake is van abnormale of verdachte activiteit in de omgeving van Priva.

3.2 Netwerkredundantie

Alle kritische componenten in de omgeving en diensten van Priva hebben een hoge mate van beschikbaarheid. Priva maakt gebruik van meerdere routers, gateways en switches om te zorgen voor redundantie op device-niveau. Dit voorkomt dat het interne netwerk van Priva 'single points of failure' heeft.

3.3 Intrusion detection en prevention

Intrusion detection en prevention mechanismen worden gebruikt voor kritieke systemen of servers van Priva. Logboekregistratie wordt gebruikt voor beheerderstoegang en systeemaanroepen op productieservers. Voor Azure-productie resources is Privileged Identity Management (PIM) geïmplementeerd voor de geprivilegieerde toegangsrechten om geprivilegieerde opdrachten uit te voeren. Bovendien wordt multifactor authenticatie afgedwongen op alle Priva-accounts.

Bij de Internet Service Provider (ISP) wordt een 'multi-layered' beveiligingsaanpak gehanteerd. Het omvat netwerkroutering, rate limitering en het verkeer wordt gefilterd.

3.4 Hardening van servers

Servers worden gehardened voordat ze in productie gaan, bijvoorbeeld door ongebruikte functies en netwerkpoorten uit te schakelen en door standaardwachtwoorden te wijzigen. Bovendien worden alle servers voorzien van hetzelfde besturingssysteemimage en consistent groepsbeleid voordat ze in productie gaan.

4. Beveiliging van data

4.1 Security by design

Elke wijziging moet aan de change management procedures van Priva voldoen. Voorafgaand aan een wijziging worden beveiligingsaspecten beoordeeld en overwogen. Ook binnen projecten wordt vooraf nagedacht over beveiliging. Daarnaast heeft Priva een Software Development-beleid met strikte vereisten over beveiligingsaspecten.

4.2 Secure software development

Binnen het Software Development-proces worden geautomatiseerde tests gebruikt om de softwarevereisten automatisch te testen. Deze softwarevereisten worden ingesteld voordat het coderen begint. De geautomatiseerde tests controleren ook op kwetsbaarheden in de code. Naast het automatisch testen, wordt alle softwarecode onderworpen aan een handmatige code review. Priva hanteert een gefaseerde Ontwikkeling, Test, Acceptatie, Productie (OTAP) aanpak. De code wordt getest op beveiligingsvereisten tijdens codebeoordelingen, met behulp van geautomatiseerde code-analysetools en door externe penetratietests.

4.3 Data-encryptie

Alle vertrouwelijke gegevensoverdrachten binnen het netwerk worden tijdens het transport versleuteld met behulp van 'Advanced Encryption Standard' (AES) 256-coderingsalgoritmen en 'Transport Layer Security' (TLS 1.2). Versleuteling wordt gebruikt als een middel om de gegevensintegriteit beter te waarborgen, via beperkingen op wie gegevens kan modificeren via de mogelijkheid om: te lezen (read), te schrijven (write), te wijzigen (modify) of uit te voeren (execute) (r/w/m/x). Priva onderhoudt de wachtwoordzinnen of sleutels die worden gebruikt voor encryptie en decryptie.

- **Data-at-Rest** – Versleuteling voor data-at-rest wordt geleverd op Azure Storage, waarbij Microsoft de codering en sleutels beheert. Alle gebruikte opslagaccounts zijn versleuteld.
- **Data-in-Transit** – Alle gegevens die via openbare netwerken worden verzonden, worden versleuteld. HTTP over TLS (HTTPS) of VPN moet zijn ingeschakeld.
- **Lokale harde schijven** – Lokale HD-codering zorgt voor de beveiliging van gevoelige gegevens die zijn opgeslagen op lokale harde schijven voor werkstations.

4.4 Data-retentie

Priva bewaart gegevens niet langer dan noodzakelijk voor de doeleinden waarvoor ze worden verwerkt. Indien de overeenkomst met klanten wordt beëindigd, zal Priva op verzoek van de klant alle vertrouwelijke informatie van de klant onverwijld teruggeven of vernietigen (zie ook de algemene voorwaarden).

Voor persoonsgegevens houdt Priva zich aan de Algemene Verordening Gegevensbescherming (AVG). Priva bewaart gegevens niet langer dan voor het doel waarvoor deze gegevens worden verwerkt tenzij de gegevens langer moeten worden bewaard om te voldoen aan wettelijke verplichtingen, zoals een wettelijke bewaarplicht periode. Raadpleeg het privacybeleid van Priva voor meer informatie over persoonsgegevens.

5. Identity en access control

5.1 Multifactor authenticatie

Multifactor authenticatie (MFA) wordt afgedwongen voor alle medewerkers en inhuur krachten van Priva. Voor klanten van Priva clouddiensten wordt MFA standaard aangezet ('by default' is dit zo ingesteld). Het wordt ten zeerste aanbevolen voor klanten om MFA te gebruiken. Het biedt een extra beveiligingslaag door naast het wachtwoord een extra verificatiefactor te vragen.

5.2 Digitale toegang

Priva hanteert de principes van 'least privilege' en 'need to know' voor toegang en machtigingen tot systemen en informatie. Toegangsrechten kunnen alleen worden verleend als er een formeel verzoek is met goedkeuring van het desbetreffende management. Daarnaast zullen de toegangsrechten periodiek worden herzien.
De toegang tot de productieomgeving van Priva wordt geregeld door Privileged Identity Management (PIM) en wordt als zodanig 'just-in-time' beheerd. Toegang tot systemen, applicaties etc. wordt gelogd en bewaakt.

6. Operationele security maatregelen

6.1 Vulnerability management

Priva heeft een speciaal proces voor het analyseren en managen van kwetsbaarheden. Er is ook een procedure voor het managen van kwetsbaarheden die de reeks belangrijke regels en overwegingen hiervoor beschrijft. Priva maakt gebruik van geautomatiseerde scantools van derden en penetratietesten door externe security organisaties. De kwetsbaarheden worden frequent beoordeeld en besproken door security specialisten van Priva. Kwetsbaarheden worden beheerd en geprioriteerd op basis van het risico. Kwetsbaarheden worden opgevolgd totdat ze zijn verholpen door ofwel de kwetsbare systemen te patchen of relevante andere controles toe te passen.

6.2 Logging en monitoring

Priva monitort en analyseert informatie die wordt verzameld uit diensten en gebruik van bedrijfsmiddelen. Deze informatie wordt vastgelegd in de vorm van eventlogs, auditlogs, fault logs, administrator logs en operator logs. Deze logs worden automatisch gecontroleerd en geanalyseerd in een redelijke mate die helpt bij het identificeren van anomalieën zoals ongebruikelijke activiteiten in de accounts van werknemers of pogingen om toegang te krijgen tot informatie. De logs worden opgeslagen op een beveiligde server, geïsoleerd van volledige systeemtoegang, om de toegangscontrole centraal te beheren en de beschikbaarheid te garanderen. De clouddiensten van Priva worden gemonitord en verstoringen worden genoteerd op het Priva Status Dashboard.
Om de verschillende logs te monitoren, worden verschillende systemen gebruikt met geautomatiseerde waarschuwingen op basis van de ernst van een alert.

6.3 Malware-protectie

Er zijn detectie-, preventie- en herstelmaatregelen geïmplementeerd om te beschermen tegen malware. Servers en werkstations binnen Priva worden automatisch geüpdatet met bescherming tegen malware. Priva maakt gebruikt van het geautomatiseerd scannen van systemen om te voorkomen dat malware zich naar het Priva-netwerk verspreidt. Priva gebruikt ook detectietools van derden om kwaadaardig verkeer, zoals phishing en spam, te identificeren. De medewerkers en inhuur krachten van Priva zijn ook verplicht om de SQC-training te volgen. Hierin worden zij getraind in beveiligingsbewustzijn, inclusief het herkennen van phishing en malware en hoe dit te melden bij Priva.

6.4 Back ups en restore

Priva maakt dagelijks back-ups van fysieke servers, virtuele servers, databases, configuraties van switches en routers en appliances. Back-ups worden lokaal opgeslagen en dagelijks naar de cloud gekopieerd. Restore van de back-ups gebeurt regelmatig in testomgevingen. In productieomgevingen wordt indien nodig een restore uitgevoerd.

6.5 Disaster recovery en bedrijfscontinuïteit

Applicatiegegevens worden opgeslagen op flexibele opslag die wordt gerepliceerd in datacenters. In de datacenters zijn stroomback-up, temperatuurbeheersingssystemen en brandpreventiesystemen als fysieke maatregelen om de bedrijfscontinuïteit te waarborgen. Deze maatregelen helpen Priva om flexibiliteit en redundantie te realiseren. Priva heeft een calamiteitenplan waarin de procedures staan beschreven bij calamiteiten of calamiteiten.

6.6 Beveiliging van de werkstations

Alle werkstations draaien op een up-to-date OS-versie en zijn geconfigureerd met antivirussoftware. Alle activiteiten worden gelogd en gecontroleerd en monitoringsystemen geven geautomatiseerde waarschuwingen indien nodig. Deze waarschuwingen worden afgehandeld door IT- en informatiebeveiligingsspecialisten. Werkstations zijn ingericht volgens de beveiligingsstandaarden van Priva. Alle stations moeten worden geconfigureerd, gepatcht en gevolgd volgens de praktijken van Priva voor werkplekbeheer. Priva heeft operationeel en technisch informatiebeveiligingsbeleid ontwikkeld en geïmplementeerd, waarin ook de beveiliging van werkplekken aan de orde komt. Mobiele werkstations van Priva zijn geconfigureerd om 'data in rest' te beschermen met behulp van Full Disk Encryption. Bovendien wordt er een complex wachtwoordbeleid gehanteerd. Op basis van dit beleid worden sterke wachtwoorden en multifactor authenticatie ook technisch afgedwongen.

7. Security incident management

7.1 Incident response

Priva heeft een Security Incident Management procedure geïmplementeerd. Incidenten worden opgespoord en indien nodig worden passende corrigerende maatregelen genomen. De procedure schetst ook de verantwoordelijkheden van alle partijen en externe communicatie. Daarnaast zal Priva root cause analyses uitvoeren om (aanvullende) controles te implementeren om herhaling van soortgelijke gebeurtenissen te voorkomen.

7.2 Datalek

Priva heeft een intern beleid voor datalekken en een procedure voor het melden van datalekken die in lijn is met de AVG. Priva meldt een inbreuk binnen 72 uur na melding van de inbreuk aan de betrokken Autoriteit Persoonsgegevens, in lijn met de AVG. Afhankelijk van specifieke wensen informeert Priva indien nodig ook de klanten. Als gegevensverwerker informeert Priva de betrokken gegevensbeheerder(s) onverwijld in geval van een datalek.