ORTHOVENTIEF
uw partner voor onderwijskwaliteit

Beveiligingbeleid Orthoventief 2018

Versiedatum: 15-3-2018

Algemeen

Orthoventief streeft naar een optimale beveiliging van de door haar, via CIS-Websolutions, gehuurde ICT systemen voor zowel ontwikkeling- als voor productie-omgevingen. Hierbij wordt gebruik gemaakt van een aantal standaard basisregels: minimale toegang, veilige verbindingen, up-to-date besturingssysteem en vooral gezond verstand. Wij onderscheiden in de basis twee soorten productie-omgevingen: shared-hosting en webapplicaties.

Voor alle servers van CIS-Websolutions gelden de volgende richtlijnen:

- hosting in professionele datacentra, gesitueerd in Nederland
- beheertoegang alleen via SSH
- SSH alleen geopend voor de strikt noodzakelijke ip-adressen
- geen shell toegang tot de server voor klanten (m.u.v. dedicated VPS omgevingen)
- dagelijkse backup van belangrijke bestanden (web-omgeving, databases en mail)
- continue monitoring van belangrijke services
- SSL certificaten worden op verzoek van de klant geïnstalleerd
- minimaal eenmaal per maand een update van het besturingssysteem en systeemsoftware
- op een enkele uitzondering na (een Windows server) draaien onze omgevingen op Centos 6 of hoger

Shared hosting

Onder shared-hosting verstaan wij webservers waarop algemene websites worden gehost, waaronder SchoolDataBeheer. Tenzij anders overeengekomen is, onderhoudt onze partner CIS-websolutions deze omgevingen op het niveau van het besturingssyteem en overige systeemsoftware zoals Apache, MySQL en PHP. Het CMS zelf wordt door Orthoventief bijgewerkt en up-to-date gehouden.

Applicatie-hosting

SchoolDataBeheer wordt gehost op een dedicated VPS. Behalve CIS-Websolutions heeft niemand directe toegang tot de shell of database. De omgeving is exclusief toegekend aan Orthoventief SchoolDataBeheer.

Alleen Orthoventief kan een verzoek indienen om deze toegang toe te kennen of af te sluiten.

Alle applicatie-servers van CIS-websolutions zijn voorzien van een versleuteld bestandssysteem zodat diefstal, vervreemding of vervanging van een harddisk uit de server niet kan leiden tot een datalek.

Kantooromgeving

De aan SchoolDataBeheer werkende ontwikkelaars van CIS-Websolutions en Orthoventief werken met Windows, Linux of Apple-systemen. Indien op deze pc's vertrouwelijke klantgegevens staan, zijn deze voorzien van een versleuteld bestandssysteem.

USB sticks worden alleen gebruikt indien deze voorzien zijn van encryptiesoftware, zoals bijvoorbeeld EncryptStick (Lite).

Documenten van vertrouwelijke aard worden zo spoedig mogelijk na gebruik vernietigd in een papierversnipperaar. Ditzelfde geldt voor CD's en DVD's met vertrouwelijke data. Defecte harddisks worden te allen tijden fysiek zodanig beschadigd dat deze niet meer bruikbaar zijn alvorens zij afgevoerd worden.

De kantoren van zowel CIS-Websolutions als Orthoventief zijn voorzien van een alarmsysteem met deurmelders, brandmelder en daaraan gekoppeld een abonnement bij een meldkamer.

Toegang door derden of partners van Orthoventief en CIS-Websolutions

Uitsluitend Orthoventief kan een verzoek indienen voor een DNS wijziging of verhuistoken om een domeinnaam gerelateerd aan Orthoventief af te geven. Dit geldt ook voor verzoeken over informatie betreffende een systeem of de beveiliging van een systeem.

Tijdelijke krachten, stagiaires en partners van CIS-Websolutions en/of Orthoventief krijgen alleen toegang tot de servers indien zij hiervoor een amenwerkingsovereenkomst met daarin een geheimhoudingsverklaring getekend hebben.

Onderhoud van de servers

Onder het onderhoud verstaan we enerzijds de dagelijkse controle op een goed functioneren van de disk-drives. De services worden continu door CIS-Websolutions gecontroleerd vanaf twee verschillende nodes. Indien een service niet werkt, wordt hierover een mailbericht en sms-bericht verzonden.

Anderzijds heeft onze partner CIS-Websolutions een abonnement op diverse nieuwsbrieven en announcement-list van hun Linux distributie. De servers draaien CentOS6 (ondersteund tot december 2020) of CentOS7.

De normale update-frequentie betreft minimaal eenmaal per maand. Voor SchoolDatabeheer geldt een intensiever backup-beleid. Bij tussentijdse, ernstige bedreigingen zoals destijds bijvoorbeeld Heartbleed en Shell Shock onderneemt CIS-Websolutions direct actie. Dit geldt voor zowel productie-systemen, maar ook voor ontwikkelsystemen.

Mail policy

E-mail is een nog veel gebruikt medium om te communiceren. Vaak worden hierbij ook gevoelige gegevens verstuurd, te denken valt aan wachtwoorden of aan gegevens die betrekking hebben op personen waarvan er gegevens in onze systemen en applicaties bewaard worden.

Mailberichten van deze aard worden direct na behandeling of afhandeling gewist op een zodanige wijze dat deze ook niet meer uit de prullenbak terug te halen zijn.