Veiligheidsbeleid Revee Creative Communication

Voor de gegevens die door Revee gehost worden, en daarmee ook voor de klantgegevens in de webapplicaties, geldt een gedeelde hoogste prioriteit voor beschikbaarheid en veiligheid. De gegevens staan op eigen servers in het streng beveiligde EvoSwitch-datacenter in Haarlem en in backup-archieven elders. De beschikbaarheid en veiligheid wordt op de volgende manieren gewaarborgd:

Beschikbaarheid

Van alle gegevens wordt elke nacht een backup gemaakt op twee geheime gescheiden kantoorlocaties in Nederland. De server zelf gebruikt redundante harddisks zodat het systeem bij een defecte schijf blijft werken, terwijl de schijf zelf zo snel mogelijk vervangen wordt om de redundantie in stand te houden. Het datacenter zelf levert bovendien een meervoudig redundante stroomvoorziening en netwerktoegang en heeft een brandbeveiliging waarin bescherming van data en apparatuur voorrang heeft (brandbestrijding d.m.v. edelgassen in plaats van blusmiddelen).

Beveiliging

Fysieke toegang

Fysieke toegang tot een server is de zwakste schakel in de keten. Het EvoSwitch datacenter heeft een streng toegangsbeleid en 24/7-bewaking die ervoor zorgt dat iedere aanwezige server alleen door bevoegd personeel bereikt kan worden. De locaties van de backup-archieven zijn geregeld bemand en anders goed afgesloten. Alle werkstations waarin opgeslagen toegang zit tot beveiligde omgevingen zijn afgeschermd met sterke wachtwoorden en hebben een automatische scherm-lock na 2 minuten inactiviteit waarna opnieuw het wachtwoord moet worden ingevoerd. De werkstations en backup-servers bevinden zich in werkruimten die worden afgesloten bij afwezigheid van bevoegden.

Wanneer fysieke opslagmedia in servers worden vervangen, worden zij voor hergebruik of afvoer “gezero’d”, dat wil zeggen dat de gehele schijf overschreven wordt met lege data waardoor verwijderde bestanden niet met recovery-software kunnen worden teruggehaald. Defecte media waarmee dit niet meer mogelijk is, worden voor afvoer verder beschadigd om recovery te voorkomen.

Data taps

Revee kan niet instaan voor de weg tussen eindgebruiker en onze servers, wel voor het feit dat alle transacties waarbij klantgegevens worden overgedragen (voor zover dat via Revee gebouwde of onderhouden websites gaat), via versleutelde (SSL)-verbindingen gebeuren.

Publiek toegankelijke poorten

De enige poorten van de server die voor de volledige buitenwereld toegankelijk zijn, zijn die voor afhandeling van email, http(s) (webpagina’s) en ftp (bestandsbeheer). Rechtstreekse toegang tot de database-server, die bijvoorbeeld de klantgegevens (van klanten van Revee-klanten) in webwinkels of andere webapplicaties, is niet

van buitenaf mogelijk, alleen door andere processen op de server zelf (zoals de betreffende applicatie). Via FTP hebben klanten van Revee alleen toegang tot hun eigen websites en via hun webapplicaties alleen tot de aan hen toegewezen databases, en dan alleen bij sites die niet door Revee worden onderhouden. Er is geen FTP-account voor globale (root-)toegang tot de servers zelf. Deze toegang is alleen mogelijk via SSH, en deze dienst is alleen bereikbaar via een versleuteld VPN dat alleen bereikbaar is met de juiste certificaten, die alleen aan bevoegd personeel worden uitgereikt. Voor de FTP- accounts van de klanten dwingt Revee zeer sterke wachtwoorden af. Verder is het aantal op onze server gehoste projecten zeer klein waardoor alle activiteit te overzien is en verdachte toegang opvalt. Hiervoor worden dagelijks de logfiles geanalyseerd (deels automatisch en deels handmatig). Verder wordt iedere poging tot het 'scannen' van FTP- wachtwoorden gedetecteerd en geblokkeerd door de firewall. Aangezien FTP zelf door Revee ook als onveilig protocol beschouwd wordt, worden de applicaties die Revee zelf bouwt of onderbouwd alleen via het Revee-VPN met FTP benaderd. Toegang van buitenaf tot deze sites is geblokkeerd.

Webapplicaties en CMS-sites

Revee is verwerker van de gegevens inclusief de web-applicatie waarin deze gegevens worden opgeslagen, de opdrachtgevers van Revee zijn daarmee in principe verantwoordelijk voor de veiligheid van deze applicaties. Er zijn hierin nuanceringen waarin Revee uit beveiligingsoogpunt meer rollen vervult dan alleen die van verwerker:

Bij **door Revee (door-)ontwikkelde webapplicaties** draagt Revee een gedeelde verantwoordelijkheid voor de applicatie samen met de opdrachtgever. Revee kan veiligheidsrisico's detecteren maar is afhankelijk van de opdrachten van opdrachtgever om deze aan te pakken. Dit geldt ook voor het installeren van beschikbare updates op software van derden.

Bij een **webapplicatie met onderhoudscontract** is Revee verantwoordelijk voor de veiligheid van de webapplicatie voor zover hiervoor nodige werkzaamheden binnen het onderhoudscontract vallen. In andere gevallen blijft de verantwoordelijkheid beperkt tot het melden van het probleem en het geven van advies met betrekking tot de oplossing.

In aanvulling op beide situaties geldt dat bij overname van de ontwikkeling van een applicatie of gebruik van een bestaand systeem (zoals Concrete5, WordPress of Magento) Revee in principe mag uitgaan van het veilig zijn van de software zoals deze wordt aangeleverd en niet geacht kan worden veiligheidsrisico's te ontdekken anders dan door het constateren van reeds optredende problemen of verdachte activiteiten, of het op de hoogte gebracht worden door de ontwikkelaars.