Bijlage e. Security IT-infrastructuur voor CIMS

Van: 5.1.2e <5.1.2e @rivm.nl>
Verzonden: donderdag 3 december 2020 11:09
Aan: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
CC: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
Onderwerp: Zwakke plekken in de IT-infrastructuur voor CIMS

5.1.2e

Na het lezen van het Kwaliteitsmanagementplan en de Code Review Procedure maak ik mij zorgen dat de informatiebeveiliging voor CIMS niet aan de eisen van de NEN7513 en de ISO27001/2 voldoet. Ik heb deze zorgpunten ook met 5.1.2e al gedeeld omdat ze van invloed zijn op de privacy en meegenomen kunnen worden in de PIA en met 5.1.2e om ze te verwerken in de overall risicoanalyse van CIMS.
Dit zijn mijn zorgpunten:

1. Het beheer van speciale toegangsrechten (systeembeheerders en databasebeheerder) is nu nog onvoldoende beperkt en gecontroleerd. Voor CIMS zou dit sterk beperkt moeten worden. Voor de database heb ik aan Ordina gevraagd wat er moet gebeuren om de logging op Oracle voor de database beheerders in te stellen. Deze vraag kwam naar voren omdat bij het bespreken van de site-to-site VPN verbinding voor beheer door Ordina bleek dat er geen logging was voor database beheerders van Ordina terwijl ze in principe bij alle data kunnen zonder dat er een audittrail is.
2. Het toewijzen van geheime authenticatie-informatie (lees wachtwoorden) is nog geen formeel beheersproces. Nieuwe tijdelijke wachtwoorden worden vaak nog via de telefoon doorgegeven zonder verificatie van de identiteit. Het instellen van een wachtwoordportaal zou hier een oplossing zijn. Er is al een wachtwoordportaal voor RIVM medewerkers maar dit werkt blijkbaar nog niet goed en is ook niet algemeen bekend.
3. De beoordeling van toegangsrechten van gebruikers op periodieke basis is voor mij een vraagteken. De eigenaar van de applicatie zou periodiek een overzicht moeten krijgen van alle gebruikers van CIMS (ook externe die via RIVM informatie krijgen uit CIMS). Dit overzicht zou beoordeeld moeten worden op juistheid en volledigheid. De eigenaar of gedelegeerde zou ook de toewijzing van toegangsrechten, met de soort toegang, moeten goedkeuren. Hiervan moet ook een registratie worden bijgehouden. Uit Active Directory kan een lijst gemaakt worden met medewerkers die toegangsrechten hebben voor CIMS. Daarin staat nog niet welk soort rechten men heeft maar wellicht wordt in CIMS zelf ook bijgehouden wie wat mag.
4. Het intrekken van toegangsrechten wordt, voor gebruikers die binnen RIVM van functie veranderen, nog niet of onvoldoende gedaan. Vooral bij interne functiewijziging of verhuizing is er geen goede registratie of van medewerkers de rechten ingetrokken of gewijzigd worden. Hierdoor kunnen rechten blijven bestaan, dus ook toegangsrechten voor CIMS. Hier zou personeelszaken een belangrijke rol kunnen vervullen door tijdig te melden dat medewerkers van functie veranderen. Vertrekkende medewerkers worden nu al goed doorgegeven omdat via IDM hun rechten tijdig worden ingetrokken maar voor interne functiewijzigingen gebeurt dit niet goed.
5. Toegang tot programmacode voor CIMS is voor mij niet helder of daar beperkingen liggen of dat beheerders daar ook bij kunnen. Nu nog kunnen beheerders in principe overal bij.
6. Er is geen beleid inzake cryptografische beheersmaatregelen en dus ook niet voor sleutelbeheer. Voor de back-up op een geografisch andere locatie zou dat wel wenselijk zijn maar ook intern gezien de gevoeligheid van de informatie. Back-ups worden met Commvault gemaakt die op dit moment 3 back-ups maakt, twee binnen het eigen rekencentrum en een naar BPM (cloud provider). Deze laatste is geen off-line back-up maar een identieke kopie van de interne back-up. Storage beheerders hebben tot alle drie de back-ups toegang.
7. Er zijn fysieke beveiligingsrichtlijnen bij Equinix (het datacenter) maar daar is recent het een en ander over te doen geweest omdat medewerkers van Equinix zonder onze toestemming toegang hebben gehad tot onze "kooi" waar de apparatuur staat. Dit is dus niet goed geregeld en afgesproken. Hiervoor loopt al een traject met andere overheidsgebruikers van Equinix.

8. Beveiliging van de apparatuur die zich buiten het terrein bevinden, en dan moet je denken aan laptops, voldoet voor de normale bedrijfsactiviteiten maar als we hier praten over BBN3 informatie dan kan ook die informatie thuis of ergens anders geprint worden op een lokale printer (geen USB-sticks). Ook via webmail kan lokaal informatie opgeslagen worden. We maken dus geen onderscheid voor de mail. Met webmail kun je dus lokaal bestanden opslaan die je via de mail hebt ontvangen. Gezien de gevoeligheid van de informatie is het advies om hier via policies op laptops beperkingen op te leggen voor die medewerkers die met informatie uit CIMS werken.
9. Scheiding van ontwikkel-, test en productieomgeving is er wel maar of dat ontwikkelaars niet in de productieomgeving kunnen komen is niet duidelijk. Het advies is om voor ontwikkelaars de rechten te beperken voor de operationele- maar ook de acceptatie-omgeving.
10. Er worden, volgens mij, wel logs gemaakt van gebruikersactiviteiten (voor Praeventis en CIMS in ieder geval wel), maar beperkt van beheerders en niet van database administrators terwijl die de meeste rechten hebben. De activiteiten van beheerders kunnen vrij eenvoudig gelogd worden door de systeemlogfaciliteiten op de servers te activeren en die logs naar het SIEM te sturen. Voor de database administrators moet dit in de database gebeuren of via RBAC. Dat laatste is een project dat nog moet starten. Voor de databaselogging ligt de vraag even bij Ordina.
11. Beheer van technische kwetsbaarheden gaat via pentesten maar de reikwijdte daarvan is beperkt. Zo worden technische kwetsbaarheden zoals bijvoorbeeld systeemhardening, netwerkisolatie voor gevoelige systemen of gebrekkige gebruikersadministratie niet zichtbaar in pentesten. Pentestresultaten zouden uitgebreid kunnen worden met de interne auditinformatie of in dit geval met de informatie uit het voorgestelde speerpuntenplan om de informatiebeveiliging naar een hoger niveau te brengen.
12. Audits op kwetsbare systemen worden niet regelmatig uitgevoerd. Met audits bedoel ik het toetsen van systemen tegen bestaande regelgeving, beleid, procedures en processen. Als die kaders er niet zijn kun je ook niet toetsen. Er ligt nu een concept informatiebeveiligingsbeleidsplan en een concept handboek informatiebeveiliging.
13. Scheiding in netwerken op basis van classificatie van systemen vindt nu niet plaats. CIMS zou geplaatst moeten worden in een aparte netwerkzone. In het speerpuntenplan staat microsegmentering al genoemd.
14. Een punt van aandacht is de overeenkomst over informatietransport tussen RIVM en externe partijen. Ik heb daar geen zicht op maar het is een onderdeel van het ISO27001 managementsysteem.
15. Geheimhoudingsovereenkomsten zijn er voor eigen medewerkers en in de meeste gevallen ook voor externen maar de vraag is of met name voor de externen daar een centraal register voor is.
16. Er is geen beleid voor beveiligd ontwikkelen van software. Er zijn wel richtlijnen en kwaliteitscriteria maar die zijn niet dwingend voorgeschreven. Ook voor een code review zijn er wel richtlijnen die aangeven wat je moet doen maar niet hoe.
17. Er zijn geen principes voor engineering van beveiligde systemen (er is een handboek waarin deze beschreven zijn maar dat moet nog goedgekeurd worden). Nu worden nog veelal de richtlijnen van leveranciers gevolgd wat op zich voldoende zou moeten zijn maar we registreren geen afwijkingen daarvan. Deze afwijkingen zijn er wel omdat door omstandigheden dit soms niet anders kan, door verouderde software e.d., maar ze kunnen en moeten wel goed geregistreerd worden t.b.v. de eventuele explain.
18. Systeemacceptatietest moet je niet alleen op functionaliteit doen maar ook op performance, beschikbaarheid, capaciteit en veiligheid. Ik heb nog geen rapportage gezien waarin ze alle vier beoordeeld zijn.
19. Testgegevens zijn vaak niet geanonimiseerd. Meestal wordt productiedata genomen met alle privacyaspecten die daarmee geschonden worden maar je kunt ook geen uitzonderingen goed testen omdat je productiedata meestal correcte gegevens bevat. Dit is niet simpel en snel op te lossen maar het advies is wel om hier eens mee te starten omdat CIMS en Praeventis gevoelige informatie bevatten en een testset met fake gegevens geeft meer informatie over de verwerking en eventuele fouten dan gebruik van productiegegevens.
20. Zijn of worden de informatiebeveiligingseisen en risico's van de data leverancier geïnventariseerd? Ik heb het nog niet meegemaakt.
21. Zijn de intellectuele eigendomsrechten geïnventariseerd en vastgelegd, van zowel data als systemen?

22. Worden alle registraties beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave? Worden alle invoergegevens in invoerbestanden na verwerking in CIMS vernietigd of opgeslagen? Niet vernietigen betekent ook dat ze beschermd moeten worden tegen onbevoegde toegang.

Met vriendelijke groet,

5.1.2e

5.1.2e