NIEUWSBRIEF ICT NML

ICT NML

Editie 2
Juli 2023

Welkom

Welkom beste gemeenteraadsleden. Voor u ligt de nieuwsbrief van ICT NML. Minimaal twee keer per jaar houden we u door middel van een digitale nieuwsbrief op de hoogte van relevante onderwerpen en ontwikkelingen op het gebied van ICT, telefonie en de samenwerking.

Veel leesplezier!

Jaarverslag

Het jaarverslag 2022 is verschenen. U ontvangt een digitaal exemplaar als bijlage bij deze nieuwsbrief.

Jurgen Tessers: “Afgelopen jaren is een stevig fundament gebouwd waarop de organisatie en onze dienstverlening kan groeien en ontwikkelen. De resultaten van 2022 zijn de verdienste van het team dat onder aanvoering van Richan, Joost, Martien en Rob een prachtig resultaat heeft gerealiseerd. Aan mij de eervolle taak om ICT NML de komende jaren verder te laten groeien en ontwikkelen, waarbij een stevig fundament en vertrouwde dienstverlening een belangrijke basis vormt. Innovatie? Groei? Ja graag, mits de basis op orde blijft.”

Nieuw Werkplekconcept

Ondanks dat het huidige werkplekconcept nog steeds een goede basis vormt, is er enige tijd geleden geconstateerd dat we hiermee niet voldoende tegemoet komen aan het ontzorgen van de deelnemers. Een nieuw werkplekconcept moet inzetten op CYOD (door bedrijf aangeboden apparaat), ofwel ‘managed devices’. Op dergelijke apparaten mag een gebruiker dan ook ondersteuning verwachten. Uit gebruikersmeldingen van de afgelopen twee jaar zien we dat deze behoefte erg groot is.

Na enkele technische tegenslagen, zijn we er met heel veel wilskracht en hard werk toch in geslaagd om de uitrol te starten conform de in december/januari overeengekomen planning. Op dit moment hebben we de uitrol bij de gemeente Someren en Asten volledig afgerond.
Op (slechts) enkele gemelde incidenten na, waar we hard mee aan het werk zijn gegaan, zijn de gebruikers tevreden over de werking en mogelijkheden van de nieuwe managed werkplek.
Bij de gerealiseerde uitrollen is de samenwerking tussen het ICT NML project team en de interne IT medewerkers bij de beide gemeenten optimaal geweest. De gebruikers zijn zo optimaal mogelijk ondersteund bij de overgang naar de managed werkplek. Er heerste, ondanks enkele uitdagingen, een algemene prettige en positieve werksfeer. Daarnaast is de managed werkplek zelf door velen als positief ervaren.

De eerstvolgende gemeente die gemigreerd wordt, is de gemeente Venlo. In de loop van de komende weken wordt er met de resterende drie gemeenten (Roermond, Weert en Nederweert) gekeken wat de mogelijkheden zijn om ook hier te starten met de uitrol van de managed werkplek. Ondanks de geplande uitrol blijven we, samen met onze leveranciers, bezig om de werking en beleving van de managed werkplek verder te optimaliseren.

Blik vooruit

Naast de reguliere ICT ondersteuning gaan we komende periode ook aan de slag om twee andere projecten af te ronden. Het gaat dan met name om:

Project Netwerk Redesign

Enige tijd geleden zijn sterk verouderde netwerkcomponenten vervangen en is er van de gelegenheid gebruik gemaakt om – middels het project Netwerk redesign - het ontwerp van het netwerk nog eens kritisch tegen het licht te houden zodat deze voldoet aan de huidige technische- en beveiligingseisen.

Het project is voor 98% afgerond en er is de afgelopen maanden de nodige tijd gestoken in de laatste twee openstaande acties binnen dit project. Dit gaat om:

- Het netwerk klaarmaken zodat IPv6 gebruikt kan worden;
- het optuigen en testen van een HA (high availability) verbinding tussen de twee datacenters.

IPv6 is op dit moment nog niet volledig beschikbaar/bruikbaar omdat de techniek hierin nog niet voorziet in standaard oplossingen. Voor wat betreft de issues met betrekking tot de HA verbinding zijn we in nauw contact met T-Mobile (Tele 2). Zij moeten zorgen voor een oplossing zodat ook dit punt kan worden afgerond.

Project Bestelproces

Het inregelen van het geautomatiseerd proces om de veiligheidsvoorraden van de gemeenten op peil te houden duurt helaas langer dan gepland. De vertraging wordt veroorzaakt door problemen bij leverancier Dustin. Vanuit ICT NML is dit geëscaleerd en er zijn inmiddels vanuit Dustin toezeggingen gedaan om e.e.a. op te pakken en af te handelen.

Meerwaarde van TPM Verklaring ICT NML

In oktober van elk jaar levert ICT NML een TPM verklaring af aan de deelnemende gemeenten. Deze verklaring is opgesteld door een onafhankelijk auditor van BKBO en vertelt de deelnemende gemeenten hoe het er bij ICT NML voor staat met informatiebeveiliging.

Wat is een TPM verklaring?

TPM staat voor Third Party Memorandum of een Derdenverklaring in goed Nederlands. De verklaring wordt opgesteld door een onafhankelijke derde, de auditor en zegt iets over de dienstenlevering en -beheersing van een organisatie. In het geval van ICT NML onderzoekt de auditor in hoeverre ICT NML voldoet aan de maatregelen van de Baseline Informatiebeveiliging Overheid (BIO).

Waarom een TPM verklaring?

Informatiebeveiliging wordt steeds belangrijker in onze gedigitaliseerde samenleving. ICT NML is verantwoordelijk voor het beheer van de ICT infrastructuur van zes gemeenten. Deze zes gemeenten samen hebben veel en ook gevoelige informatie. Via de TPM verklaring rapporteert ICT NML aan de gemeenten hoe wij om gaan met informatie-beveiliging. De auditor kijkt naar een breed spectrum van maatregelen, variërend van het sluiten van de voordeur tot het maken van back-ups en het reageren op beveiligings-incidenten.

Minstens net zo belangrijk is dat de auditor ons ook adviezen meegeeft waarmee we informatiebeveiliging naar een nog hoger niveau kunnen brengen. Deze adviezen zijn voor ons daarom erg belangrijk en we vertalen die dan ook naar concrete actiepunten.

Niet van ICT NML alleen

Hoewel ICT NML de TPM verklaring laat opstellen, is de verklaring niet van ons alleen. De auditor kijkt naar de hele samenwerking en geeft ook adviezen over wat de gemeenten moeten regelen of waarover ICT NML en de gemeenten samen afspraken moeten maken. Ook op het gebied van informatiebeveiliging zijn we een echt samenwerkingsverband.

SIEM/SOC

Het is een veelgehoord begrip en ook een verplichting vanuit de Baseline Informatiebeveiliging Overheid: overheidsinstanties moeten een SIEM hebben om daarmee hun digitale infrastructuur te beschermen. Maar wat is het en wat heeft u eraan?

Wat is een SIEM/SOC?

SIEM/SOC wordt vaak in een adem genoemd maar het zijn feitelijk twee aparte onderdelen die elkaar aanvullen.

- SIEM

SIEM staat voor Security Information and Event Management. Dit is een softwareproduct dat in staat is om informatie uit diverse informatiesystemen te verzamelen, te correleren en te analyseren op mogelijke risico's voor informatiebeveiliging.

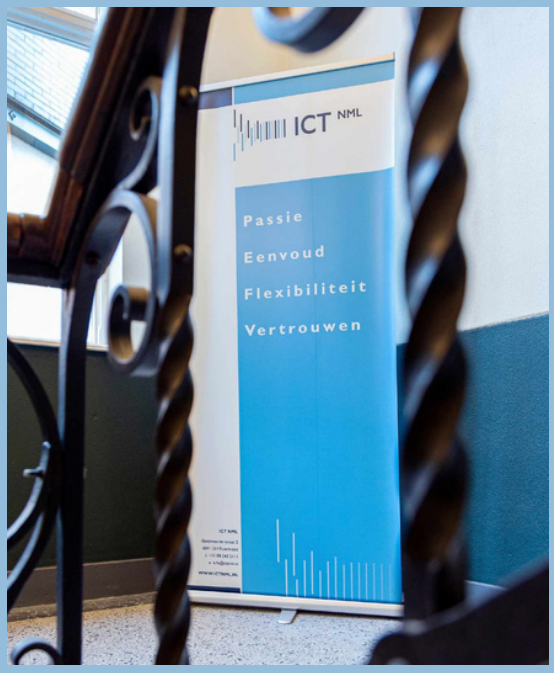
- SOC

SOC staat voor Security Operations Center. In het SOC werken goed getrainde analisten dag en nacht om meldingen uit o.a. een SIEM te onderzoeken en erop te reageren. Bij een incident, kunnen zij meteen actie ondernemen; bij een cyberaanval telt elke seconde.

Deze twee onderdelen samen leveren een belangrijke bijdrage aan de informatiebeveiliging van een organisatie. Maar het vraagt ook iets van een organisatie, want op een melding van het SOC moet adequaat gereageerd worden. Daarvoor moet een goed proces ingericht zijn en moet bekend zijn wie op een melding kan reageren.

Waar staan we?

Bij ICT NML vinden wij het belangrijk om zowel een SIEM als een SOC te hebben. Tegelijk willen we hier de noodzakelijke expertise bij hebben. Om deze redenen heeft ICT NML naar een ervaren partner gezocht die ons kan ondersteunen bij het zo effectief mogelijk inzetten van een SIEM/SOC. We zijn momenteel bezig met de voorbereiding voor een proef met de SIEM/SOC dienst van deze partner. Deze proef zal medio juli afgerond zijn. Als de geleverde dienstverlening voldoet aan onze acceptatiecriteria, gaan we daarna direct verder met de gekozen oplossing. Daarmee zetten we een belangrijke stap naar nog betere beveiliging.



Dit is een uitgave van:
ICT NML
Godsweerderstraat 2
6041 GH Roermond